

Practicing Safe Computing by [Hal Bookbinder](#)
Index

Article	Published	Page
#106: Your password has expired	November 2024	113
#105: Accidental and criminal cyber disruption	August 2024	112
#104: Free product trials	July 2024	111
#103: One of the biggest breaches that you never heard of	June 2024	110
#102: Avoiding payment app theft	May 2024	109
#101: Even if you do everything right...	April 2024	108
#100: Data breach awareness	March 2024	107
#99: Finding your iPhone, Android, and more	February 2024	106
#98: Password Managers, a 2024 update	January 2024	105
 #97: Translation tools	 December 2023	 104
#96: 23andMe personal data exposure	November 2023	103
#95: Internet Relationship Scams	October 2023	102
#94: Spear phishing messages	September 2023	101
#93: Ten Commandments to avoid AI Scams	August 2023	100
#92: Computer Cache and Cookies	July 2023	99
#91: Your own Internet access point	June 2023	98
#90: Artificial Intelligence	May 2023	97
#89: Tax Scams	April 2023	96
#88: Dangers of saving passwords in your browser	March 2023	95
#87: Cybersecurity Tips	February 2023	94
#86: Package delivery, banking, and Social Security scams	January 2023	93

See next page for earlier articles

[Go to Index](#)

Practicing Safe Computing by [Hal Bookbinder](#)
Index

Article	Published	Page
#85: Search tips for selected genealogy websites	December 2022	92
#84: Stopping Text and Voice Spam	November 2022	91
#83: Your wallet has been stolen, now what?	October 2022	90
#82: Cyber warfare 2022, a midyear update	September 2022	89
#81: Free Online Databases Courtesy of Your Public Library	August 2022	88
#80: Take care what you share	July 2022	87
#79: Phishing Text Messages	June 2022	86
#78: 1950 Census Search Tips	May 2022	85
#77: Nothing is certain but death and taxes	April 2022	84
#76: Upgrading to Windows 11	March 2022	83
#75: Cyber warfare, 2022	February 2022	82
#74: A Browser that will not track your every move	January 2022	81
#73: Charity Review Websites	December 2021	80
#72: Contingency Planning	November 2021	79
#71: Keeping email contacts up to date	October 2021	78
#70: Windows Ease of Access – Vision Support	September 2021	77
#69: Even an 8-year-old Yahoo breach can bite!	August 2021	76
#68: Protecting your credentials	July 2021	75
#67: Recovering files using OneDrive	June 2021	74
#66: Yet Another Data Breach!	May 2021	73
#65: Looking your best while on Zoom	April 2021	72
#64: Private Browsing	March 2021	71
#63: Using Zoom to Create a Personal Video Message	February 2021	70
#62: Reducing the Impact of Data Breaches	January 2021	69

[Go to Index](#)

Practicing Safe Computing by [Hal Bookbinder](#)
Index

Article	Published	Page
#61: Ten Software Fixes	December 2020	68
#60: Misleading Google Results	November 2020	67
#59: We are holding a package for you	October 2020	66
#58: Vishing (Voice phishing)	September 2020	65
#57: Ransomware in the age of COVID-19	August 2020	64
#56: Practicing Safe Zoom	July 2020	63
#55: COVID-19 Statistics	June 2020	62
#54: Credit card skimming	May 2020	61
#53: Avoiding COVID-19 Scams	April 2020	60
#52: You've Got DNA Matches!	March 2020	59
#51: USB recharging cord and Bluetooth Risks	February 2020	58
#50: Discovering if you have been pwned	January 2020	57
 #49: Data Management and Protection	 December 2019	 56
#48: Making the most of your Password Manager	October/November 2019	55
#47: Windows Updates	September 2019	54
#46: Apples are also vulnerable	August 2019	53
#45: You Likely Need a VPN	July 2019	52
#44: PC Magazine as a Source	June 2019	51
#43: Is Windows Defender Sufficient?	May 2019	50
#42: Synthetic Identity Theft	April 2019	49
#41: Google Chrome Critical Error!	March 2019	48
#40: '5G', Fifth Generation Cellular	February 2019	47
#39: Ten Tips	January 2019	46

[Go to Index](#)

Practicing Safe Computing by [Hal Bookbinder](#)
Index

Article	Published	Page
#38: Practicing Safe Tzedakah	December 2018	45
#37: Facebook 'Tokens'	November 2018	44
#36: iPhone Tips	October 2018	43
#35: Google Search Tips and Techniques	August/September 2018	42
#34: Urgent Demand for Payment	July 2018	41
#33: Best Anti-virus Protection of 2018	June 2018	40
#32: Microsoft Word Tips & Tricks	May 2018	39
#31: What is GEDCOM?	April 2018	37
#30: Precautions while Traveling	March 2018	36
#29: Meltdown and Spectre	February 2018	35
#28: Password Managers, again	January 2018	34
 #27: Take care when you use Google	 December 2017	 33
#26: What is the 'Dark Web'?	November 2017	32
#25: Top 10 Tips for Detecting Phishing	October 2017	30
#24: The Internet is forever	September 2017	29
#23: Phishing email from your Bank	August 2017	28
#22: Modems and Routers	July 2017	27
#21: Verizon 2017 Data Breach Report	June 2017	26
#20: Protection from WannaCry Ransomware	June 2017	25
#19: Malware Protection	May 2017	24
#18: Viruses, Worms, Trojan Horses, Spyware	April 2017	23
#17: Searchable Government Databases	March 2017	22
#16: Wireless Access	February 2017	21
#15: Yahoo again, Biggest Hack Ever!!!	January 2017	20

[Go to Index](#)

Practicing Safe Computing by [Hal Bookbinder](#)
Index

#14: Verifying What You See	December 2016	19
#13: Yahoo Email Services	November 2016	18
#12: Password Managers	October 2016	17
#11: Sharing Your Family Tree & Identity Theft	September 2016	16
#10: Passwords	August 2016	15
#09: Social Engineering	June 2016	14
#08: Avoiding becoming victim of Ransomware	May 2016	13
#07: Backing up your System	April 2016	12
#06: Is it true that Apples are safer than PCs?	March 2016	11
#05: What are 'cookies' and should they concern you?	February 2016	10
#04: Is Your Virus Protection Actually Working?	January 2016	9
 #03: A Free Scan of Your Computer	 December 2015	 8
#02: Credit reporting agencies	November 2015	7
#01: Don't help them steal your identity	October 2015	6

[Go to Index](#)

#1: Don't help them steal your identity

Originally published in the October 2015 issue of *Venturing into our Past* (JGSCV)

You receive an email letting you know that your information may have been part of a recent breach of health records. The email looks official with the familiar logo of a hospital that has treated you. It expresses sincere apologies and is signed by the CEO of the hospital. It asks you to click on a link to find out more about what the hospital will do to protect you from identity theft.

When you click on the link you see a screen with the hospital's logo that lets you know that they will pay for credit monitoring service for the next 2 years at no cost to you. You can decline and take your chances or accept the free offer. It seems like a no-brainer and you are relieved that the hospital is taking the breach and your financial protection seriously.

You click on the "I accept" button and a form is displayed to initiate the coverage. You are asked for your full name, mailing address, phone, email, date of birth, etc. You are a bit concerned however when you see that you are also asked for your social security number and a major credit card. When you click on the question mark by these fields, an explanation is displayed that makes sense.

You enter the data and confirm its accuracy. The screen provides you with a reference number for your free policy and a phone number to call if you have any questions. Surprise, you have been "phished" and your data is on its way to a third world country where it will be sold to con artists who may use it to steal your identity, purchase big ticket items on your credit or obtain Federal tax refunds in your name.

Never provide personal information when contacted unexpectedly, no matter how legitimate and logical the request seems; do not even provide basic information like your address and phone number. Rather, close the email and if you are concerned contact the hospital (or bank or insurance company) directly. You will likely find out that they never sent the email.

Institutions may well send you email about an issue. However, when an unsolicited email asks for personal information, this is a warning that you are at risk. These scams rely on the headlines of the day. Today's headlines tell of huge data breaches. So, when you get an email about this, it seems legitimate. These criminals know what they are doing. Always remain on your guard.

If you have been phished, take immediate action. Close credit or debit cards or bank accounts whose information you provided and contact the three main credit-reporting agencies to place a fraud alert on your accounts. These are minimum actions, do your research to see what other steps you should take. Yes, it is a hassle, but nothing like the hassle if your identity is compromised.

#2: Credit reporting agencies

Originally published in the November 2015 issue of *Venturing into our Past* (JGSCV)

My October “Safe Computing” article suggested you contact the credit reporting agencies if you have been “phished” and feel that your identity may have been compromised. This article covers how to do this and what you might request.

There are three major credit-reporting agencies in the U.S. - TransUnion, Experian and Equifax. By law, you are entitled to one free credit report from every year. To get your free credit report, go to www.annualcreditreport.com. You will be quizzed to ensure your identity. For example, you might be asked the amount of your monthly mortgage or car payment and be given a number of ranges.

You can obtain any or all of your three credit reports. While there are some differences, for the most part they are redundant. Therefore, what I do is put a reminder on my calendar at four-month intervals to get one of the three credit reports, keeping me aware throughout the year. Check the report carefully for accuracy. It will provide you with instructions for contesting erroneous information.

There are commercial sites, with the words “free” in them that look a lot like the official free site above. Using some will start a monthly charge while others are truly free and rely on up selling you additional services. If you do sign up for a credit monitoring service, be sure you know what you are getting for your money. In addition, check your credit card statements carefully for any resultant charges.

If you are concerned that your identity may have been compromised, consider establishing a “security freeze” with each of the three credit reporting agencies. With a credit freeze, the agency will not approve credit, loans and services being approved in your name without your consent. However, this may delay, interfere with or even prohibit the timely approval of legitimate requests for new credit.

The nominal fee for a security freeze is typically waived if you are over 65 or have submitted a complaint with a law enforcement agency stating that you believe you are a victim of identity theft. You can later temporarily, or even permanently, suspend the security freeze. Again, a nominal fee is typically waived if you have an active complaint.

A less intrusive alternative is a “fraud alert”. This requests that the potential credit grantor verify your identification before proceeding with the transaction. A fraud alert is free and lasts 90 days. If you request a fraud alert of any of the three companies, they are required to notify the other two. (However, I would verify that the others have recorded the alert). A fraud alert can be renewed for 90 days. It can be extended to one or seven years if you have submitted a complaint to a law enforcement agency.

Contact Information for the Credit Reporting Companies:

TransUnion, <http://www.transunion.com>, 1-800-680-7289,
Experian, <http://www.experian.com>, 1- 888-397-3742,
Equifax, <http://www.equifax.com>, 1-888-766-0008

To obtain your free annual credit report:

<https://www.annualcreditreport.com>

For more information:

<http://www.consumer.ftc.gov/articles/0155-free-credit-reports>

<http://www.federalreserve.gov/creditreports>

<https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#3: A Free Scan of Your Computer

Originally published in the December 2015 issue of *Venturing into our Past* (JGSCV)

You are surfing the web when a screen pops up telling you that you have 23,179 instances of malware (or viruses or worms) or porn on your computer. It offers to scan your computer and remove these at a low cost or even for free. Never take these people up on their offer to protect you through a one-time cleaning of your computer. They are great at scaring you. Do not take the bait.

The pop-up has no idea how many instances of bad stuff you have on your computer (though it is a pretty good bet that even with anti-virus software, you have some). If you give the soliciting message the authority to scan or to fix the problem you are giving them control of your computer. In addition, you have no idea what they will actually do with that authority. One thing for sure, it will benefit them and not you.

In a similar scam, the pop up informs you that you are infected with some specific virus (often one that you have recently read about in the news). This message is likely being spammed to hundreds of thousands of others expecting that some percentage will pay to be “cleaned.” If you pay, at best there will be a faux cleanup letting you know that everything is now Ok.

At worst, the spammer, once given control of your computer will install new viruses, steal your information, or even freeze your computer with ransomware (a topic for another article). The company name displayed often mimics well-known and trusted brands. However, these trusted companies do not operate in this way. If you give these con artists control, nothing good will come of it.

If the message scares you, this is not all bad. You should be concerned to keep your computer free of malware. Close the message without responding. Do not click on the box in the popup asking to be taken off the contact list. This just confirms to the spammer that you are real and you will result in even more spam.

Allay your concerns by running your antivirus software to check the current state of your computer. If your virus protection is out of date, get a current subscription. Consider going to a trusted site (like www.microsoft.com or www.mcafee.com) and see what tools they offer to check the health of your computer. However, under no circumstances give control to strangers who, unsolicited, reach out to you.

Similarly, do not fall for emails that you receive offering free or low-cost scans and cleanup of your computer. Again, you really do not know with whom you are dealing. Do not accept the offer no matter how tempting, scary, or trustworthy it seems. In addition, as before, never click on the request to receive no further emails. This will instead result in you being placed on even more spammers’ lists.

#4: Is Your Virus Protection Actually Working?

Originally published in the January 2016 issue of *Venturing into our Past* (JGSCV)

We all know the importance of maintaining virus protection on our computers, but many do not realize that their virus protection is not protecting them at all. Virus protection consists of two equally critical components. One is an engine that runs regularly to scan your files and messages for signs of malware and to then block or clean the malware that is found.

The second component is a list of current malware patterns. Without this, your anti-virus engine may continue to run and to protect your computer against the malware that was known in the past, but may not recognize the latest patterns and so let them slip by. You must maintain your subscription or the updating of patterns will cease, even as the engine continues to function.

Folks are sometimes fooled in that they see that the anti-virus product that came free with their computer continues to run long after its initial period has ended. They ignore the messages encouraging them to make a subscription payment figuring that they will handle this later, and the product seems to be working.

Some think that going for a time without virus protection is no big deal. They can always purchase an even better product later. However, as the days drag into weeks and then months the computer continues at risk and the malware multiplies. Additionally, some of this malware can burrow so deeply into the system that removal without a complete and expensive rebuild becomes impossible.

While your friends may prefer one product to another, all of well-known commercial products work well. The critical thing is to ensure that you have some product installed and that its list of patterns is being kept up to date. If not sure, go to the website of the product, you have and it will certainly offer to run a scan to tell you if you are up to date and running properly or at risk.

Sometimes software installation instructions instruct you to temporarily turn off your virus protection. Unfortunately, people sometimes neglect to turn it back on and so are running at substantial risk. Your virus protection should be set to scan all incoming messages, periodically check your entire system, and regularly download the latest malware patterns. If unsure, use the default settings.

Two virus-protection programs are not better than one. Each will perceive the other to be doing something that warrants monitoring. This conflict may actually slow your computer as each continues to confirm that the other is not, in fact, malware. So, if you decide to switch to another anti-virus program, uninstall the old one and then immediately install the replacement.

One anti-virus product, PC-Matic, touts that it is American made and uses “white-listing” to better protect you from visiting dangerous websites. While I like both concepts, I do not endorse this or any product. I just encourage you to spend the \$15-\$30 per year and stay current. This is far better than losing valuable data and paying \$300-\$400 to reinstall your system.

#5: What are 'cookies' and should they concern you?

Originally published in the February 2016 issue of *Venturing into our Past* (JGSCV)

While baked cookies can add on the pounds, computer cookies are so light that you can have hundreds or thousands of them on your computer and they will not slow it down. Cookies are small files of data that are used to facilitate your use of the Internet. They are not inherently bad. You can set your security settings to disallow them, but you will not like the results, as you will find that you cannot access many sites that require cookies to be enabled. You can set your system to purge cookies each time you close your browser or simply let them accumulate.

Cookies provide “persistence” which allows you to stay logged into a website. When you log in to a site, a handshake value is placed in a cookie file on your computer that is specific to that website. Each time you then send a transaction to that website (an update or query), the transaction grabs this handshake and includes it, thus confirming who you are and that you are indeed still logged in.

Cookies can contain preferences to personalize your experience for a specific website. Therefore, if you identify topics of interest and these are displayed when you go to the site, this is because your preferences are stored in a cookie and sent to the website when you access it. If you identify at a brokerage site which page is to be initially displayed, this information is similarly stored in a cookie. Cookies are unique to a single website and generally only useable when linked to that website.

A potentially dangerous use of cookies is to use them to store your login information, including your password, for a particular site on the Internet. You have certainly been asked if you “want to be remembered from this computer” and so speed your login. If you accept this offer, your ID and possibly your password are stored in a cookie that is then queried when you later access the site.

Even though the information is encrypted (i.e., scrambled so that it cannot be easily read), it could be used by someone who gains access to your computer to log into sites with your credentials. Malware could even use or export them. As I would prefer to leave no opportunity for another to log into my brokerage account, bank or credit union and take actions in my name I routinely decline to accept offers by websites to remember me.

Deleting cookies will not harm your computer. However, this will remove the website “personalizations” you have constructed over time. You can instruct your computer to delete all cookies each time you close your Internet browser, except those related to selected “favorite” sites. This is precisely the way I have set up my Internet Explorer, Chrome and Firefox browsers.

For specific instructions for your setting cookie rules for your browser, search for “Managing cookies in Firefox 40.0.3” using the actual name and version of your browser. To find the version of Firefox you are using, click on three bars symbol in the upper right-hand corner of the page, then click on (?) and then “About Firefox”. For Chrome, click on the three bars symbol, then “Help and About” and then “About Google Chrome”. For Internet Explorer, click on the Tools icon (looks like a gear), and then “About Internet Explorer”.

#6: Is it true that Apples are safer than PCs?

Originally published in the March 2016 issue of *Venturing into our Past* (JGSCV)

Yes, it is true. Apples IOS operating system has proven to be less impacted by viruses than PCs running any version of Windows. The reason is two-fold. First, with about 7.2% of the market for desktop and laptop computers vs. 91.4% for Windows based PCs, virus creators find it more attractive to write malware for PCs (the remaining 1.4% of personal computers use a variant of the Linux operating system).

The second reason relates to the way Apple updates its operating system vs. the way Microsoft updates Windows. Microsoft does its best to provide for backward compatibility. In other words, they want to see that programs that ran on earlier versions of the operating system continue to run. This translates into lots of old code being included in current Windows operating systems.

With about 50 million lines of code, much of it carried forward, there are many opportunities for mischief as hackers discover flaws in the software that they then exploit through malware. When this occurs, Microsoft releases a security patch to close the flaw and the anti-virus companies release an update to counter it. However, they are always playing catch up and there is an inevitable lag.

When Apple releases a major operating system upgrade, it is built fresh. If older software will not run, so be it. Apple is more focused on the overall user experience with its current operating system and associated software rather than compatibility with older versions. So, as an Apple user you may find that you have to buy a new version of software when upgrading to the newest operating system.

By writing new code, Apple can concentrate on protections and the user experience and does not have to contend with protecting old operating system code. While Apple does a good job in controlling viruses endangering the Apple system, it does not do as much regarding viruses and worms simply using the Apple as a landing place on their way to a Windows PC.

Apple users remain at risk for phishing in which unscrupulous folks strive to obtain personal data. Therefore, Apple users still need to be on their guard. Half a dozen companies provide Apple-specific anti-virus software. While the risk is lower, Apple users owe it to themselves (and the PC users with whom they interact) to acquire and run anti-virus software on their machines.

As PC Magazine wrote on February 13, 2015, "Mac users simply cannot be complacent and leave their machines unprotected. Even if they never encounter malware, they would certainly benefit from social media protections and keeping their machines from being used to attack other computers. And with numerous free options, there's simply no excuse; get antivirus protection for your mac today." - [11 Antivirus Apps for Mac](#).

#7: Backing up your System

Originally published in the April 2016 issue of *Venturing into our Past* (JGSCV)

We all know that we should be regularly backing up our data. However, the fact is that many of us do not back up our data frequently enough, if at all. Some think it is complicated or expensive and many have become complacent after years of using computers without problems. Do not wait for a data loss to shake this complacency.

We all need to frequently back up our data and store these backups in a different location from the computer on which it normally resides. Many purchase an external hard drive and set it up so that automatic backups are taken daily. This is good as far as it goes. However, what happens in a disaster where there is a fire, flood, or earthquake and both the computer and its local backup are destroyed?

This can be avoided by using one of the available commercial services through which your data is automatically backed up to the cloud. These services are relatively inexpensive. Alternatively, you could set up a cloud backup yourself by placing a cloud storage device at another location and backing up to it using software that performs regular backups, daily or more frequently.

Recognize that backing up everything on your computer is not necessary. The Operating Systems and computer software can be re-installed. Downloaded music and movies can be re-downloaded. However, your own pictures, family information, research, financials and more should be backed up off site.

Consider setting up a logical drive or directory on your computer dedicated to the data that is to be backed up. You can routinely copy the contents of this drive or directory onto a USB “thumb” drive and keep it on your key chain as I do. So, I have my data wherever I happen to be, whether or not I have Internet access.

This is not a substitute for regular, scheduled backups, but an additional step you may consider. If you have a particularly important file that you have just created and cannot afford to lose, you could copy it to the thumb drive or attach it to an email and send it from your home to office or vice-versa.

Most of us have experienced that horrible feeling when our computer loses power after we have put a great deal of time into creating or updating a file and just before we were going to save it. To avoid this, set your system to regularly save your files as you update them. Consider setting this to occur every five or ten minutes. Additionally, consider taking a backup of any critical file before you start modifying them.

Another approach is to keep your data in the cloud. These cloud services routinely back up your data for you. However, as I never like leaving anything to chance, I would want to have two physical backups under my own control as well, in two different physical locations. If I sound paranoid, I am a little. Once you experience a painful data loss, you may become a bit paranoid as well.

#8: Avoiding becoming victim of Ransomware

Originally published in the May 2016 issue of *Venturing into our Past* (JGSCV)

Ransomware is a form of malware that encrypts files on your computer and then demands payment in exchange for the passkey to access them.

In February, Hollywood Presbyterian Medical Center became the victim of a ransomware attack. Cybercriminals took control of the hospital's computers and encrypted data so that the hospital could not access or record patient notes. The cybercriminals demanded a payment to provide the hospital with the necessary passkey to unlock its files. The hospital paid \$17,000 in bit coins, an untraceable way to pay the cybercriminals who likely accomplished this attack from a country with weak extradition treaties. The cybercriminals provided the passkey and Hollywood Presbyterian was back in business. They insist that no patient was at risk during the episode. However, they redirected emergency patients to other hospitals while dealing with the attack.

Cybercriminals target individuals as well as institutions. Playing the numbers, they likely make more money at \$200 to \$400 per attack against individuals who tend to focus less on protecting their systems than institutions. Most people will readily fork over a few hundred dollars to regain control of their system and data. When the cybercriminals take control, they display a warning screen letting you know you have been hacked and instructing you to purchase bitcoins or a cash card and then go to a site on the untraceable "dark web" to make your payment. The passkey to unlock your data is then provided. The cybercriminals want to maintain their reputation for honesty after the payment is made.

"Locky" is the nickname of one strain of ransomware. It encrypts and then renames all your important files so that they have the extension .locky. It generally arrives as an email attachment. When you open the attachment, it appears scrambled and you are instructed to "enable macros" to unscramble the message. In actuality, this will run code to implant the ransomware on your computer. "Jigsaw" is another new ransomware program that actually starts destroying files if you delay in obtaining the bitcoins to pay off the cybercriminals. It displays a countdown clock on your screen to let you know that you have one hour to make the payment and if late, you will not get back all of your data files.

To protect yourself:

- Be cautious about unsolicited attachments. If in doubt, do not open it.
- Avoid going to sites on the Internet that you do not know to be safe.
- Do not enable macros in document attachments received via email.
- Consider installing the Microsoft Office viewers. They let you see what documents look like without opening them in Word or Excel and do not permit macros.
- Maintain current virus protection and automatically download security patches for your various programs (like Office, Flash and Chrome).

Finally, backup regularly and keep a recent copy off-site. You will then have the unhappy choice of paying the cybercriminals for the passkey or paying your computer support person to reinstall your system and files. Such is life in the cyber age!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#9: Social Engineering

Originally published in the June 2016 issue of *Venturing into our Past* (JGSCV)

Ever notice that when a big headline hits the news you get emails on the topic? This is a typical way social engineers get through your defenses. Prince suddenly died this past April. The news, the blogs, television and radio contained almost non-stop coverage of the tragic event, speculating on the cause of his death and extolling his memory. You likely received at least a few emails on the event.

Since the story was all over the place, we tend to be less suspicious of an email on it. Therefore, if you are into pop music, or just a news junkie, you may have opened the email without thinking whether it might contain a virus. You might have even clicked on the button in the email to play a commemorative Prince tune. Social engineers recognize that folks let their guard down in such circumstances.

However, you feel that this will never happen to you because you would just delete such a message. After all, you are not into such pop music culture and know not to open emails from sources you do not know. Ok. Now substitute a recent bus bombing in Israel or the latest outrageous thing that Donald Trump said or (and I love this one) an email about the latest scam in the news.

Social engineers use topical news to send out viruses to infect your computer and possibly steal your personal information. So, maintain your guard when you receive emails on the latest headline. If you do not recognize the source, be wary about opening the email. In addition, never, never, click on any link or button contained in the email. You will be inviting viruses to come aboard your computer.

When you get a call from Citibank informing you that they have a thieving teller who has been inappropriately accessing customers' accounts and that they need your help to trap her, be wary. They may even offer you an award if you help provide evidence. Of course, they will need some information from you. The person is friendly and seems sincere and very believable, which is typical of a good social engineer. You want to help, and the \$500 reward does not hurt.

You think that you would never be fooled by such a call. You know it is likely a scam. However, when it occurs, you may not be thinking as clearly. In addition, the caller seems so nice, friendly and believable. Enough people fall for such approaches to provide the social engineer with a regular stream of stolen identities and cash. Never be tricked into giving out personal information when you are contacted by phone, email, instant messenger or at your door.

Additionally, older people tend to be more trusting. Possibly, it is because we grew up in a different age. Whatever the reason, do not let yourself be fooled into sharing your personal information, opening emails or linking to websites when contacted by social engineers who rely on our good nature, greed, curiosity, trust and desire to be helpful.

[Go to Index](#)

#10: Passwords

Originally published in the August 2016 issue of *Venturing into our Past* (JGSCV)

We all know that we should be careful about selecting, protecting and changing passwords. However, how can you do this when you are told to maintain different passwords for your various websites, that they must be long and complicated, that you should not write them down and you should change them frequently? Impossible! Right? While this may be an annoying challenge, it is not nearly as bad as suffering an attack in which your accounts are emptied or critical personal information is stolen.

Passwords should not include any information that could be found about you. You mention that “blue” is your favorite color on Facebook. Your bio says you were born in the “Bronx”. You occasionally mention your dog “Scooby” in emails. These bits of information provide a great start in guessing your password. Do not use family names, pet names, towns or streets where you now or have ever lived, phone numbers or favorite colors, foods, songs, movies or drinks. Simply putting a “1” at the end will not help. Hackers will use automation to try all these things and will add digits and special characters.

Do not use simple sequences like “ABCD”, “4321”, “1111”, “1a2b3c4d”, or “1234ABCD”. Do not use “QWERTY”, “14789” or any other simple string of characters from your keyboard or phone keypad. If it is simple to remember, it is simple for the hacker to crack. The hacker’s automated tool will attempt all of these predictable sequences.

The best passwords are random collections of upper- and lower-case letters, numbers and special characters. However, these are generally impossible to remember. Therefore, your best bet is to choose a couple of unrelated words and combine them, with a digit or two and a special character or two. So, say you choose “Home” and “Spring” and make the password “Home4Spring5!” or the slightly more complicated, “HoMe4SpRiNg5!”.

Realistically, if you have a half dozen or more of these you will have a hard time remembering them. However, if you write them down, this list could fall into the wrong hands. I record them in a password-protected file on my encrypted computer. I just have to remember one complex password, the one to open this file.

This is a low-tech version of a password wallet - an online tool that keeps all of your passwords and provides them as needed directly when needed. Better wallets will even generate new complex passwords as required. Then, you could have a hundred complex passwords, all different. You will need to remember just one password, the one to authorize and access your password wallet.

While you can pay for an encrypted USB stick or a software-based password wallet, there are excellent free services as well. One is “dashlane.com”. However, you still have the challenge of remembering that one complex password to get into your password wallet. Ok, write it down, just in case you forget, and store it in a safe place, like your safe deposit box - and not on the back of a business card in your wallet!

#11: Sharing Your Family Tree & Identity Theft

Originally published in the September 2016 issue of *Venturing into our Past* (JGSCV)

Some choose not to share their family trees out of concern about identity theft. Your tree does contain personal data of interest to identity thieves such as birth date and place, address, phone number, email and mother's maiden name. However, it does not contain the information they most want including social security number, credit card, bank account and investment account numbers and passwords.

At the recent IAJGS conference, Randy Schoenberg stated that there are "zero instances of identity theft resulting from shared family trees." He further stated that family members perpetrate the majority of identity theft. While it would surprise me if there were truly no instances of identity theft related to the sharing of family trees, a quick Internet search did not turn up much.

According to Bruce Kennedy in CBS Moneywatch, "Numbers vary, but a study quoted by credit information firm Transunion revealed that nearly one-third of identity theft victims later determined that a family member or relative was responsible for the crime."

Posting your family tree can vastly increase it as you link up with others and identify possible relatives about whom you knew little or nothing. There is simply no better way to expand your tree than through the cooperative effort of others, some whom you may not yet know.

You may find some or all your tree already posted by others and this may contain incorrect or private information. You may also see information on living relatives. Some sites suppress such information, others permit it. There is no legal obligation to hide such information. While this may disturb you, you have little legal right to force its removal.

Before you upload your tree, read the "terms of use" for the site. You may find that by uploading your data, you are "contributing" it and the company has ongoing rights to its use, even if you no longer want it exposed. Check on what privacy is offered and what rights you have. You may not like what you find. However, you may conclude that the tradeoff is something with which you can live. Identity thieves have other ways to get the personal information they need. They do not need access to your family trees.

To lessen the likelihood of identity theft, use and regularly change complex passwords, password-protect the logon to your home computer, log off when you walk away, do not provide other users "administrator" rights, shred your paid utility bills and carefully review all credit card and bank statements. Take note if you do not receive an expected statement, periodically review your credit report and consider tightening the rules pertaining to getting credit under your name with the credit agencies. All of these steps were discussed in prior articles in this series.

There are legitimate reasons for not sharing your family trees. However, there are more important steps to take to protect yourself from identity theft.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#12: Password Managers

Originally published in the October 2016 issue of *Venturing into our Past* (JGSCV)

Password managers store your login information for the sites that you visit. They then automatically log you in to the site once you bring up the login page. Better password managers will generate unique complex passwords for you, fill in forms and synchronize across your devices. Some even provide legacy features to pass on your access to another, so that if you become incapacitated or die, someone will be able to access your accounts.

I tried the free version of one of the very best password managers, Dashlane 4. It did a great job in automatically capturing IDs and passwords as I logged into websites and then replayed them when I went to those sites again. However, it was constantly pushing me to purchase the commercial version that was required for important functions like being able to view, update, delete or synchronize passwords across various devices. Eventually, I uninstalled it and focused on the free password managers.

An excellent free password manager is LastPass 4.0. It is intuitive, providing “cards” for each website you wish to access and displaying them in logical folders. You enter a description, ID and password into each card. I set up separate folders for financial sites, frequent flyer sites, genealogy sites, email sites, retail sites and social sites. I then simply clicked on the card for the site that I wished to open and LastPass logged me in.

LastPass presumes sites have a single ID and single password to log in. You may have to enter some fields for sites that do not fit this profile. For example, the American Airlines’ Frequent Flyer site requires an ID, a last name and a password. LastPass entered the ID in both of the first two fields requiring me to overtype my last name - a minor annoyance.

Some sites do not permit you to go directly to a login page but rather have an icon on the home page that displays the login function. In these cases, clicking on the LastPass card icon brings up the home page. You must then click on the login icon and then have LastPass fill in the required information. Some of the commercial tools are more sophisticated and include unique profiles for hundreds of sites.

LastPass also generates complex passwords on request that you can use to better protect yourself. This is especially for important sites. Download it from <http://www.lastpass.com>. Please do your own investigation to select the right tool for you.

Commercial password managers cost \$20 to \$40 per year. For excellent comparisons of these tools, see “The Best Password Managers of 2016” (<http://www.pcmag.com/article2/0,2817,2407168,00.asp>) and “The Best Free Password Managers of 2016” (<http://www.pcmag.com/article2/0,2817,2475964,00.asp>).

A password manager is a convenient, secure way to maintain different passwords for the various sites that you visit. Of course, you must create and remember a password for your password manager. Consider recording it in a secure location, like your safe deposit box - just in case.

[Go to Index](#)

#13: Yahoo Email Services

Originally published in the November 2016 issue of *Venturing into our Past* (JGSCV)

You are all likely aware of the mass theft of user data from Yahoo in which information for over 600 million customers was stolen in 2014, becoming known only in the last few months. (If you have a Yahoo account and have not changed your password since 2014, do so immediately. If you use the same password on other accounts, change them as well.)

Yahoo is reeling and playing defense in trying to retain its business. The LA Times reported in its October 11, 2016 edition that Yahoo has quietly shut down the ability of users to turn on mail-forwarding services. According to the article, Yahoo claims that this is temporary while they “improve” the service. This standard function permits you to receive email in one mailbox and immediately forward a copy to another. It permits you to consolidate all email into one mailbox.

I have email accounts in Gmail, Yahoo, MSN, UOP (University of Phoenix), UCLA Bruin and Roadrunner (Times Warner Cable) and consolidate them all into my primary UCLA Medical Center account. Therefore, if you send an email to me at hal@jgscv.org or hal.bookbinder@ucla.edu, you will likely get a response from hbookbinder@mednet.ucla.edu. This is the account that I monitor.

Along with consolidating email, forwarding is also used to facilitate moving from one email service to another and Yahoo clearly does not want to help you do this. Once you set up a new email service, by setting up forwarding, email from those who use your old email automatically shows up in your new mailbox. By using an “out of office” notification in your old mailbox, you can let them know that this mailbox will shortly close. Alternatively, you can just notify those you want to be aware of the change.

You then can opt to close your old email or not. If you close it, those who use it will get a message that it is not a valid address. If you leave it active but simply stop using it, emailers, including spammers, will have no awareness that it is now dead. Some family or friends may wonder why you are ignoring them.

If you had forwarding turned on in your Yahoo email before they took this action, the Times reports that it should still work. Yahoo simply turned off the ability to invoke this feature. This is presumably a defensive move to make it more difficult to move away from Yahoo. Likely, the blowback they will get will result in Yahoo restoring the function. With their mass-hacking, bleeding money (reported loss of \$5.19 per share as of 7/18) and anti-customer actions such as these, one might question whether to remain with Yahoo it all.

Of course, there are issues with other email services as well. Many are concerned about the scanning of emails reportedly done by Gmail and what other free services are doing with your information. Email has become a lifeline. Pay attention to your email service and have an escape plan.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#14: Verifying What You See

Originally published in the December 2016 issue of *Venturing into our Past* (JGSCV)

We all receive emails from friends passing on the latest information that they got from the Internet. It sounds plausible, you trust your friend and so you pass it on to more friends, or worse yet, act on the information without checking it first.

In February 2016, folks were receiving advice to reset their iPhone date manually to January 1, 1970. Various reasons were given which sounded compelling. Yet, doing so would result in permanently disabling your iPhone. Apple acknowledged this bug and fixed it in iOS 9.3.1 in April. I am not brave enough to check it out myself on my iPhone. DO NOT TRY IT!

Another item that periodically circulates is a notification that you may be infected and to check your computer for a particular file or value to confirm this. It then advises that you should immediately take an action, like deleting a particular file or running a script from a particular website. The file or value indicated is a normal component and removing that file may cripple your PC. Be assured that the script, should you choose to run it, will be infecting or otherwise damaging your PC.

Be careful about acting on, or passing on, information you get on the Internet, whether through searching websites, emails out of the blue, or emails from trusted friends. Much of what is passed around is completely false or plausible sounding half-truth. Taking action without checking it out may cause you real damage. Sending it to friends may just spread a falsehood, or worse, a virus.

If you get an unsolicited advisory regarding your financial institution log directly into their website (DO NOT CLICK THE LINK IN THE EMAIL) to check it out. If you get an advisory related to Microsoft, Dell, Apple, Intuit or whatever, similarly check it out before taking action. Links in emails may bring you to a page that looks legitimate, but is not. If you attempt to log in, you may be giving your log in information to folks who may use it fraudulently. Subsequent challenge questions may be used to obtain even more information.

Two websites that have a good reputation for investigating and debunking Internet nonsense are www.snopes.com and www.truthorfiction.com. The descriptions below come from Wikipedia.

"Snopes.com, also known as the Urban Legends Reference Pages, is a website covering urban legends, Internet rumors, e-mail forwards, and other stories of unknown or questionable origin.] It is a well-known resource for validating and debunking such stories in American popular culture, receiving 300,000 visits a day."

"TruthOrFiction.com (or TruthOrFiction.org) is a "myth busting" website about urban legends, Internet rumors, e-mail forwards, and other stories of unknown or questionable origin. The topics are researched by TruthOrFiction's staff, and rated "Truth" (if true), or "Fiction" (if untrue). When the accuracy is not known with certainty, the stories are rated "Unproven," "Disputed," "Reported to be Truth" or "Reported to be Fiction." Partially true stories are rated "Truth & Fiction."

#15: Yahoo again, Biggest Hack Ever!!!

Originally published in the January 2017 issue of *Venturing into our Past* (JGSCV)

In mid-December, Yahoo announced that they had discovered another hack in which 1,000,000,000 (one billion) accounts were compromised. The hack occurred in 2013 and so the hackers have had three years to exploit the information. This is twice the size of the hack that they announced just a few months ago (see article in November 2016 newsletter).

In addition to IDs and passwords, the hackers retrieved challenge questions answers (like, “What is your mother’s maiden name?”). People tend to use the same password and/or challenge questions on their accounts. With the information from Yahoo, hackers can use programs that generate various combinations until they are able to access your other accounts. Challenge question answers may also be discoverable or guessable – especially if they are true.

While Yahoo claims that the breach did not include financial information, identifying your bank and other financial institutions is relatively easy using services available on the Internet. Alternatively, the hackers can simply try to access your accounts at a series of financial institutions until they find the one that works.

Previous articles have provided recommendations to secure your account access. However, they did not address the issue of challenge questions being compromised. Here are steps you should take:

- 1) Have different, complex, passwords for each of your accounts, especially ones that are sensitive, like financial and medical sites. (August, 2016)
- 2) Use a password manager to generate your complex passwords. I use LastPass. Complex passwords that you build yourself may still be able to be guessed. (October, 2016)
- 3) Store all of your login information in a password manager secured with its own complex password which you will need to remember. (October, 2016)
- 4) Keep a copy of the password to your password manager in a safe place, possibly your safe deposit box and definitely not on a slip of paper in your wallet! (October, 2016)
- 5) Set up your challenge questions with false and varied answers. Consistent, accurate challenge answers are discoverable. But, how can you now remember them? (new)
- 6) Record the challenge questions and answers in the notes area associated with each login in your password manager. (LastPass provides a visual “card” for each account). (new)
- 7) Change your passwords periodically - every 90 days is a good rule. (October, 2016)
- 8) Never click on an email link to what you think is your account. It may take you to a simulated page that simply captures your login information. Type the address yourself. (October, 2015)
- 9) Be careful when sharing personal information and never share login information. (June, 2016)
- 10) Immediately change your password if you suspect your password may have been compromised. (August, 2016)

The Yahoo breaches were not discovered for three years. So, do not wait for an announcement that your account may have been compromised. Take action now!

Think it is too much trouble to take these steps? Compare it to the trouble if your financial, medical or even social accounts are hacked. At a minimum, secure your most critical accounts.

[Go to Index](#)

#16: Wireless Access

Originally published in the February 2017 issue of *Venturing into our Past* (JGSCV)

You have a wireless router so that you can connect from anywhere in your home. Be aware of the exposures that come with wireless. Some of us retain the standard settings (ID and password) on the router. Anyone can easily find out the standard settings for your Linksys, Asus or other brand of router. This ID and password permits them to log into your router and update its settings.

Once someone logs in, they can then use this information to hijack your router, eat up your bandwidth or even intercept your traffic. Your wireless access does not stop at the walls of your house but can be accessed by your neighbors and by folks on the street. So, take the obvious first step and change the ID and password on your router. In addition, make it one that is not easy to guess. I routinely find folks with the password of "password". Misplaced the paperwork on your wireless router? Just check the router manufacturers' website for instructions.

You need to also set a wireless password so that only the devices you want to be able to connect to your router are able to do so. If you do not, your neighbor or the fellow on the street may be sharing your bandwidth, slowing your access. So, be sure to set a wireless password as well as updating the router login ID and password. Once you set the wireless password, you will need to add it to your laptop, tablet and smart phone so they will be able to access your wireless network.

A second line of defense is to encrypt your network traffic. This way, even if someone is able to intercept your transmissions, they will have a difficult time unraveling it. When you connect to a secure website, it generally has "https://" at the beginning instead of "http://". Your bank will quickly take you to their "https://" entry point where your subsequent traffic will be encrypted. For example, if you type in "www.bankofamerica.com", you will be taken to "https://www.bankofamerica.com/".

Many email systems, including Gmail, encrypt your messages. When you next go to "www.gmail.com" notice that what is displayed is "https://mail.google.com/mail/#inbox". If you use another email service, look to see if it takes you to an encrypted website. If it does not, consider switching to one that does.

It is especially important that your transmissions be encrypted when you connect in an exposed, shared environment like Starbucks or the airport. Someone with the appropriate device may be intercepting the transmission and "listening in". If you cannot get an encrypted connection, be very careful what you share. You never know who is listening.

While we typically obtain a wireless router so we can access the Internet from anywhere in the house, be sure to read the guide that comes with it and you will see that there are other functions that you may want to consider - including setting up a firewall and locking down access to adult or dangerous sites. More about routers and firewalls in a future article.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#17: Searchable Government Databases

Originally published in the March 2017 issue of *Venturing into our Past* (JGSCV)

The articles in this series have focused on avoiding computing problems. This article shifts to some government resources that may help find people. We will get back to avoiding problems next month.

Government agencies maintain numerous interesting searchable databases. For example, the Office of Inspector General at the U.S. Department of Health & Human Services maintains a searchable database regarding individuals and entities currently excluded from participation in Medicare, Medicaid and all other Federal health care programs. As of February 2017, it contained 2,974 entities and 63,306 individuals. One can search by the first letter(s) of the entity name or surname (Entering the wildcard “%” retrieves everything).

Searching the Entity database for “Los Angeles” returned three hits. Here is the first entry:

Entity: LOS ANGELES DOCTORS HOSPITAL CORPORATION, General: OTHER BUSINESS, Specialty: HC CONGLOM – PARENT, Address: 2231 S WESTERN AVE, LOS ANGELES, CA 90018-0000, Excl. Type: 1128(a)(1)- PROGRAM-RELATED CONVICTION, Excl. Date: 06/14/2012

Searching the Individual database for “COHEN” returned 37 hits. The first one is:

First Name: ABBOTT, Middle Name: B, Last Name: COHEN, DOB: 12/25/1968, General: PODIATRY PRACTICE, Specialty: PODIATRY, Address: 105 PRENTISS, ALPENA, MI 49707-0000, Excl. Type: 1128(a)(4)- FELONY CONTROLLED SUBSTANCE CONVICTION, Excl. Date: 08/19/2004

You can use this database to check out individuals and entities about whom you might have a concern. You also might be able to find information on lost or potential relatives. Try it with the surnames you are researching. Access it at <https://oig.hhs.gov> and select the “Exclusions” tab. The first option is its Online Searchable Database. It also contains a helpful FAQ.

Various federal and state entities maintain publicly accessible staff directories. For the U.S. Department of Health & Human Services go to <http://directory.psc.gov/employee.htm>. It provides the specific organization for which the person works, his/her job title, location, phone and email.

If interested in seeing if an organization has a publicly accessible directory, enter “Staff Directory - DHS CA” (citing the specific agency you want). In this case, you will find a staff directory for the California Department of Health Services. Try it with federal, states or local agencies. Be creative. If your search does not work, try alternative wording like “phone directory” or “employee directory.”

The first several listed responses to such searches will often be commercial search facilities which themselves scour many publicly available databases for information on individuals...for a fee. They pay to be listed at the top. If you skip over them and look for URLs ending in “CA.GOV”, “NY.GOV” or just “GOV” you have gotten beyond the commercial sites. If you are interested in California governmental sites, include “CA.GOV” in your Google search.

Of course, not all government databases are free. For example, I was searching for a nurse and knew that each state maintains a registry of licensed nurses. In another search, I was trying to find someone based on mortgage information. A friend has a professional practice that subscribes to various licensure and property databases. Accessing these databases quickly located the individuals.

The scope and availability of governmental databases are more than you might imagine. Happy hunting!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#18: Viruses, Worms, Trojan Horses, Spyware

Originally published in the April 2017 issue of *Venturing into our Past* (JGSCV)

Malware (**malicious software**) comes in diverse forms. “Viruses”, “worms”, “Trojan horses”, “spyware”, “adware”, “zombies”, “ransomware” and “scareware” are different forms of malware. Some of these refer to the way the malware transports itself to your computer and others to what it does once you are infected.

There are two ways of transporting malware to your computer. You unknowingly invite “viruses” onto your computer and share them with others while “worms” find you on their own. They can be equally disruptive, from being petty annoyances to being highly destructive. The designation “virus” or “worm” describes how they travel and not their function or destructiveness.

Viruses may arrive on emails you open or websites you visit. Typically, a further action results in their installation, like clicking on a button or link on the website or in the email. Sometimes, the mere fact of visiting a dangerous website or opening an infected email is sufficient. Worms are routinely on the lookout for new hosts and once they find them, transport themselves to the unlucky target.

The rest of the terminology refers to the actions taken by the malware. Trojan Horses appear to be something benign or desirable. However, when you run them, they are also installing viruses on your computer. You receive a birthday card that instructs to click on it for a tune and sure enough when you do so it plays “Happy Birthday”. At the same time, it is installing a virus.

Spyware is a form of virus or worm that captures information on your computer and sends it to an outside recipient. This might include copying and sending your address book, your financial or medical information or IDs and passwords you may have stored in your computer. Some spyware records your keystrokes as you type, emailing them to the recipient. Adware invokes popup advertisements. Visiting websites might trigger these popup ads. A timer may also trigger them. Generally, adware is more annoying than dangerous.

Zombies, once installed in your computer, make your computer a “slave” to an outside “master”. They periodically check the remote site for instructions and take action when instructed to do so. Zombies may turn your computer into a relay for spam, forwarding a downloaded email to your contact list (seemingly coming from you) or to a list provided by the master. Alternatively, zombies can attack specified websites, with thousands of zombie computers overwhelming the target with simultaneous traffic. Since zombies are continually checking with their masters for instructions, they can slow your computer.

Ransomware encrypts your data and instructs you to pay a fee to regain control. The more aggressive forms of ransomware will threaten to, and then proceed to, destroy your data. Scareware, as the name implies will use social engineering techniques to instill fear, generally to cause you to buy unneeded software or services. Sometime it will attempt to scare you into taking potentially disruptive actions or running dangerous software.

#19: Malware protection

Originally published in the May 2017 issue of *Venturing into our Past* (JGSCV)

The April Practicing Safe Computing article described the various types of malware and mentioned that the designation “worm” and “virus” relate to the way the malware arrives in your computer. Viruses come in emails, or reside in websites or files you might access. To avoid them, you could avoid dangerous websites, avoid opening strange emails, avoid clicking of buttons that trigger programs to run and avoid accessing files on USB drives. Of course, if you religiously followed these rules, you would accomplish little on your computer.

Worms require no action to find you to implant their malware on your computer. They are constantly scanning for devices to which they can connect and once they discover a potential host, transport themselves to that host. They could be resident in a website you open or come to you from another infected device. The Stuxnet worm crippled Iran’s nuclear reactors for more than a year. It is likely that an Iranian scientist placed an infected USB flash drive into his PC. Stuxnet infected the PC and used it as a launching pad to transport itself to the computers controlling the centrifuges concentrating uranium.

Each device on the Internet broadcasts its address and availability so that others may see it. The downside is that this exposes a computer to worms. To lessen the risk, install a firewall between your computer and the Internet. The firewall broadcasts its address and availability (or none at all) and shields the address of your computer. Worms cannot see your computer through the firewall unless you provide a pathway by connecting to an infected website or inserting an infected USB drive. Be sure to turn on the built-in firewall on your computer or wireless router.

In addition to firewalls and being careful as to websites, emails and USB drives, you must have current anti-virus software on your computer. If you are not certain whether your anti-virus protection is up to date and configured properly, go to the vendor’s website and check. They have utilities to verify whether your software is functioning properly. If unsure, choose the default configuration.

An article by Neil Rubenking in the March 3, 2017 issue of PC Magazine evaluated 46 utilities to protect your Windows PC from malware. It lists the following ten as the best antivirus protection programs of 2017: McAfee AntiVirus Plus, Webroot SecureAnywhere Antivirus, Bitdefender Antivirus Plus 12017, Symantec Norton AntiVirus Basic, Kaspersky Anti-Virus (2017), Avast Pro Antivirus 2017, Emsisoft Anti-Malware 11.0, ESET NOD32 Antivirus 10, F-Secure Anti-Virus (2017) and Trend Micro Antivirus Security (2017).

The article contains a side-by-side comparison of functions and links to more in-depth reviews. Access it at: <http://www.pcmag.com/article2/0,2817,2372364,00.asp>. All these products function well. Pick one that you prefer and be sure to configure it to check all of the files, emails and websites you access. While most have higher “regular” prices, watch for sales and spend \$20 to \$40.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#20: Protection from WannaCry Ransomware

Originally published in the June 2017 issue of *Venturing into our Past* (JGSCV)

The WannaCry ransomware has been all over the news as it has infected hundreds of thousands of computers worldwide, impacting major institutions as well as individuals. While all of the information below is available online, I have not found it written in nontechnical terms in a single place. Hope you find this helpful.

What is the issue?

- The WannaCry (or WannaCrypt) ransomware exploits a vulnerability in all versions of the Windows Operating System (OS).
- Microsoft issued the following to explain this exploit, <http://tinyurl.com/me8rx8g>.
- The above bulletin contains a link to Microsoft Security Bulletin MS17-010, which includes the security patch to fix this vulnerability.

Do I need to worry?

- If your computer is running a supported version of the Windows OS (7, 8.1 or 10) AND is set to automatically accept security patches from Microsoft, you should be protected.
- If you are running Windows 10, automatic updates are turned on and cannot be turned off by the home user, so you should be protected.
- If you are running a supported version but it is not set to automatically accept security patches, you are at risk.
- If you are running a non-supported version Windows OS (8.0, XP or earlier), you are at risk.

What if I do not know which version of Windows I am running?

- A quick facility to check what Windows OS you are running is <http://tinyurl.com/zmk89k4> (this is not a Microsoft site). It will display your OS at the top of the page and give you instructions if you want more details.
- Alternatively, you can find instructions at <http://tinyurl.com/hd645o6>. Though not quite as convenient and only covering supported versions, this is a Microsoft site.
- What if I am running Windows 7 or 8.1 and do not know if automatic updating is turned on?
- For instructions, see the following Microsoft publication, <http://tinyurl.com/z6t342p>. Go down to the portion entitled "Turn on and use Automatic Updates".
- If you find that you do not have automatic updating turned on, you are strongly advised to turn it on.

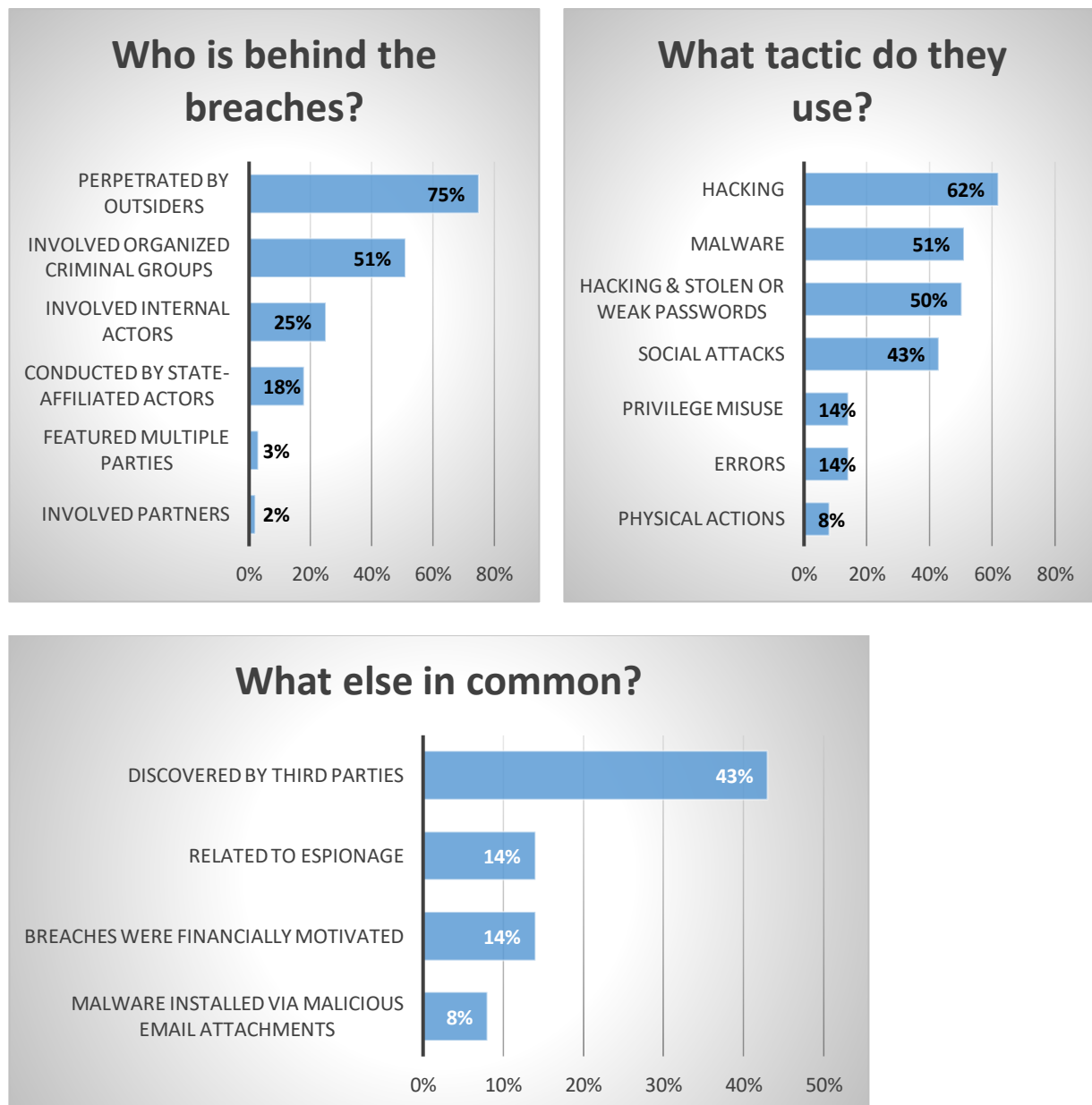
What do I do if I am at risk?

- The Microsoft bulletin cited in the first section, <http://tinyurl.com/me8rx8g>, contains links to download the MS17-010 patch
- In a highly unusual move, Microsoft has issued security patches for several unsupported Windows versions, including XP and 8.0, which are otherwise not supported with any fixes. Microsoft also offers a patch for Windows Server 2003. However, this is primarily a business installation and it is highly unlikely you have it on your home computer. Links to these downloads are at the bottom of the bulletin.
- If you are running an earlier version of Windows, no fix is available from Microsoft.
- If you are on an unsupported version of Windows, it is highly recommended that you upgrade.

[Go to Index](#)

#21: Verizon 2017 Data Breach Report
Originally published in the June 2017 issue of *Venturing into our Past* (JGSCV)

For the past 10 years, Verizon has issued an annual Data Breach Report. Here is a quick summary, with thanks to the University of California Information Security department. As the Verizon report is based on actual investigations, it is one of the best sources for data on what is happening.



So, most breaches are perpetrated by criminals outside the organization using a combination of hacking and malware and relying on poor password practices. Most were NOT financially motivated or related to espionage. So, this would imply that most were motivated simply by malicious intent, likely as a challenge. It is also interesting to note that 43% (2 in 5) were not discovered by the targeted organization but rather by outside parties. Bottom line, recognize that your data is at risk and so be careful what you share, practice good password management and keep your virus protection up to date. If interested in reviewing the entire report (which is 73 pages) please go to <http://tinyurl.com/mzyk6vt>.

[Go to Index](#)

#22: Modems and Routers

Originally published in the July 2017 issue of *Venturing into our Past* (JGSCV)

A modem (**mod**ulate and **demod**ulate) is a device that accepts a series of analog signals (tones) and converts them into their digital equivalents (represented as 0's and 1's) and vice versa. Digital to analog is "modulation". Analog to digital is "demodulation". Your telephone typically sends and receives analog signals. Your computer recognizes 'digital' streams. The cable or telephone vendor provides you with a modem to interface between the communications line and your digital devices. It is the first device into which you would connect the cable coming into your home.

A router is a network device that takes a digital signal (after being converted by the modem), and intelligently distributes or suppresses it. It may connect directly to a desktop computer and broadcast via Wi-Fi for your wireless devices (laptops, smartphones, tablets etc.). Routers can have rules, including what signals to permit (for example you might bar adult content or specific websites), passwords (to restrict which devices can access it), encryption (to protect transmissions) and a built-in firewall (to protect your devices).

Most routers include built-in firewalls. This article provides easy instructions to check if yours does and, if so how to turn it on: <http://tinyurl.com/mt6cfml>. Check the user guide that came with your router or the vendor's web page for router-specific instructions.

Wireless routers are those that transmit digital data via Wi-Fi for use by your wireless devices. While not all routers provide wireless transmission, virtually all that are relevant to a home user do. Such routers offer one, two or even three "bands." Bands are the radio frequencies over which the router transmits Wi-Fi signals. If it only provides one band, it may be competing with other wireless devices (e.g., Bluetooth). Most offer two bands, 2.4 gigahertz (2.4 GHz) and 5 gigahertz (5 GHz). A few, offer three. Two is normally adequate. The router automatically switches as needed.

You generally do not need the fastest and most expensive routers since these likely far exceed the data rate from your Internet service provider (ISP). Older routers may be slow and use protocols that do not keep up with today's devices. A current or recent generation router providing 300 million bits per second (300 Mbps) is likely more than sufficient. Consider faster speeds if you are a "gamer", concurrently share several wireless devices, or stream videos.

Wireless routers will generally have one or more antennae. More antennae typically correlate to wider coverage. So, if you have a large area to cover, consider a router with several antenna. If you need to cover an especially large area or need Wi-Fi to go through certain types of walls and doors, you might need a separate range extender. Such a device amplifies the signal to reach additional areas.

Routers will have one or more USB and Ethernet ports for directly attached devices. This can include a computer, shared storage and printers. If you are connecting a USB 3 capable device, be sure the router has available USB 3 ports. USB 3 devices connected to USB 2 ports will transfer data more slowly.

Review the features before you buy a router and check objective online articles. For comparisons of the best current-generation wireless routers see <http://tinyurl.com/n63a3f3>, <http://tinyurl.com/hoon5qg>, or <http://tinyurl.com/8xjrafp>.

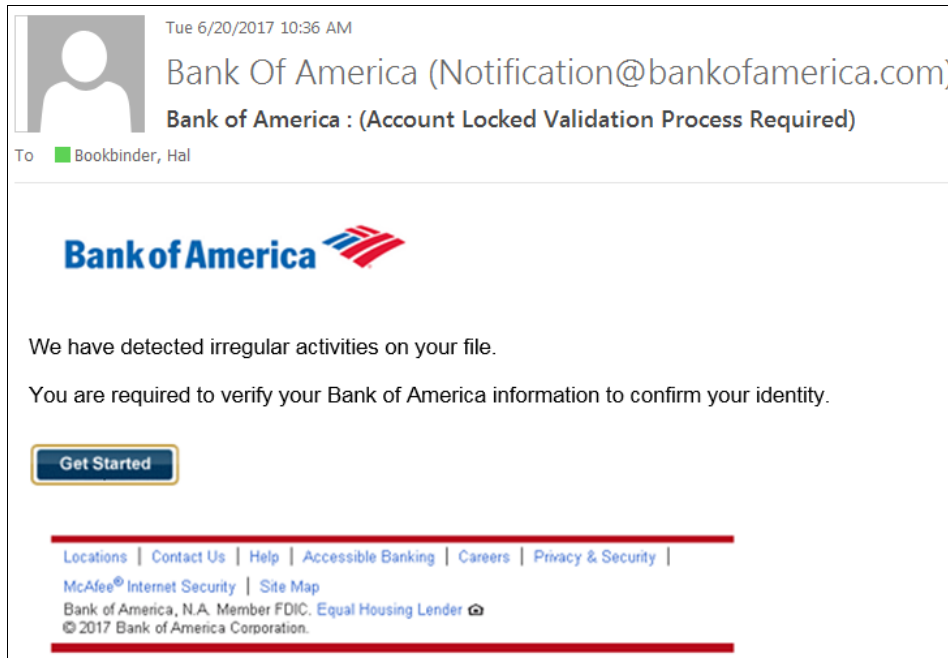
[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#23: Phishing email from your Bank

Originally published in the August 2017 issue of *Venturing into our Past* (JGSCV)

I recently received the email snapshotted below. Note that the sending email address looks legitimate and the Bank of America name and logo do as well. The “To” address is mine and there are no obvious spelling or grammatical errors. It tells me that my account has been locked which is certainly something I would want to fix quickly. Yet, this is a phishing email sent to obtain my personal information, including my Bank of America ID and Password. It is assuredly not from Bank of America.



Hovering my cursor over the Notification@bankofamerica.com address, the actual source address, “waqar.hussain@descon.com”, displayed. Try hovering over the supposed bankofamerica.com link and you will see this. Further, this is likely not even the real address. It is certainly not from Bank of America! Be assured that, if I were to click on the “Get Started” button, I would be taken to a website that looked like a legitimate Bank of America login screen. I will be asked to log in with my ID and Password. However, I will not be identifying myself to Bank of America. Rather this will be sent to “Waqar Hussain” or whoever is actually behind this email. They could then use this to access and drain my account.

Your bank would never send you such an email. DO NOT click on the link. Not only will you be taken to unsafe pages that likely will appear legitimate, but just clicking on the link may result in malware being installed on your computer. If you feel that this warning might be legitimate, call or log in to the bank using your normal method of doing so. NEVER click on a link in such an email.

Most readers will say that they “would never be fooled” by such an email. This is likely true if they thought about it. However, we often go ahead and click on links before thinking them through. Each time we do so we open ourselves to risk. Undoubtedly, thousands or even hundreds of thousands received this email. Some actually have accounts at Bank of America, and some percentage of these will fall for it making it a profitable scam. Think before you click!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#24: The Internet is forever

Originally published in the September 2017 issue of *Venturing into our Past* (JGSCV)

Some truisms to consider

1. "Don't email when angry"
2. "Anything you post may be viewed more widely than you intend"
3. "Deleted files may be recoverable" and
4. "The Internet is forever."

Be careful what you text, tweet, email, post to Facebook, place on a webpage or even save to your computer. Copies may exist on your computer, on servers, in email archives and of course, in the recipient's mailbox or message processor. Deleting or recalling an item does not remove copies and may not even remove the original.

When upset I often proceed to vent my anger in an email. I then set it aside and reread it the next day. 80% of the time I delete it. When I do decide to send it, I generally tone it down. Emails can often convey a harsher tone than intended. Once sent, it is too late to change one's mind.

Items erased from websites, and defunct websites, may not be gone forever. Check out the "Wayback Machine" at <http://archive.org/web/web.php> (if you forget the URL, just Google, "Wayback"). It periodically snapshots websites, preserving them forever. To date, it has saved over 300 billion web pages. For example, if you enter www.iajgs.org into the Wayback Machine search field you will find that it has snapshots of the website going back to 2000.

If you select 2001, a calendar will show that snapshots were taken on March 31st, April 3rd, July 20th and September 25th. If you click on the September 25th snapshot and select "Officers", you would see that Hal Bookbinder was president, Anne Feder Lee was vice president, Joel Spector was secretary and Michael Posnick was treasurer. The Wayback Machine began operation in 1996. It can be a great research tool. It can also preserve things that you wish would go away.

In the U.S. your employer has the right to monitor your use of company equipment, including your browsing, emails and instant messaging. Some believe that stricter privacy laws in Europe do not permit this. However, according to BBC News, The European Court of Human Rights ruled in January that a company had the right to check on a worker's activities and may read his Yahoo Messenger chats sent while he was at work. It did caution against unfettered snooping.

Even your own computer may contain files you "deleted" and your surfing history. When you delete a file, what you are actually doing is removing the index entry for the item and freeing up the space for reuse. Until overwritten, it continues to exist on your hard drive. Utilities can retrieve such files. Sophisticated utilities may even be able to recover overwritten files. Internet browsers generally preserve your surfing history unless you consciously turn this feature off. You might also consider turning on your browser's "private browsing" option to lessen the trail of crumbs you leave behind.

Be careful what you write, save, post, send and the sites you visit. You never know who may be watching – a family member, your company's security department, a co-worker, a friend, an enemy or even a potential boss.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#25: Top 10 Tips for Detecting Phishing

Originally published in the October 2017 issue of *Venturing into our Past* (JGSCV)

Recently, UCLA Health IT Security released the following tips for staff to use to recognize when they are being phished (i.e., the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers). These are good tips for us all.

1. **Hover over the From**

Probably the easiest way to identify if an email is legitimate or not, is to simply hover your mouse arrow over the name in the “From” column. By doing so, you will be able to tell if the email is from a recognizable domain that is linked to the actual sender’s name. For example, an email from Match.com should typically have the “From” domain of “match.com” (not “motch.com” or “humbletemper.com”).



2. **Are the URLs legitimate?**

Continuing on with the theme of hovering over certain parts of the email, another place to check would be any URLs the email is trying to get you to visit.

3. **Incorrect grammar/spelling**

A common practice of many hackers is to use misspelled words on purpose. While it may seem that this would easily reveal an illegitimate email, it is actually a tactic used to find fewer savvy users. Spammers have learned that if they get a response from a poorly written email, they are on to an easy target and will focus their efforts to bring that user down.

4. **Plain text/Absence of logos**

Most legitimate messages will be written with HTML and will be a mix of text and images. A poorly constructed phishing email may show an absence of images, including the lack of the company’s logo. If the email is all plain text and looks different than what you’re used to seeing from that sender, it is best to go with your gut feeling and ignore the message.

5. **Message body is an image**

This is a common practice of many spammers. Make sure the email is a good mix of text and images. Also, there may be embedded links for you to hover over within the image for an extra step of precaution.

6. **IP Reputation**

If you can easily [identify the sending IP of that email](#), you can look up the IP’s reputation through Return Path’s [Sender Score site](#). This tool will reveal a score (0-100) and will be able to give you

[Go to Index](#)

some insight into the sending IPs historical performance. The lower the score, the more likely the email is a phishing or spoofing attempt.

7. Request for personal information

One tactic that is commonly used by hackers is to alert you that you must provide and/or update your personal information about an account (e.g., Social Security number, bank account details, account password). Phishers will use this tactic to drive urgency for someone to click on a malicious URL or download an attachment aiming to infect the user's computer or steal their information.

8. Suspicious attachments

Is this new email in your inbox the first time your bank has sent you an attachment? The majority of financial institutions or retailers will not send out attachments via email, **DO NOT OPEN** attachments from senders or messages that seem suspicious. High risk attachments file types include: .exe, .scr, .zip, .com, .bat.

9. Urgent/Too good to be true

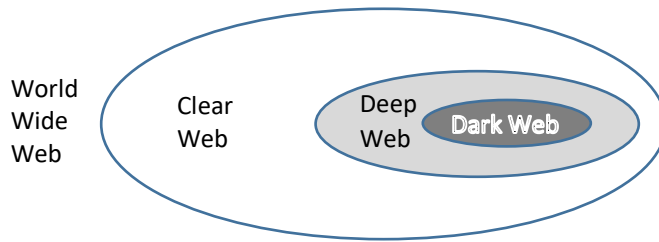
If an email seems too good to be true, it most likely is. Be cautious with any message offering to place money into your bank account by simply "clicking here". Also, if the content places any kind of urgency as far as "you must click into your account now", it is most likely a scam and should be marked as "junk".

10. Is my email address listed as the "From" address?

If you notice that your email address is being identified as the "From" address, this is a sign of a fake email message. Along those same lines, if the "To" field shows a large list of recipients, you should also be cautious. Legitimate emails will most likely be sent directly to you and you only. You may see "undisclosed recipients" and this is something to keep an eye on as well. It could be a valid send, but double check by using the other tips identified above.

#26: What is the 'Dark Web'?

Originally published in the November 2017 issue of *Venturing into our Past* (JGSCV)



The Internet connects you to the World Wide Web (WWW). This comprises all of the sites on the Internet accessible through their Uniform Resource Locators (URLs). Search engines (like Google or Bing) index only a small portion of the WWW, likely less than 5%. The portion of the WWW visible to these search engines is called the “Clear Web” (or “Surface Web” or “Clear Net”).

The 95% that is not indexed is referred to as the “Deep Web” (aka “Invisible Web” or “Hidden Web”). The Deep Web includes database, email and private messaging content. When you access your bank account, download a video on demand, search for your surname in Ancestry, or your town on JewishGen, you are accessing the Deep Web. While your bank’s main website, a video sharing site, Ancestry.com and JewishGen.org are public forms and part of the Clear Web, digging into the data underneath takes you into the Deep Web.

The “Dark Web” is that portion of the Deep Web that requires special software to access. Traffic on the Dark Web is typically transmitted through numerous intermediary sites and encrypted multiple times, providing anonymity. This includes small friend-to-friend networks as well as large networks such as “Freenet”, “I2P” and “Tor”. The Tor Network is the most widely used Dark Web browser. Its URLs end with “.onion” (rather than “.com” or “.org”). Hence, it is sometimes referred to as “the Onion Domain”.

It you are in Los Angeles and accessing a Dark Web site hosted in New York you might be routed through Belgium, Russia and Jamaica. New York sees the sending site as Jamaica and you see the send-to site as Belgium. These landing points, or nodes, are referred to as “botnets.” They forward your traffic from one node to another, repeatedly encrypting it along the way. This frustrates discovery of who you are, what you are accessing and what you are communicating. A user of the Dark Net can take further steps to hide his/her browsing. While I cannot attest to its accuracy, you might check out <https://darkwebnews.com/help-advice/access-dark-web/>.

Significant legitimate traffic exists on the Dark Web, including discussion groups, in which peers simply wish to confidentially message, blog or share files. Another use is for “Bitcoin” exchanges and anonymous searching. However, due to its anonymous nature, it is also used for illegal trading, buying and sharing by extremists, drug dealers, hackers, pedophiles and terrorists.

We are all aware of the major hacks of personal data that have occurred in recent months, including the enormous one at Equifax. Some data from these hacks is certainly available for purchase on the Dark Web. To make it more difficult for criminals to gain access to your personal data, maintain strong passwords that you regularly change and instruct the credit bureaus to limit the use of your information. Carefully monitor your financial statements and take quick action when you notice something is amiss.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#27: Take care when you use Google

Originally published in the December 2017 issue of *Venturing into our Past* (JGSCV)

We all use search engines like Google and Bing multiple times each day and generally trust that the algorithms they use are taking us to legitimate pages on the Web. We know that the first few links pay for this placement. So, we skip over these and go to the first or second link after the advertisements.

Some malware experts have devised ways to trick the search engines and get their own sites at or near the top. You click on the link and think you are on a legitimate site. After all, you searched for it and used a great tool like Google or Bing. The site then directs you to another and maybe another site. You are still not suspicious.

It now presents you with a button to download a Word document with the information you want. You have no reason to suspect anything and so click on the button. When you open the Word document, it asks you (usually in a banner at the top of the page) to “enable macros”. You have come this far and everything looks legitimate and so you do so.

Microsoft Word defaults to not allowing macros because they can be dangerous. A macro is an executable script that could do almost anything, including installing malware on your computer. You finish your reading and do not realize that you are now infected with software that may be recording and transmitting your keystrokes, displaying adware or deleting your files.

My purpose is not to make you paranoid about search engines. But, when you do search, look at the URL. Does it appear legitimate? If it redirects you several times, be suspicious, never providing personal information. Most importantly, think twice before downloading a file, and if you do and are asked to “enable macros”, run for the nearest exit. This is rarely a good sign.

A class of malware called “Zeus Panda” uses this clever way to cause you to let your guard down. It has been implanted into certain web pages which are designed to display near the top in a Google search. These pages appear completely legitimate, but are infected. You are then directed to a site that asks you to download a Microsoft Word document which contains macros.

Once you agree to “enable macros” they are active and you are at risk. These same Word documents are distributed as attachments to SPAM email. Most of us are rightfully wary of downloading files from SPAM email or agreeing to “enable macros”. However, the hackers know that by offering this after a search you initiate, you might let down your guard. Never agree to “enable macros” unless you are confident that the document is legitimate and permitting it to run scripts is safe.

Want to read more about Zeus Panda? Just Google it. (Yes, I see the irony. Do not abandon Google; just to be careful.)

[Go to Index](#)

#28: Password Managers, again

Originally published in the January 2018 issue of *Venturing into our Past* (JGSCV)

In October 2016 I wrote about Password managers, sharing my experience with a free tool, LastPass. I have been using it now for well over a year and remain quite satisfied with its features. It supports my access to over 100 sites with a variety of IDs and passwords. I commend it to you as a tool which can streamline your access to sites on the Internet while providing enhanced security.

Password managers store your login information. They then automatically log you in to the site once you bring up the login page. They often include other valuable security features, like recognizing new sites that you have logged into and offering to save the login information, filling in forms, synchronizing across your devices, generating impossible to remember complex passwords and permitting you to designate a person to obtain your access if you become incapacitated.

LastPass is intuitive, providing “cards” for each website you wish to access and displaying them in logical folders. You enter a description, ID and password into each card. I set up separate folders for email sites, financial sites, genealogy sites, shopping sites, social media sites, travel sites and work sites. I then open the appropriate folder and click on a card. LastPass takes me there and logs me in.

Typically, sites ask for an ID (or email) and a password. Sometimes, however, they ask for a third entry. A site I use asks for my last name, ID and password. LastPass permits you to add a third entry along with the two typical ones. So, you can script it to accommodate unique situations. LastPass resides in the Cloud. So, you can access it from any computer. For computers you typically use, you can link it into the browser (Internet Explorer, Chrome, Firefox, Safari) so that it is immediately available without first logging in. Do not do this if others share the computer as they will then have the ability to log in as you.

Some sites require you to click on a link to the login page and then to enter your information. Consider setting up the card with the login page rather than the initial page. LastPass also generates complex passwords on request which you can use to better secure your most critical sites. You can download it from <http://www.lastpass.com>.

For excellent comparisons of commercial Password Managers, see “The Best Password Managers of 2018” (<https://www.pcmag.com/article2/0,2817,2407168,00.asp>) and “The Best Free Password Managers of 2017” (<https://www.pcmag.com/article2/0,2817,2475964,00.asp>). PC Magazine rates two free Password Managers as “Editors’ Choice”, LastPass and LogMeOnce. Please do your own investigation to select the right tool for you.

A password manager is a convenient, secure way to maintain different passwords for the various sites that you visit. Of course, you must create and remember a password for your password manager. Consider recording it in a secure location, like your safe deposit box - just in case.

[Go to Index](#)

#29: Meltdown and Spectre

Originally published in the February 2018 issue of *Venturing into our Past* (JGSCV)



You may have heard of two widely-reported vulnerabilities, Meltdown and Spectre. They take advantage of the way personal computers, mobile devices and the cloud intuitively pre-position data in “cache” to speed performance. This data may then be exposed to other programs running on the device or otherwise sharing workspace. This risk can impact iPhones, iPads, Android devices, Macs, Windows and Linux computers.

This is a difficult issue to fix as the problem is inherent in virtually all processors created in the past 20 years. Software fixes reduce but do not eliminate the exposure. Further, these software fixes may slow processing 10% to 30%. In their haste to respond, Intel released fixes that actually introduced problems in which computers rebooted themselves unexpectedly. They then advised customers not to install available updates. On January 22nd, Intel announced that it was testing a fix to address this rebooting problem. By the time you read this, it will likely be available. For the latest from Intel, go to <http://www.intel.com> and click on “Find out the latest news...”

While the likelihood of you being impacted is slight, there are some precautions you can take to further reduce the risk. Keep your software programs current, close individual browser windows when you no longer need them and rather than simply walking away from your computer or just locking it, log off. If you are using an older operating system that is no longer being maintained (like Windows/XP or Windows/ME) upgrade to a current version (Windows/7 or later).

Notwithstanding the recent Intel issue, you are likely better served by updating your devices with the latest software patches and versions as they are released. Generally, devices are set to check for updates automatically and either accept them or ask whether to install the update. Sometime we opt to defer so as not to interrupt our use of the device. As these updates may contain fixes to these or other vulnerabilities, it is best to accept them, especially if noted as a “security patch” or a “critical update”.

If you are not sure whether you have all current updates and patches, check the vendor’s website. This applies to your browser (Internet Explorer, Edge, Safari, Chrome and Firefox), your operating system (iOS for Apple devices, Windows and Linux for PCs and Oreo for Android devices) and your hardware (Intel, AMD and ARM). Once on their website, search for “Meltdown” or “Spectre”.

Be wary of folks who may try to trick you. Do not click an email link purported to contain critical security updates. These are generally scams. Rather, go directly to the vendor’s website. You will likely find that you are already current due to automatic updates. Legitimate fixes do not come through links in emails!

Expect further fixes to be issued over time as hackers discover creative ways of exploiting these vulnerabilities. As of this time, however, no such misuse has been detected. If you want to better understand Meltdown and Spectre, check <https://meltdownattack.com>. It offers a quick description, an excellent set of FAQs and a lengthy research paper on each. Access it through Chrome, Firefox or Safari. It was not created to operate correctly under Internet Explorer or Edge.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#30: Precautions while Traveling

Originally published in the March 2018 issue of *Venturing into our Past* (JGSCV)

The U.S. Department of Health and Human Services Office of Civil Rights (HHS OCR) recently published a lengthy list of precautions to limit your exposure when traveling. Along with the obvious things like requiring passwords to access your devices that cannot be easily guessed and backing up your data before your leave on your trip, following are six that you may not have previously considered:

Bring and Use Your Own Power Adapters and Cords

It's never safe to charge your devices using anything other than your own power adapters. Cyber thieves may install malware onto hotel lamps, airport kiosks and other public USB charging stations. If you absolutely must charge your device on the road, and you don't have access to your charger/adaptor, power down your device before you connect it into any airport chair or public USB charging station.

Install Security Updates and Patches

Be sure to patch and update operating systems and software (including mobile device apps). This should be a regular practice, but it is particularly important if you will be unable to update while traveling. Updates and patches can fix security flaws and enable security software to detect and prevent new threats.

Turn Off Wi-Fi Auto-Connect and Bluetooth

Go into your device's Settings feature, and disable the Wi-Fi auto-connect option so that you manually connect when it is safe to do so. Similarly, disable Bluetooth connectivity. If left on, cyber thieves can connect to your device in a number of different and easy ways.

Avoid Public Wi-Fi

Avoid connecting to any public Wi-Fi network. Using your mobile network (like 4G or LTE) is generally more secure than using a public wireless network. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Always log into your work networks through VPN, and only use sites that begin with "https://" when online shopping or banking.

Ensure Physical Security of Your Devices

NEVER let your devices leave your sight. If you cannot physically lock devices in your hotel room safe or other secure place, take them with you. There are no good hiding spots in your hotel room! Many breaches occur because a device was left unattended when an opportunistic thief struck. When traveling with laptops and tablets, the best protection is to carry them with you. It's never safe to pack your devices in your checked luggage.

Use Geo-Location Cautiously

Most social media sites are happy to automatically share your location as you post photos and messages. This also tells thieves back home that you are away, which is a great time to break in. So, limit the information you post regarding your location at any point in time.

See <https://www.hhs.gov/sites/default/files/ocrcybersecurity-newsletter-december-2017.pdf> for the full HHS OCR list of traveling precautions.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#31: What is GEDCOM?

Originally published in the April 2018 issue of *Venturing into our Past* (JGSCV)



GEDCOM (**G**enealogical **D**ata **C**ommunication) provides a set of rules for exchanging data between genealogical software. The LDS Church created GEDCOM in 1984, with its final update in 1999 (version 5.5.1) offering it freely to the genealogical community. The LDS Church now sponsors the 'GECCOM X' Project. More about this later.

When you create an EXPORT file from your family tree program to share or upload family data, it is created using the GEDCOM standard. GEDCOM is a "Hypertext" language. Hypertext languages include level numbers, descriptors and data, all in plain text, which can be read by different programs running in various operating systems on different computers. The level numbers and descriptors define the subsequent data so that the receiving program knows how to handle it.

HTML (Hypertext Markup Language) is another hypertext language which is used to define every page on the World Wide Web. If you hold down the CNTL key and press "U" while viewing a web page you will see the underlying HTML code. Don't worry, this will do no damage. XML and HL7 are other hypertext languages. XML (Extended Markup Language) is used to share data and HL7 (Health Language) is used to share medical information.

Below is some typical GEDCOM code (on the left) and what it means (on the right).

0 @11@ INDI	Indicates that the following data relates to individual #1
1 NAME John /Smith/	Provides the name of individual #1, denoting the surname with "/"
1 SEX M	Indicates that the sex of this individual is male
1 FAMS @F1@	Indicates that this individual is a member of family group #1
0 @12@ INDI	Indicates that the following data relates to individual #2
1 NAME Mary /Jones/	Provides the name of individual #2, denoting the surname with "/"
1 SEX F	Indicates that the sex of this individual is female
1 FAMS @F1@	Indicates that this individual is a member of family group #1
0 @13@ INDI	Indicates that the following data relates to individual #3
1 NAME Sam /Smith/	Provides the name of individual #2, denoting the surname with "/"
1 SEX M	Indicates that the sex of this individual is male
1 FAMS @F1@	Indicates that this individual is a member of family group #1
0 @F1@ FAM	Indicates that the following data relates to family group #1
1 HUSB @I1@	Indicates that the husband in this family group to be individual #1
1 WIFE @12@	Indicates that the wife in this family group to be individual #2
1 MARR	Indicates that the current state is "married:
1 CHIL @13@	Indicates that a child in this family is individual @3

There are 134 GEDCOM descriptor tags, including BIRT (birth), MARR (marriage), DEAT (death), BURI (burial), EMAI (email), PHON (phone), RESI (address or place of residence), OCCU (occupation), RELI (religion), BARM (bar mitzvah) and BASM (bat mitzvah). For a listing of all of the tags, see <http://tinyurl.com/lah2stk>.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

Some programs are designed to read data directly from other program's files. For example, RootsMagic can directly import a FamilyTreeMaker (FTM) data file. However, FTM will not directly import a RootsMagic file. To transfer data from RootsMagic to FTM, you must first export it as a GEDCOM file.

GEDCOM has some limitations. Pictures, Videos and links to web pages will generally not transfer through GEDCOM. A program may have unique fields or might be using a proprietary version of GEDCOM, such as GEDCOM 5.5 EL (Extended Locations). Nonstandard fields may not be transferred.

A program may permit you to create your own tags, sometimes by replacing standard ones with ones you define. Say you replace "Christening" with "Brit Milah". This may work just fine in your program. But when transferred, the underlying tag may still be the one for christening.

Generally, when you are creating an export to GEDCOM, your program will permit you to identify which fields to export. Be sure to carefully review this to ensure you are exporting only the desired fields. For example, you may not want to export your notes, sources or some data you wish to keep private.

Sometimes a receiving program has rules which block certain data. For example, it might not accept information on living individuals. So, when transferring data, be sure to understand both the exporting rules of your program and the importing rules of the receiving program.

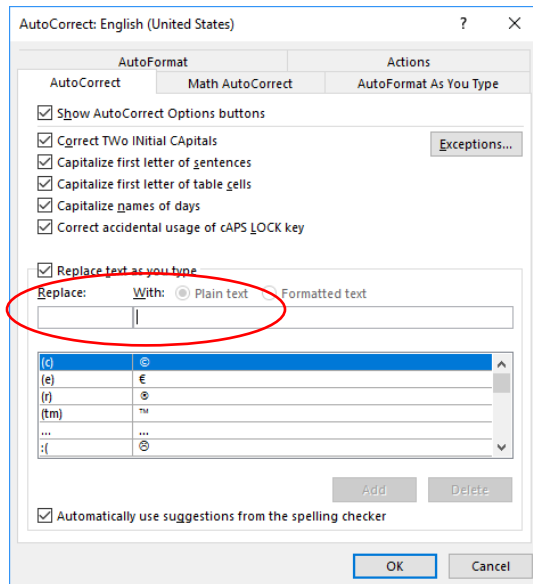
If data you expected to be transferred seems to have been dropped, check the 'Notes' field. Sometimes, receiving programs will dump the data that they could not interpret into Notes. Another thing to check is your export settings. The default settings may not have included the missing data.

As noted at the beginning of this article, GEDCOM has not been updated in over 17 years while a lot of technological advances have occurred. With all of these limitations, why isn't someone doing something about it? And, this is where GEDCOM X comes in. Family Search (the genealogy arm of the LDS Church) launched the "GEDCOM X" Project in 2011. The GEDCOM X Project invites a diverse community of developers to create new specifications which, once approved, grow the product. If you want to read more about GEDCOM X, see <http://www.gedcomx.org>. For now, however, your programs likely continue to use the GEDCOM 5.5.1 standard.

#32: Microsoft Word Tips & Tricks

Originally published in the May 2018 issue of *Venturing into our Past* (JGSCV)

Do you routinely spell a particular word incorrectly and wish Word would automatically correct it rather than just flagging it as misspelled? Do you wish it would stop automatically correcting the spelling of another word? This kept happening to me when I would type 'EHR', (Electronic Health Record). Word kept 'helping' me by changing it to 'HER'. It also kept helping me by changing 501(c)(3) to 501©(3).

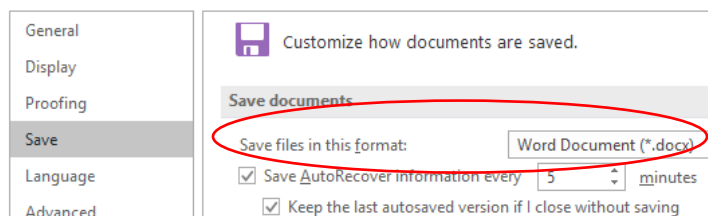


To fix such annoyances, click 'File' (in the upper left-hand corner of the Word page and then 'Options', 'Proofing' and 'AutoCorrect Options'. You will see two fields under the titles, 'Replace' and 'With'. If you type ehr in the 'Replace' field you will see that it displays her in the 'With' field. I deleted this entry and can now type EHR without it being changed. As I want ucla to be automatically converted to UCLA, I added an entry to do this. When I type resume, I usually mean résumé. So, I added this as well.

If you wonder how to enter é or any other special character, click on the 'INSERT' tab on the top of the Word screen and the 'Symbol' icon all the way on the right. A short list of popular symbols will be displayed. If you do not see what you want, click on 'More Symbols' and select from a wide array of special characters.

We have all experienced the frustration of having our PC freeze while creating a document. You can have Word save your work periodically (every minute if you like) so that you will never lose too much of it. Similar to Proofing, select 'File' and 'Options'. Now select 'Save'. You will be able to define where and how often you would like backups taken.

Word Options



These are just two of many helpful features you can find within 'File' and 'Options'. Choose 'File', 'Options' and 'Customize Ribbon' to display more or fewer icons in the ribbon across the top of the page). You can add ones you would like to have handy and remove ones that you never use. If you have not explored 'File' and 'Options', I encourage you to do so. There are literally hundreds of things you can set to make your Microsoft Word experience more pleasant and efficient.

The other Microsoft Office products (like Excel and PowerPoint) each have an array of preferences you can set under their 'File' and 'Options.' Understand, however, that options you set are only effective for that product. So, if you set your automatic save option to preserve copies every minute in Word and want this in Excel as well, you will need to set it directly in Excel.

[Go to Index](#)

#33: Best Anti-virus Protection of 2018

Originally published in the June 2018 issue of *Venturing into our Past (JGSCV)*

Prior articles in this series (January 2016 – “Is Your Virus Protection Actually Working?” April 2017 - “Viruses, Worms, Trojan Horses, Spyware”, May 2017 – “Malware Protection”) discussed the need for a properly running antivirus program on any computer connected to the Internet. Each year, PC Magazine publishes its recommended list of the top ten antivirus programs. This year’s list includes:

<u>Antivirus Program</u>	<u>2018 Rank</u>	<u>2017 Rank</u>	<u>2016 Rank</u>		
McAfee Antivirus Plus	1	1	3		
Webroot SecureAnywhere Antivirus	2	2	4		
Symantec Norton Antivirus Basic	3	4	--		
Bitdefender Antivirus Plus	4	3	1		
Kaspersky Anti-Virus	5	5	2		
Avast Pro Antivirus 2017	6	6	5		
ESET NOD32 Antivirus	7	8	9		
F-Secure Anti-Virus (2017)	8	9	10		
Sophos Home Premium	9	--	--		
Trend Micro Antivirus Security	10	10	--		

For more information about these antivirus programs, pricing and a side-by-side comparison, see <https://www.pcmag.com/article2/0,2817,2372364,00.asp>. All of these products function well. Pick one that you prefer and be sure to configure it to check all of the files, emails and websites you access. While many have higher “regular” prices, watch for sales and spend \$25 or less per computer.

PC Matic, which advertises heavily as the only product fully American-made and based on whitelisting is not on the list. While I like both concepts, PC Magazine testing has found that whitelisting blocks too many legitimate sites and is not significantly more effective than competing commercial tools. PC Matic claims to include legitimate sites quickly once identified.

Below are rules to remember regarding antivirus software:

1. Antivirus programs include an “engine” and a list of current virus profiles. Both are automatically updated so long as the subscription is maintained.
2. Once the subscription ends, the engine may continue to run. However, without updates both to the engine and to the profiles, protection is incomplete and may miss current viruses.
3. New computers typically include a “free” antivirus program for a limited period. Be sure to pay to extend the subscription or install another program when the subscription ends.
4. Antivirus programs may provide you with the ability to raise or lower the level of protection. Setting this too high may block things that you want. Setting it too low may put you at risk.
5. If you are instructed to turn off virus protection while installing new software, be sure to promptly turn it back on as soon as you are able to do so.
6. Multiple antivirus products on the same computer can dramatically slow it down. If you decide to switch antivirus programs, be sure to uninstall the old one before installing the replacement.
7. If unsure whether your antivirus software is configured and running properly, go to the vendor’s website. Most will provide a facility to check your settings and suggest appropriate changes.
8. NEVER accept unsolicited offers to scan your computer, to provide antivirus software, or any other service. If you do, you will likely end up with more issues than solutions.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#34: Urgent Demand for Payment

Originally published in the July 2018 issue of *Venturing into our Past (JGSCV)*

On June 6, 2018, the following notice was issued:

UCLA Office of the Administrative Vice Chancellor**Urgent Notice**

To the Campus Community:

An unknown suspect has been calling UCLA students claiming to be a UCLA Police Officer and demanding money. The UCLA Police Department (UCPD) does not call students or anyone else asking for money.

Do not send money to any law enforcement or government agency via wire transfer.

The suspect is falsely claiming that UCPD has a warrant for the student's or family member's arrest and a payment via wire transfer (Western Union, Money Gram, etc.) will resolve the issue. In one instance, the student was instructed to purchase gift cards and ship them to a PO Box. Even if a student does have an outstanding warrant, fines for such violations are always paid to a court and never to an individual or company. There are no circumstances in which UCPD would ask for money via a wire transaction.

This is true for other enforcement agencies as well, including the Internal Revenue Service (IRS), Immigration and Customs Enforcement (ICE), and Immigration and Naturalization Service (INS). If you owe back taxes or action is required regarding your student Visa status, you will be notified via official channels. None of these agencies or departments would ask for money over the phone or via a wire transaction.

If you have any questions, please do not hesitate to contact UCPD at (xxx) xxx-xxxx.

Sincerely,

Michael J. BeckAdministrative Vice Chancellor

While you may well believe that you would never fall for such an attempt to scam you, in the heat of the moment when a con artist connects with you and demands immediate payment, can you be sure you will be thinking so clearly? These con artists are very good at what they do. They may have some of your personal information and use it to convince you that they are indeed from the government or they might scare you with the story of a relative or friend trapped overseas. There will be a sense of urgency with dire consequences if you do not comply. **Requiring immediate payment by wire transfer or through untraceable items (like Bitcoin or gift cards) is a clear red flag.**

Consider this...Do your family or friends post updates on Facebook while traveling? Think of how easy it is for a con artist to identify family members and friends and their vacation location and then to use this information in contacting you with an urgent request for money to get your family member or friend out of a terrible jam in a faraway place. Be on your guard and do not fall for such scams!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#35: Google Search Tips and Techniques

Originally published in the August/September 2018 issue of *Venturing into our Past (JGSCV)*



Google is the primary way virtually all of us routinely search the internet. My students feel that they have performed their research by simply doing a Google search. As genealogists we seek confirmation of information we find. Here are a few tips to make you a more powerful Google user (most work for other search engines as well).

Add symbols and special words to your search, such as

- - (minus sign) to exclude a word from your search (must be immediately before the word)
- " " (quotation marks) around a phrase to return that exact phrase
- **define** to look up the meaning of a word
- **image** to display images related to the search word(s)
- **map xxx** to display a map of the location. You can then take a closer or farther away look
- **OR** to indicate that you want pages with either word or phrase (must be capitalized)
- **related:xxx.com** to search related sites to xxx.com
- **site:xxx.com** to search only in that domain
- to convert currencies, enter something like "**200 zlotys to dollars**"
- **translate** to convert a phrase from one language to another
- **weather** to look up the current and forecast for a location

Want to learn more? Search "**Google Tips**". But, be aware that Google periodically changes these features. For example, they used to allow wild cards within words but do not now do so now. Some tip sites are out of date. I prefer ones published in the past year.

OR is a powerful tool to speed research. Say you are searching for Joseph Bookbinder but it may be spelled Buchbinder, you could search for "**Joseph Bookbinder**" **OR** "**Joseph Buchbinder**" and do this in one search rather than two. Remember, you must capitalize the **OR**.

The minus (-) function can be used to narrow your search. One of the families I am researching is Barenberg. There are lots of pages on Russ Barenberg, a guitarist. When I want to exclude these pages, I search **Barenberg -Russ** (note that Russ immediately follows the minus sign with no intervening blanks).

I have found the **map** function to be particularly useful. In preparing for my trip to the Warsaw Conference and associated travel in Poland and Ukraine I used this tool regularly to understand the proximity of a location to others as well as to check out a town's street layout. One can easily move the map, hone in for a closer view and back up for a wider one. I printed several for use during the trip.

A final tip is to use Google to track your packages. Simply type in the FedEx, USPS or UPS tracking number and this will retrieve the package's history and current location. No need to enter the company.



If you don't find what you want, consider another search engines, like Bing or Yahoo! Features are similar to Google but they scan the Internet and present findings differently.

They may find something that Google did not, or return it on one of the first pages rather than many pages down. To learn more, search for "**BING tips**" or "**Yahoo tips**".

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#36: iPhone Tips

Originally published in the October 2018 issue of *Venturing into our Past (JGSCV)*

After this summer's conference in Warsaw, I spent several weeks traveling across Poland and Ukraine, taking thousands of iPhone pictures. I was bummed after inadvertently deleting some before transferring them to my laptop. I then found that the iPhone was prepared for this. Here are some iPhone tips, starting with recovery of deleted photos.



Photos that you “delete” from your iPhone are recoverable for about 40 days. Use the “Photos” app on your iPhone to recover them. To do so, click on “Albums” and then on “Recently Deleted”. Icons of your recently deleted pictures will be displayed with a number of days until they will be permanently gone. You generally have 40 days to recover deleted photos. Once you click on a picture icon, you can choose to “recover” it or to “delete” it permanently.



Once you see a highlighted location in the Map app in which you are interested, tap on it and see information about it such your distance from it, its address, directions to get there, phone number, hours, website, what Wikipedia has to say about it and more. You can even look inside an airport or shopping mall to find a gate, restaurant or restroom.



In an emergency, first responders can access important medical information without needing your passcode. To provide info, such as medications you take, open the Health app and fill out your Medical ID. I had forgotten where it was located. So, I swiped down on the home screen and typed “Health” into the search field. The Health app icon was displayed along with its folder's name.



Want an alternative to using your thumbs to enter names or text messages? You can speak these instead. Tap the microphone symbol and speak the name or message. It will be automatically typed. Like Victor Borge, you can even speak the punctuation. Oh, come on, you remember Victor Borge!! You don't? Look him up on YouTube.



Want to be able to use your iPhone as a magnifying glass? Go to Settings > General > Accessibility and turn on Magnifier. Then triple-click the Home button at any time to use the camera to zoom in on small details. Review other accessibility options as well. Also, check out “Display and Brightness”. Among other settings, you can adjust “Text Size” and even make text “Bold” so that it easier to read - a great alternative to squinting!



Over time, you may find that your iPhone is getting sluggish. There are a number of steps you can take to clear the cobwebs and speed it up. Check out the following for several hints: <https://www.macworld.co.uk/how-to/iphone/speed-up-slow-iphone-3463276/>



Ever wish to take a screenshot of what is displayed? Press the Home button (at the bottom center of the iPhone) and the Sleep/Wake button (on the right side of the iPhone) at the same time. The picture will be saved to the Screenshots album in Photos. A small version of it will be briefly displayed in the lower left corner of the screen.

Want more? Go to <https://tips.apple.com/en-us/ios/iphone> for more iPhone tips. Or, to get help with a specific problem, simply Google, “How do I xxxx on my iPhone?” substituting your issue for the x's.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#37: Facebook 'Tokens'

Originally published in the November 2018 issue of *Venturing into our Past (JGSCV)*



When I was 80% done with this article Word froze with an hourglass and I had to kill it. Due to "autosaving", however, my work was not lost. To turn this on, click on "File," "Options," and "Save." Then, choose how often to take backups and where to store them. Also, check, "Keep the last autosaved version if I close without saving."



According to Facebook, on September 25, 2018, they discovered that they had been hacked exposing 50 million Facebook accounts. The estimate was later revised to 30 million. Finding a vulnerability in Facebook code, the hackers were able to obtain "tokens" for millions of Facebook users and use these tokens to simulate being the user and so access their data.

Tokens are strings of data provided when you connect to an application. The token is stored in a cookie in your computer. Another copy is kept by Facebook. Each time you perform an action with that application (inquire, update, etc.) Facebook queries the cookie, extracting the string and including it with the requested action. If it matches the Facebook copy and has not yet expired, it permits the transaction to take place.

Tokens have expiration dates and times. Typical tokens expire after two hours. But they may be set to expire more quickly or even last for up to 90 days and can be renewed if permitted by the application. Presumably, the hackers were able to obtain the copies of the tokens held by Facebook (not from your computer). So long as they had not yet expired, they could then use them to pretend to be the owner. It is possible that they were even able to renew these tokens.

Using the tokens, they could access some of the data that you have provided to Facebook, including personal details such as name, email address, phone number, posts, friend lists, group memberships and the names of recent message conversations. They did not have access to the contents of the messages. But, with the information they were able to get, they could obtain tokens for your friends and through them their friends. They could even see the most recent 15 searches and 10 locations you visited as Facebook keeps a record of these.

By getting friends' tokens and then their friends' tokens, and so on they could rapidly obtain millions of them (30 million, apparently). Once Facebook learned of the hack, they installed patches for the three vulnerabilities that together permitted the hackers to do what they did. They further expired 90 million tokens on their sites making them useless. If you had been able to access a function through Facebook without logging in and suddenly found that you had to do so, it is likely that your token was forced to expire.

Such hacks will continue. So, you need to think about what you share and what you do on the Internet, realizing that it all might be exposed someday. This experience does emphasize the need to log off of applications rather than just disconnecting. This notifies the application to expire your token, rather than letting it sit there, unexpired, awaiting the next hacker.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#38: Practicing Safe 'Tzedakah' (Charity)

Originally published in the December 2018 issue of *Venturing into our Past (JGSCV)*



As December 31st approaches, phony charities ramp up their solicitations through mailers, TV ads and online. Do you know whether a charity is legitimate, and even if it is, how much of the collected funds actually go to the cause you support and how much is eaten up in fundraising and administration? Commercials and mailers are often unclear or misleading about how the money is spent.

We have all heard the Kars4Kids jingle innumerable times. But, do you have any idea how much of the collected funds go to help kids? Do you know what programs are offered, where they are offered and for what kids? This charity is operated by an Orthodox Jewish community in New Jersey, primarily to support its Jewish camps and youth activities. While there is nothing wrong with this, you wouldn't be aware of it from the charity's incessant jingle which was recorded in 1999.

Kars4Kids has a "D" rating from Charity Watch due to the fact that 63 cents of every dollar collected goes into fundraising and overhead. They have been sued by several states for misleading advertising and insider business deals. Per Charity Watch, comparable Jewish and youth development charities spend, on average, 15 to 21 cents per dollar on fundraising and overhead.

If this isn't enough to give you pause, on November 13, 2018, [HackenProof](#) reported that a Kars4Kids database, containing information on 21,612 individuals (one week's worth of data) was found unsecured and with evidence that it may have been copied by cyber criminals. The report details the difficulty they had in getting Kars4Kids to secure the database.

Often there is confusion about exactly what a charity does. For example, the Association for the Prevention of Cruelty to Animals (ASPCA) focuses most of its programs in NYC. When they mention "our shelter", that is where it is located. Your local animal shelter is likely not associated with the ASPCA and derives little benefit from your donations to it. This in no way disrespects the great work of the ASPCA. But, if you want to help animals here, consider giving to your local shelter.

To research a charity, you might check its annual IRS 990 filings. These can be accessed through the Foundation Center's "[990 Finder](#)". If you search for Kars4Kids, you will find information on its income, expenditures and programs for several years up to 2016 (the most recent year available). You will also find that most of the funds raised are transferred to Oorah, Inc., a sister charity that operates its programs. If you then look up Oorah you will find that it spends millions on management and overhead.

Don't give to a charity just because the name and mailer or commercial seems appealing. Rather, understand how much of the funds actually go into programs you want to support. Ask the solicitor to mail you this information; read their website; Google their name; review their IRS 990 filings and check their reviews and ratings on the various charity monitoring websites. These include [Charity Watch](#), [Charity Navigator](#), [Consumer Reports](#) and the [Better Business Bureau's Wise Giving Alliance](#).

[Go to Index](#)

#39: Ten Tips

Originally published in the January 2019 issue of *Venturing into our Past (JGSCV)*



Welcome to 2019. Below are my top ten tips for practicing safe computing, along with references to past articles in this series which provide additional information on each item. Wishing you a year of safe and productive computer and Internet use.

1. Ensure a current antivirus program is installed, running, and set to scan all incoming files. [Best Anti-virus Protection of 2018, Jun 18](#)
[Malware protection, May 17](#)
[Is Your Virus Protection Actually Working?, Jan 16](#)
2. Set your computer to automatically accept security updates. [Precautions while Traveling, March, 18](#)
[Protection from WannaCry Ransomware, June, 17](#)
[Avoiding becoming victim of Ransomware, May 16](#)
3. Regularly back up your data to a remote location. [Microsoft Word Tips & Tricks", May 18](#)
[Avoiding becoming victim of Ransomware, May 16](#)
[Backing up your System, April 16](#)
4. Do not open suspicious emails or click on risky email links. [Take care when you use Google , Dec 17](#)
[Top 10 Tips for Detecting Phishing , Oct 17](#)
[Phishing email from your Bank, Aug 17](#)
[Social Engineering, Jun 16](#)
[Avoiding becoming victim of Ransomware, May 16](#)
[A Free Scan of Your Computer, Dec 15](#)
5. Do not provide personal information unless you trust the requester. [Phishing email from your Bank, Aug 17](#)
[Don't help them steal your identity, Oct 15](#)
6. Do not respond to offers that sound too good to be true or require immediate response. [Urgent Demand for Payment, Jul 18](#)
[Phishing email from your Bank, Aug 17](#)
7. Set up different complex passwords for all critical files and use a password manager. [Password Managers, again, Jan 18](#)
[Password Managers, Oct 16](#)
[Passwords, Aug 16](#)
8. Log off applications. Don't just close the window. [Facebook Tokens, Nov 18](#)
[Sharing Your Family Tree & Identity Theft, Sep 16](#)
9. Be careful what you write, save, post, send and the sites you visit. You never know who may be watching. [Precautions while Traveling, Mar 18](#)
[The Internet is forever, Sep 17](#)
10. Update default passwords on devices you acquire, including wireless routers. [Modems and Routers, Jul 17](#)
[Wireless Access, Feb 17](#)

[Go to Index](#)

#40: '5G', Fifth Generation Cellular

Originally published in the February 2019 issue of *Venturing into our Past (JGSCV)*

Top Speed (characters/second)	1G →	2G →	3G →	4G →	5G
	3 hundred	4 thousand	3.4 million	7.2 million	50 million

Verizon and AT&T are introducing the latest wireless cellular technology, labeled “5G” for Fifth Generation. In honor of this milestone, here is a short history of cell phone technology.

While car radio phones go back to the 1940s (remember Humphrey Bogart in “Sabrina”?), the first cell phone was demonstrated in New York City in 1973 by Martin Cooper of Motorola. It would be 10 years before cell phones would be commercially available in the U.S., and then at a very steep price. There are now more than 7 billion cellular capable devices, or approximately one for every person on Earth.



Cell phones were introduced commercially in Japan in 1979 and here in the U.S. in 1983. ARCO provided me with my first cell phone in 1987. It looked like this, weighed several pounds, cost over \$3,000 (equivalent to \$6,800 today), took 8 hours to charge and offered 30 minutes of talk time. With it, the folks at the ARCO data center that I was managing could reach me wherever I was (so long as I was within range of a cell tower).

1G was analog, meaning that sound traveled as analog radio waves to the nearest tower where it would be converted to a digital signal to travel to the tower serving the other party. It would then be reconverted to analog and be delivered to the target cell phone. This technology is no longer used in the U.S. nor most of the rest of the World.

2G came along in 1991. By providing encrypted digital transmission directly from the cell phone, it was more secure, faster and far more efficient. It supported text and picture messages. This technology has generally been replaced by 3G and 4G around the world. In the U.S. AT&T shut down its version in 2017. Verizon and T-Mobile plan to shutter their remaining 2G networks in 2019 and 2020.



3G was introduced in the U.S. by Verizon in 2002. It is faster than 2G, supporting mobile Internet access, video calls and mobile TV technologies. 4G was introduced in 2008. It replaced circuit-switched telephony service with full Internet Protocol. Though this and other technical enhancements it provides faster speeds for enhanced mobile web access, full IP Telephony, enhanced gaming, high-definition mobile TV and video conferencing.

Your cell phone is likely 4G capable, Most areas in and around Los Angeles support 4G. A few areas are still serviced by 3G networks. For example, much of western Malibu, including Point Dume, are serviced by AT&T with 3G. Either is probably sufficient for your use. When I was in Ukraine this past summer, I frequently found myself out of cell phone range. In checking cell phone coverage maps. I found that Ukraine has 4G in major cities, 3G along major routes, and little coverage in much of the countryside. Google “worldwide cell phone maps” and you will see a number of sites offering such maps.

5G is not only faster than 4G, it is likely even faster than your home Wi-Fi. It provides the speed necessary for intense wireless applications, like self-driving cars. 5G is now available in limited areas. The major carriers plan nationwide 5G coverage by 2020. Of course, you will need a 5G capable device and a network plan that provides 5G. See <https://www.cnn.com/2018/12/18/tech/5g-mobile-att/index.html> to learn more about 5G.

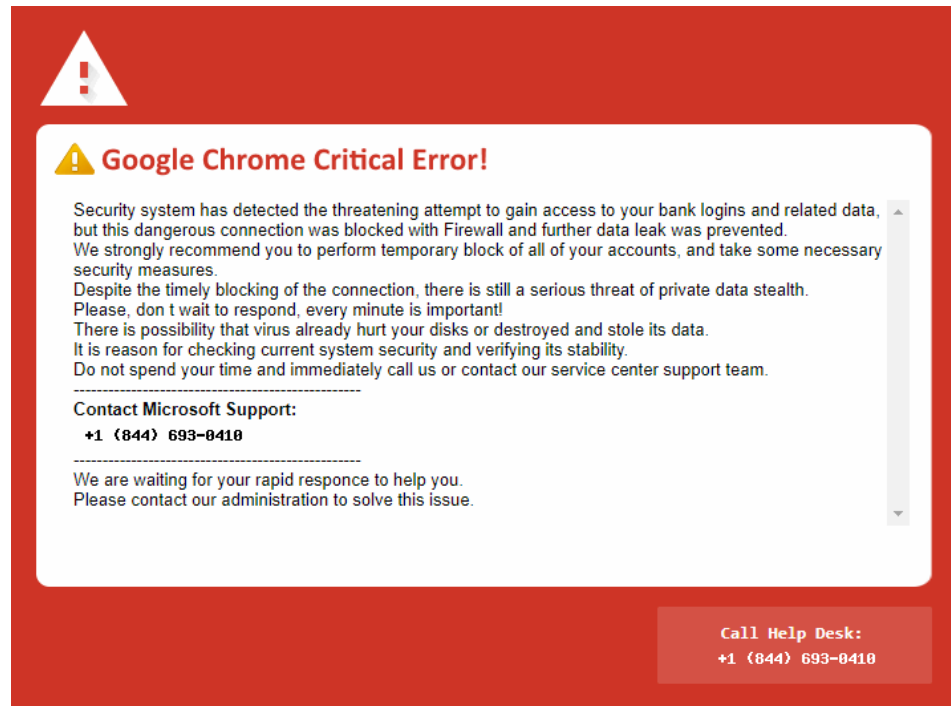
[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#41: Google Chrome Critical Error!

Originally published in the March 2019 issue of *Venturing into our Past (JGSCV)*

Have you ever gotten a screen like this? As you likely suspect, it is a scam. The number is not to Microsoft Support but rather to the scammer who will try to sell you services for your nonexistent problem and seek to obtain your private information. Most believe that they would never be fooled by this. However, these scammers are very good at scaring you and in gaining your confidence.



They may ask to take a look at your system to assess the problem. Granting them such access allows them to implant malware on your computer. Never give another access to your computer unless you have full faith in them. I have given access to staff from my employer's help desk to troubleshoot a problem. But I am hard-pressed to think of anyone else to whom I would grant such access.

This pop-up is triggered by visiting unsafe sites. You may have inadvertently accessed such a site by clicking on a link or mistyping an address. Generally, you are not at risk and should simply close the window. If the malware prevents you from doing so, simultaneously press 'Alt', 'Ctrl', 'Delete' and choose 'Task Manager'. The programs you are running will be displayed. Highlight 'Google Chrome' and press 'Delete'. This will force close the program, not actually delete it. If this does not work, power off and then back on your PC. Generally, the pop-up will not return until you visit another unsafe site.

If you get such a message and wonder if it is real, Google it (go ahead and search for 'Google Chrome Critical Error!'). You will likely learn that it is a known fake message designed to part you from your money and information. You will likely also see sites displayed offering programs and services to clean your computer. Tread carefully as these too may not have your best interest at heart.

There are various clues in this message that it is not real, including not showing the source (though implying it is Microsoft), the sense of urgency, and the fact that the number shown is not that of Microsoft Support (which is 800-642-7676). These messages are invariably fake. Do not fall for them! Never call the number or click on any link on such a warning message. If you want to reach out to Microsoft Support, call them directly and they will surely reassure you that this is a scam.

[Go to Index](#)

#42: Synthetic Identity Theft

Originally published in the April 2019 issue of *Venturing into our Past (JGSCV)*



Synthetic ID theft is where a thief creates a new identity using some of your information, like your social security number and birth date. The Federal Trade Commission (FTC) estimates that as much as 85 percent of all identity fraud involves “synthetic” or fictional IDs. While you can reduce its likelihood, the possibility remains that you will become a victim. So, it is important that you pay attention and then follow up when something seems amiss.

The best way to catch synthetic ID theft is to monitor your credit report closely. If you see anything out-of-the-ordinary, such as addresses you’ve never lived at or jobs you’ve never had, it’s possible you’re a victim of synthetic ID theft. You have the legal right to receive your credit report for free once each year and it is easy to do so. Just go to www.annualcreditreport.com and respond to the quiz. It will ask you such things as your monthly mortgage, rental or car loan payments providing several ranges from which to choose.

Once the system is satisfied that it is indeed you, it will ask you to indicate which of the three credit agencies’ reports you would like. You can choose to view one, two or all three of them. I recommend you choose just one and do this every four months cycling through the three over the course of a year. I put reminders on my calendar to do so (e.g., January: Equifax, May: Experian, September: TransUnion). The credit report will be displayed as a PDF which you can review, print and save. The website includes actions you can take if concerned.

Other things which might indicate possible Identity theft are charges on your credit card statements that you do not recognize or bills that have not arrived. A credit card, utility or bank statement that has not come may indicate that someone has changed your billing address to hide their activities. So, it is vital that you recognize when bills have not arrived and not just react to them when they do.

Of course, it is far better to avoid becoming a victim. The California Department of Justice website shows these “Top 10 Tips for Identity Theft Protection”.

1. Protect your Social Security number.
2. Fight "phishing" - don't take the bait.
3. Polish your password practices.
4. Be mysterious on social networks.
5. Shield your computer and smartphone.
6. Click with caution.
7. Check your statements.
8. Stop pre-approved credit offers.
9. Check your credit reports – for free.
10. Ask questions.

Select <https://oag.ca.gov/idtheft/facts/top-ten> to read more about each of these tips. Additionally, <https://oag.ca.gov/idtheft/information-sheets> provides a number of useful reference sheets about avoiding, recognizing and responding to identity theft.

[Go to Index](#)

#43: Is Windows Defender Sufficient?

Originally published in the May 2019 issue of *Venturing into our Past (JGSCV)*



Windows 10 includes Windows Defender antivirus software. There are no fees to install or operate it and it has a light footprint, minimally impacting computer performance. It also includes a firewall providing protection against malware that might find you. In March 2019, Microsoft changed the name to “Microsoft Defender Advanced Threat Protection” or “Defender ATP” and began offering a MAC OS version alongside the existing Windows version. However, the MAC version is currently only being marketed to businesses. Windows Defender can also run on Windows 7, 8 and 8.1.

Like most of its competition, it relies on both an internal engine to do the scanning and regularly updated signature files of known malware. It runs automatically and cannot be disabled. When you install another antivirus program, it automatically goes dormant, coming alive again if you remove the other antivirus product.

It tests well against other products, catching virtually all malware as the malware attempts to launch. It does have a significantly higher false-positive detection in which it misidentifies and stops perfectly innocent software that it suspects to be malware. While noteworthy, this should still be a minor inconvenience and not a significant disruptive issue.

It has not always been this way. Go back three or four years and Microsoft Security Essentials (the prior name of Windows Defender) tested poorly against the competition. This reputation hangs on and so some just do not trust that a free, easy to use product from Microsoft is all that they need for protection. For most users, Windows Defender is quite enough.

Windows Defender looks for suspicious activity but does not look for indicators that undetected malware might have been active. For example, if a normally static system file has been updated this might indicate the presence of malware. In addition, while Windows Defender warns you that a malicious program is attempting to run, it does not stop you from opting to let it run.

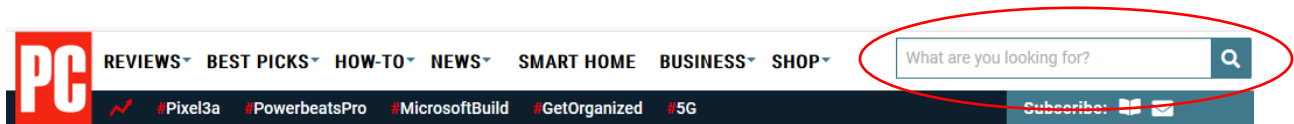
Commercial alternatives may offer additional features such as password managers, VPNs (virtual private networks), or scans to find indicators that malware may have been active. These additional features add to the “bloat” or “footprint” and may result in performance impacts. In considering a commercial alternative check the additional features and satisfy yourself that they are sufficiently valuable to you to warrant the cost and potential performance impact.



If you decide to stay with Windows Defender, consider installing the free version of Malwarebytes. They can coexist since the free version of Malwarebytes only runs when you invoke it (Two anti-virus programs running concurrently may impact system performance). Consider periodically scanning your PC with Malwarebytes, especially if you suspect an issue. You can also use Windows Defender Offline to scan your PC. For more about Windows Defender Offline see, <https://support.microsoft.com/en-us/help/17466>. To download Malwarebytes, see, <https://www.malwarebytes.com/mwb-download>.

[Go to Index](#)

#44: PC Magazine as a Source

Originally published in the June 2019 issue of *Venturing into our Past (JGSCV)*

PC Magazine <http://www.pcmag.com> has all kinds of good stuff that can help you Practice Safe Computing and it is free. It has a search field (shown above) that allows you to find information on most any PC, Internet or technology topic imaginable. The articles are in plain English and do not take a technical degree to read. Based on your interests or the latest news, you might search for articles on “Facebook hacks”, “best notebook computers”, “Google privacy”, or even the “best photo printers”.

When you do you a search, expect to see associated advertisements as well. PC Magazine clearly makes their money through advertising. While I have found good, seemingly unbiased information in PC Magazine, it is always best to do additional research before making important decisions. PC Magazine has several articles on the best antivirus protection for 2019 (enter “best antivirus” in the search field above). There are articles for PCs and MACS, for paid and for free tools. While acknowledging the advances made by Windows Defender (which I wrote about last month) they continue to recommend other solutions, many of which are advertisers. Probably just a coincidence ☺.

An April 2019 article on DNA kits compares 23andMe, AncestryDNA, Living DNA, HomeDNA, National Geographic Genographic Project and MyHeritage DNA. You may find it to be worthwhile even if you have already obtained DNA results and especially if you have yet to test your DNA. You can find it at <https://www.pcmag.com/roundup/356975/the-best-dna-testing-kits>.



Notwithstanding repeated issues regarding Facebook, we still rely on it, as do 2.38 billion Mostly Active Users (MAU) Worldwide. Earlier this year, PC Magazine provided a series of tips on hidden Facebook features. You can find the article at <https://www.pcmag.com/feature/324797/24-hidden-facebook-features-only-power-users-know>. Along with each tip, the article provides step-by-step instructions, often with great diagrams. These are the titles of the tips that the shared article shares:

- | | |
|--|--|
| 1. The Inbox You Didn't Even Know You Had | 13. Turn Off Autoplay Videos |
| 2. See Who's Snooping In Your Account | 14. Embed Public Content |
| 3. Restrict Select Friends from Seeing Posts | 15. Send Money Through Facebook |
| 4. Save Posts for Later | 16. Transfer Files Over Facebook Messenger |
| 5. Download a Copy of All Your Facebooking | 17. Upload '360' Pics and Vids |
| 6. Find All the Photos Liked by...Anyone | 18. Make a Fundraiser |
| 7. Choose a 'Legacy Contact' for After You Croak | 19. Facebook Is a Virtual Arcade |
| 8. Add Some Extra Security | 20. Visit Town Hall |
| 9. Edit Your Ad Preferences | 21. Stop with the Birthdays |
| 10. Block Facebook Mobile Browser Tracking | 22. There Are Lots of Secret Emoji |
| 11. Curate Your News Feed | 23. Upside Down or Pirate Speak |
| 12. See All The Friends You Requested, Ever | 24. Using SMS Texts to Get Facebook Status, Access |

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

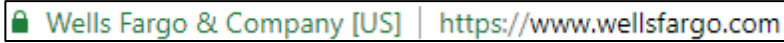
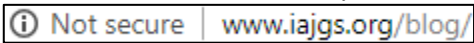
#45: You Likely Need a VPN

Originally published in the July 2019 issue of *Venturing into our Past (JGSCV)*

You have likely heard of Virtual Private Networks (VPNs) and may even use one for your work. Consider obtaining and using a VPN, especially if you use public Wi-Fi on a bus, train, or plane, or in a coffee shop, restaurant, airport, or hotel. While your home Wi-Fi poses less of a risk, it can also be compromised.

A “Private Network” is one that is self-contained, typically within one building or physical campus. VPNs provide an encrypted “tunnel” from a PC outside this network into it so that the PC becomes a “virtual” member of the network. Businesses use this so that employees can work remotely and access systems and data as if they are within the building or campus. A non-business VPN typically provides no systems or data. It does, however, provide a secure, encrypted connection so that no one can spy on you.

Without a VPN, entering the URL itself is unencrypted and subsequent traffic is only encrypted if you attach to a secure website. With minimal technology, an individual can view keystrokes and data that are transmitted over public WiFi without encryption. You can recognize whether a website is secure by looking at the URL displayed in the address field. A secure website will begin with <https://>, rather than <http://> and display a tiny lock symbol. Most sites to which you attach are secure.

If you type in “wellsfargo.com”,  is displayed in the address field. Notice both the lock symbol and “https”. Subsequent traffic is encrypted. Now, type in “iajgs.org”.  will be displayed. Both the message and the lack of an “https” show that your traffic is not secure. Pay attention to the “https”!

If you are not passing sensitive information to an unsecure website, it may not concern you that someone could be spying on you. But, you might not want folks to even know what sites you are visiting. You can avoid this by using a VPN. VPNs encrypt all outbound and inbound traffic, including your initial connection to a web location. You are effectively hidden making spying on you and surreptitiously accessing your PC or laptop significantly more difficult.

There are numerous options for VPN services. Your Internet Service Provider (ISP) likely offers one. You may be able to find a better, cheaper one with a little research. Take a look at these recent articles in PC Magazine: [The Best VPNs for 2019](#) and [The Fastest VPNs for 2019](#). Five VPNs appear on both 10-best Lists: NordVPN, Private Internet Access VPN, TunnelBear VPN, IPVanish VPN, and TorGuard VPN.

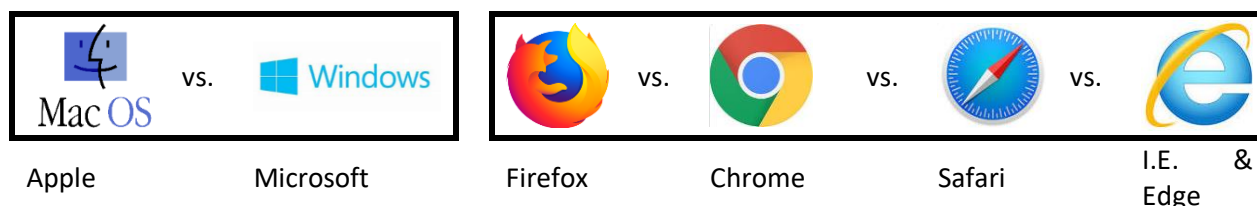
To invoke a VPN once you have installed it on your computer, you would typically click on its icon and enter your password. It then connects to the physical location of the VPN, encrypting all traffic, including the initial connection. Additionally, the sites on the Internet to which you connect will not see your location. Rather, they will see the physical location of the VPN.

If you connect through a public Wi-Fi, you need a VPN.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#46: Apples are also vulnerable

Originally published in the August 2019 issue of *Venturing into our Past (JGSCV)*

On May 26, 2019, Forbes published an article entitled, [“Unpatched Apple macOS Vulnerability Lets Malicious Apps Run -- What You Need To Know”](#). As of the end of June, this flaw was still being reported in various technical publications, including [Wired](#) and [techradar](#).

MACs are less susceptible to malware than PCs. PCs have significantly greater market share and the MAC operating system carries with it less old code that hackers search for vulnerabilities. As of June 2019, Windows is running on 87% of all desktops and laptops while MAC OS is on 10%. While MACs are less likely to be hacked, they remain vulnerable. MAC users should remain alert and have current antivirus software installed, current and running.

<https://www.cvedetails.com> tracks identified vulnerabilities by vendor, hardware and software. While intended for security professionals, it is interesting to look up any product to see the number of vulnerabilities over time. You can even drill down for a description of each. The chart below summarizes data from this website. It shows the number of vulnerabilities found (and presumably fixed) in the Apple and Microsoft operating systems and in the four most common browsers. The 2019 data is through June. The number of vulnerabilities should concern us all.

Year	Apple OS (MACs)	Microsoft Windows (PCs)	Firefox	Chrome	Safari	I.E. and Edge
2010	201	114	106	150	121	1
2011	141	105	101	266	49	18
2012	68	49	163	249	90	128
2013	81	158	149	174	23	243
2014	162	151	108	127	72	231
2015	452	668	179	187	135	156
2016	221	609	133	172	56	214
2017	303	878	1	153	179	277
2018	110	726	333	161	50	201
2019*	116	659	37	173	68	66
Total	1,855	4,117	1,310	1,812	843	1,535

* through June

Apple OS with Safari has had 184 vulnerabilities during the first six months of 2019. Microsoft Windows with Firefox has had 696.

While there are far more vulnerabilities in Microsoft Windows, there were plenty of vulnerabilities to exploit in the Apple OS and in its browser.

Application software (such as Microsoft Word or Apple Pages, Microsoft Excel or Apple Numbers) also contains vulnerabilities. Whatever your device, OS, browser and applications, maintain current anti-malware software and definitely practice safe computing.

Apple users may be overly complacent as to their safety and not realize that along with malware, they are at risk of phishing, where criminals attempt to steal data through trickery. Phishing does not discriminate between MacOS and Windows users. There has been dramatic growth in phishing attacks. Be wary whenever asked to share personal data, to “confirm” your login ID and password, or to, “just answer a few questions for our survey”. More about phishing in a subsequent article.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#47: Windows Updates

Originally published in the September 2019 issue of *Venturing into our Past (JGSCV)*

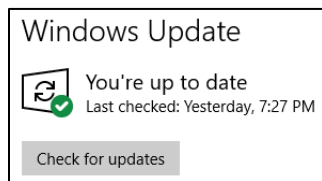
When hackers find a new Microsoft vulnerability, they quickly release malware to exploit it. When Microsoft learns of the new vulnerability, they create patches to fix it. When anti-virus companies learn of new malware, they update their rules to trap it. The race is on. You are at serious risk if the malware gets onto your computer before you install the needed patches and anti-malware updates.

Generally, your computers are set up to automatically check for and install Microsoft patches and anti-malware updates. If this does not work, or work quickly enough, your computer is at risk.

Recently, Microsoft announced that serious vulnerabilities had been found in Windows operating systems, including Windows 7, 8.1 and 10 that could permit hackers to take control of your computer without your knowledge or permission. They strongly advised owners of the 1.5 billion Windows devices Worldwide to download the latest Windows security updates to lock down these vulnerabilities.

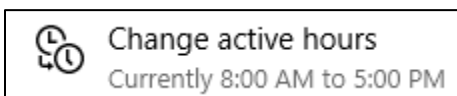


You can easily check if you have the latest Windows updates. First, right click on the Windows 10 icon at the bottom left corner of your screen. Select “Search” and a search box will appear. Enter “Windows” in the search box. As you type, you will see the option “Check for updates” appear in a list of relevant links. Click on it and a “Windows Update” window will appear.

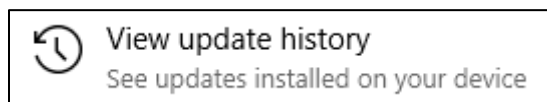


You will see a message like this one that confirms when your computer last checked and obtained the latest Windows updates. If you like, you can have it check now by clicking on the button shown. The check will take several minutes during which time you will be watching a series of green dots chasing each across the screen.

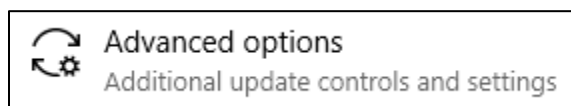
While you are here, check out the other options available on the page.



You can change the hours when you are likely to be using the computer. The computer will then schedule checks for Windows updates outside of these times.



You can view recent updates. I checked and found that there had been 10 during the month of August. Keeping your computer safe is an ongoing challenge!



Under Advanced Options, you can instruct it to check for other Microsoft updates when it checks Windows (like Word, Excel and Explorer). If off, turn it on!

Check out the various **Update & Security** settings. Click on **Windows Security** to turn on the Defender Firewall (see the May, 2017 article in this series, “Malware Protection” for a short discussion about the value of firewalls). Click on **Backup** to schedule automatic backups to attached storage devices. Click on **Recovery** to learn how to reinstall Windows – which may speed up your computer.

If you are on an earlier version of Windows and are not sure how to get to the **Windows Update** screen, Google, “how to bring up the windows x update screen”, replacing the “x” with your version.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#48: Making the most of your Password Manager

Originally published in the October/November 2019 issue of *Venturing into our Past (JGSCV)*



If you are not using a password manager, seriously consider it. They support different complex password for each login site, recognize when you are at a login page and automatically fill in the fields and recognize when you are logging into a new site offering to save the new credentials you have just created.

Most can generate complex passwords, can pass your credentials on to a predetermined heir and can work on any device with information stored in the cloud. They can also be used to store addresses, credit card information, bank account information or any other information that you would like to preserve securely and retrieve safely wherever you are. I have yet to hear of a password manager being hacked. For more background, including the tool I have chosen, please refer to my earlier articles on password managers in the October 2016 and January 2018 issues of *Venturing into our Past*.

Here are PC Magazine's 2019 ratings of Password Managers – click on the links to learn more

[Best Free Password Managers](#)

- 1 LastPass
- 2 Myki Password Manager & Authenticator
- 3 LogMeOnce Password Mgmt Suite Premium
- 4 Symantec Norton Password Manager
- 5 Avira Password Manager
- 6 Bitwarden
- 7 1U Password Manager
- 8 WWPass PassHub
- 9 Enpass Password Manager
- 10 KeePass 2.34

[Best Password Managers](#)

- 1 Zoho Vault
- 2 Dashlane
- 3 Keeper Password Manager & Digital Vault
- 4 LastPass Premium
- 5 RoboForm 8 Everywhere
- 6 AgileBits 1Password
- 7 Password Boss
- 8 Sticky Password Premium
- 9 Bitwarden Premium
- 10 LogMeOnce Password Mgmt Suite Ultimate

If you are using a password manager, you have made a wise decision. But, are you still reusing the same password or just a few or ones that are easy to remember? If so, you remain at risk. Use the power of the manager to create different complex passwords for each site for which you have a login, especially your more sensitive sites like ones which access your financial and medical information.

Consider using your password manager to remember bogus answers to your challenge questions as well. The purpose of challenge questions is to identify that it is really you. As genealogists you know that you can find anyone's mother's maiden name, birthplace or given name. Others know your favorite color, food and vacation spot. You may even be sharing these on social media. The password manager can be a great place to store and retrieve bogus answers to challenge questions. They generally have a comment or notes section for each set of login credential which can be used to record these false answers.

What if you forget the password to your password manager? What if the Password Manager disappears? While this is far less likely, I want to be prepared for anything. So, periodically I print off the contents of my password manager and write down its master password. No, I do not keep this critical information where it can be found. Rather, I put it my bank safe deposit box.

It is not enough to have a password manager. You need to use it wisely.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#49: Data Management and Protection

Originally published in the December 2019 issue of *Venturing into our Past (JGSCV)*

Protecting your data is not optional, so...



1. Maintain meaningful file names and logical folders.
2. Password protect sensitive data files and folders
3. Back up data files automatically and frequently.
4. Maintain both local and remote backups.
5. Periodically, test data restoration from backups.
6. Protect backed up data from exposure.
7. Automatically back up files as you work.



If you find yourself spending time trying to find a specific document, spreadsheet, or picture, consider giving them meaningful, differential file names and grouping them into logically named folders. You might further group all of your data files into one master data folder.

If a family member, employee, guest, workman or intruder were to get into your computer, are there files you would not want them to be able to access? If so, you should [password-protect](#) them. Remember the password or you will not be able to open the file. Consider [encrypting](#) your files for even more protection (However, Windows 10 Home does not support encryption 😞).

Sometimes, programs have hidden components that are created upon installation. So, it is best to reinstall them rather than restoring them from a copy. Focus on backing up data and not programs. Be sure to record the program registration keys that you will need to complete the installation. Record your keys and back them up along with your other files.

Files created or changed since your last backup will not be on the backup and therefore will not be recoverable. So, it is best to have a frequent automatic backup. Backup software is included with external backup disks and backup cloud subscriptions. If you are a bit more adventuresome you can use the [Windows System Backup feature](#) to set this up yourself.

Typically, genealogy program backups are placed on the same internal hard disk as the original. This is worthwhile if the original becomes corrupted. But it is of no use if the disk crashes or the computer is stolen. Maintain a local backup on a separate device (like an external hard drive) and a remote backup, preferably in the cloud. See [The Best Online Backup Services for 2019](#).

Periodically test restoring files from your backup, both to verify that the backup is working and that you know how to recover your data. Take reasonable steps to protect your backups. I periodically back up important files to a USB drive which I keep on a keychain. This drive is encrypted and password protected so if lost, my data is not at risk.

Finally, set up rules to automatically save files as you work. Then, if you close the file without saving it, your system freezes or loses power, your work will be preserved. To learn more, Google, "Autosave Word 2016", "Autosave Excel 365" or simply "Autosave." Important! If creating a new file, be sure to save it when you start your work to trigger the Autosave feature.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#50: Discovering if you have been pwned

Originally published in the January 2020 issue of *Venturing into our Past (JGSCV)*

In one of the most massive recent data breaches, 267 million Facebook users had their IDs, phone numbers and real names exposed. This was confirmed on December 19, 2019.

';--have i been pwned?

Do you wonder if your email or password might have been part of a data breach? <https://haveibeenpwned.com> may let you know.

If you enter your email address you will either see

Good news — no pwnage found!

or

Oh no — pwned!

Along with the number of breached sites and pastes in which your email was found. A “paste” is any of a number of sites in which compromised emails have been published. Each of the breaches and pastes are then described including when the breach occurred and the data fields that were exposed.

Many of these are marketing or sales lead sites. Discovering that your email has been scooped up on one or more of these may be annoying, but is probably not a serious issue. However, if you see a site that you log into or one where the breach exposed IDs and passwords, pay attention. Immediately change your password on any such site AND on any other sites where you use the same password. Once they have your password, they will try it on other sites knowing that we often reuse passwords.

Select the “Passwords” tab at haveibeenpwned.com to see if a password you use has been seen in a data breach. If something common, like “mary123” it has likely come up many times, and not only when used by you (this one popped up 14,157 times). Of course, you should never use easy-to-guess passwords. If a more complex password you use shows up as having been pwned, change it immediately, wherever you use it.

Different, strong, complicated, impossible to remember passwords are best, like “R28t&pPPTx2o”. I just used my Password manager, LastPass, to generate it. I do not need to remember it as the password manager will do so. When I set up (or change) passwords on a site, I bring up LastPass and select, “Generate Secure Password”. I had set it to generate 12-character passwords containing uppercase, lowercase, numbers and symbols. I then paste the generated password into the password field on the form (as well as the “confirm password” field). LastPass recognizes that I have done this and offers to save it along with the other information for that website so that it can log me on in the future.

You can further protect yourself from being compromised by setting up two-factor authentication at the site. Many now offer this, in which they will send a text or voice message to your smart phone which you must then enter to complete your login. This ensures that someone (or some tool) that has gotten hold of your ID and Password cannot log in as you without also having your smart phone to complete the two-factor authentication. Yes, it is annoying. But, weigh this against someone hacking you.

The haveibeenpwned.com website recommends the password manager, “1Password”. It is one of the 10 best as assessed by [PC Magazine](#), as is LastPass, the one I use. All are likely good choices. Read the comparisons and try them yourself to decide which works best for you.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#51: USB recharging cord and Bluetooth Risks

Originally published in the February 2020 issue of *Venturing into our Past (JGSCV)*



Catharine Hamm wrote a piece in the Los Angeles Times on December 1, 2019 entitled [“Beware public USB ports.”](#) The port might be infected with malware and your smart phone likely has little protection from the port passing the malware through the USB cord directly into your smart phone.

You can avoid the risk while at public locations (airports, hotels, restaurants, etc.) by carrying your own power bank to recharge your device or a USB cord with your own power plug to connect to an electrical outlet. For more info, see PC Magazine’s, [“The Best Portable Chargers and Power Banks for 2019”](#).



Most smart phones, tablets and laptops include Bluetooth. It is intended for local data transfers within about 33 feet. By design, others can connect if your Bluetooth is set to “Discoverable”. They could send you messages, malicious functions or links to files containing malware. Be careful in opening any file or invoking any function sent to your smart phone.

Folks tend to be less careful in scrutinizing incoming SMS messages on their smartphone than incoming emails on their computer. Bluetooth hackers may rely on this. So, be just as cautious in responding to an SMS message as you would be in opening and clicking on the contents of an email.

There are a variety of ways a serious hacker could use Bluetooth to put you at risk. Your movements might be tracked, unwanted messages could be sent to your device, and malware could be implanted. Given the prevalence of discoverable Bluetooth devices, incidents of Bluetooth hacking will surely increase. Recently, attendees at a conference of security professionals were advised to disable Bluetooth to reduce the risk of a fellow attendee hacking their devices.

Consider turning off Discovery when you do not need it. To do so, go to your device’s Settings. Find “Bluetooth” and switch off Discovery. Switch it back on when you next need it. I generally leave my smartphone’s Bluetooth in Discovery mode as I routinely use it. So, I am especially cautious when handling or responding to incoming messages.

If you want to read more, see, [“Could Your Bluetooth Devices Be Hacked in 2019?”](#)



Windows hint: To snapshot a rectangular portion of the screen, press the Shift, Microsoft and “S” keys simultaneously. Click on the upper left corner of the area and hold down the left mouse button while you drag the mouse to the lower right corner of the area to be snapshot. Release the button. Now, copy and paste into an email, Word document or other file.

Windows hint: To snapshot a rectangular portion of the screen, press the Shift, Microsoft and “S” keys simultaneously. Click on the upper left corner of the area and hold down the left mouse button while you drag the mouse to the lower right corner of the area to be snapshot. Release the button. Now, copy and paste into an email, Word document or other file.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#52: You've got DNA Matches

Originally published in the March 2020 issue of *Venturing into our Past (JGSCV)*

A few years ago, I submitted my DNA to one site and then uploaded the results to another. Like many of you, I regularly receive notices of "You have new DNA Relatives" from 23AndMe and "You've got DNA Matches!" from MyHeritage DNA. With endogamy (marriages within a group) over the centuries among Ashkenazi Jews, the number of 1.0% to 1.5% DNA matches can be huge while the likelihood of being able to determine an actual relationship is low.

Given the low likelihood of actually establishing a match, I certainly do not want to put a lot of effort into reaching out. Yet, I do not want to ignore potential matches either. With minimal effort, I would like to share enough information to see if a connection can be made.

I composed a message as follows and saved it for repeated use:

Hi xxxx,

xxxx indicates that we share x.x% DNA. I am sharing the names and birth locations of my great-grandparents. If you spot a name/place that seems familiar, please let me know.

Bookbinder & Wagner - Dubno, Rivne Oblast, Ukraine
 Barenberg & Margolis - Medzybzh, Khmelnytskyi Oblast, Ukraine
 Sacharow - Poltava, Poltava Oblast, Ukraine & Cooper - Warsaw, Poland
 Horwitz or Muhlstein & Steinwertzel - Soroka, Moldova

Best,

Hal Bookbinder

hal.bookbinder@ucla.edu



When notified of a potential match on a tree managed by a third party, I replace the first sentence with, "xxxx indicates that I share x.x% DNA with xxxx on a tree that you manage."

I paste the message into my response, replacing the x's. I can send meaningful, individualized notes to a dozen potential mishpucha in a few minutes. My response rate has been about 15%. While most of these turn out to be dead ends, they often lead to interesting exchanges.

If you have submitted your DNA to one site, be sure to upload the results to the other sites to expand your potential matches. You can upload at no cost to Family Tree DNA, MyHeritage DNA, Living DNA and GEDmatch. AncestryDNA does not permit uploading of DNA results from another service.

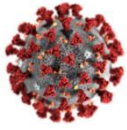
While we must be careful when sharing personal information, I will continue to share ancestors' surnames and locations as widely as I can. On rare occasions, I have been asked follow-up questions that made me uncomfortable and ended the exchange. However, being a genealogist means never giving up. I will continue to respond and keep hoping for additional connections! 😊

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#53: Avoiding COVID-19 Scams

Originally published in the April 2020 issue of *Venturing into our Past (JGSCV)*



Cyber criminals see COVID-19 (coronavirus) as an opportunity to steal your identity, take your money and install viruses on your computer. They believe in Rahm Emanuel's maxim to "never let a serious crisis go to waste." They count on folks acting emotionally, rather than thinking clearly, when such a crisis hits. Some of the reported scams include:

- Emails that appear to come from the CDC (Centers for Disease Control and Prevention) alerting you to "New confirmed cases in your city" and asking you to click on a link to see cases so that you can avoid exposure. You are then asked for personal information, or even asked to log in to what looks like your email page. Your information goes directly to cyber criminals.
- Emails that appear to be from the World Health Organization (WHO) which warn about the dangers of COVID-19 and ask that you click on a link to review the key steps you need to take to protect yourself. While you are reading the list of precautions, a virus designed to steal your personal information is being installed on your computer.
- Cybersecurity firm Check Point announced on March 5th that over 4,000 coronavirus-related domains, containing words like "corona" or "COVID", have been registered since the beginning of 2020. Of those, 120 were considered malicious and another 200 were suspicious. Many will likely be used by scammers. Do not trust sites just because the name sounds legitimate.
- Televangelist Jim Bakker has been ordered by the New York Attorney General to stop advertising "Silver Solution" as a COVID-19 treatment. Shas, the Israeli ultra-religious party has been fined for giving out charms to protect from COVID-19. Undoubtedly, the Internet will be filled with "cures" and "preventions" that are worthless, and worse.
- Amazon said recently that it has barred the sale of over one million products that falsely claim to cure or provide protection against COVID-19. The company has also removed third-party merchants that had engaged in price gouging on items such as surgical masks. These sites may gauge, misuse your personal information and provide nothing of value for your money.

Be on your guard. Do not click on email links unless you are certain that the source is legitimate. If not certain, but believe the information may be of value, close the email and type the website, like www.cdc.gov or www.who.int. Do not click on the purported link in the email as it may be to a mock site that may look real while actually set up to scam you or to infect your computer.

Follow CDC guidelines (www.cdc.gov/coronavirus/2019-ncov/about/prevention-treatment.html) and do not let fear impact your practice of safe computing.

#54: Credit card skimming

Originally published in the May 2020 issue of *Venturing into our Past (JGSCV)*



Even if you hide your keystrokes, you are still at risk of credit card skimming. A few years ago, I found unknown charges on a Visa credit card. I contacted the bank. They removed the charges, cancelled my card and issued a new one. Within weeks, unknown charges showed up on the new card. The bank again reversed the charges, cancelled the card and issued me yet another one. Almost all of the legitimate charges on that card were for gasoline purchases at a specific service station. Figuring there might be a connection, I stopped using the service station and had no further illegitimate charges.

I later learned that some of the pumps at the station were found to have skimming devices. While still around, this is stone age skimming. More modern variants steal your credit card information as it travels through cyberspace or by compromising the records as they are received by a vendor. With the current COVID-19 pandemic we are stuck at home and doing more of our shopping on the Internet. Some are shopping for the first time on-line. So, there is more opportunity for skimming mischief.

Digital credit card skimming happens when malware is injected into a shopping payment page with the goal of stealing credit card information. On March 26, 2020, Security Week reported that, per Malwarebytes (a cybersecurity firm), cybercriminals apparently hacked the Tupperware site and planted malicious code designed to steal payment card information. The malware may have been active for two or three weeks before it was detected and removed.

“According to Malwarebytes, the credit card skimmer planted on the Tupperware website displayed a fake payment form during the checkout process. The form asked unsuspecting users to provide information such as name, billing address, phone number, credit card number, card expiry date, and CVV. Once the information was handed over to the hackers, a ‘session timed out’ message was displayed and the victim was directed to the legitimate checkout page. However, by that time the attackers already had their information.” You can read the full article at <https://www.securityweek.com/credit-card-skimmer-found-tupperware-website>

You can minimize the risk of digital skimming by not entering payment information into numerous sites, sticking instead to one or two major portals that already have your information stored in your account profile. If something seems amiss when entering credit card information, monitor charges on that card carefully.

If your credit card information is skimmed it may be posted on the dark web for sale and then used some time in the future. To read more about the dark web see, [“What is the ‘Dark Web’?”](#). Closely monitor all credit card charges as you do not know if and when you may have been skimmed. Typically, you have 60 days to challenge fraudulent charges. But the faster you recognize and deal with them, the better.

#55: COVID-19 Statistics

Originally published in the June 2020 issue of *Venturing into our Past (JGSCV)*

If you are interested in unbiased Coronavirus information, check out the New York Times' websites. The diagrams, graphs and tables are clear and well organized. The sites are updated each night.

<https://www.nytimes.com/interactive/2020/us/states-reopen-map-coronavirus.html>.

<https://www.nytimes.com/interactive/2020/world/coronavirus-maps.html>,

<https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html>

Television, newspapers and the Internet routinely offer sensationalized and often misleading coverage. I just listened to the story of three states that ended their stay-at-home orders only to see a jump in cases and deaths. The implication is that states that end these restrictions risk substantially more deaths due to Coronavirus.

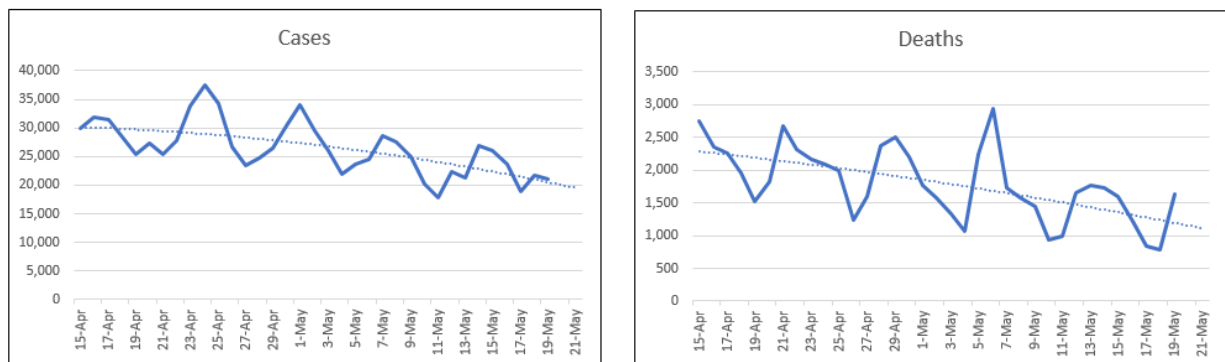
Each day for the past two months, I have extracted detailed information from the New York Times Coronavirus files, graphed the results, analyzed the data and shared this with my hospital coworkers. With 24 years in healthcare information technology, I am keenly focused on healthcare data.

When I examined the nationwide data collected by the New York Times, I found that of the 39 states that ended these orders and have started to open up, 27 have seen fewer Coronavirus deaths while 12 have seen increases. Overall, the death rate has dropped over 10% across these 39 states.

The number of cases (positive Coronavirus tests) has risen about 5% after states ended their stay-at-home orders. However, this may be the result of increased testing rather than increased virus.

The graphs below reflect the data extracted from the New York Times files and show the number of cases and deaths across the U.S. While I cannot predict what the future will bring, the stats over the past six weeks are trending down.

United States COVID-19 Stats, 15-Apr through 19-May



<https://github.com/nytimes/covid-19-data> provides files of daily counts of Coronavirus cases and deaths starting with the first case in Washington State on January 21. Three files are available, one for each of the more than 3,000 counties across the U.S., one for each of the states and one for the overall U.S. These are great sources of raw, unbiased data.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#56: Practicing Safe Zoom

Originally published in the July 2020 issue of *Venturing into our Past (JGSCV)*



The use of video conferencing and especially Zoom has skyrocketed. In December 2019, Zoom reported 10 million participants in Zoom meetings each day. By the end of April, they were claiming 300 million. By now, most of us have participated in Zoom meetings and have seen the stories about uninvited individuals disrupting meetings, often with outrageous and offensive behavior. There have also been concerns about hackers silently spying. Zoom has a number of features to mitigate these issues. The three key features are passwords, waiting rooms, and encryption.

Passwords – Most Zoom meetings now include passwords. Without passwords, a hacker who has learned, or has guessed, the 9 to 11-digit meeting ID can jump in as an uninvited participant. With passwords that differ for each meeting this becomes more difficult. Risks remain as the password for the meeting is a shared one. However, it does reduce the risk. Although you may be asked to enter the password displayed on the invite, I generally see it being incorporated directly into the invite link, making it less of a burden.

Waiting Rooms – When this feature is activated participants appear to the host in a “waiting room” and must be invited in individually or all at once. If the host does not recognize the individual, they can leave the person in the waiting room. The person cannot see, hear, or otherwise communicate with others. Meetings can be set up to allow predefined participants to bypass the waiting room. However, this is more appropriate to business than our avocation.

Encryption – Through encryption, the data streams containing the Zoom meeting are protected from snooping eyes. Zoom has long had strong encryption in its core components (that is, between the Zoom servers). But they only offered end-to-end encryption (between your computer and the first Zoom server) for corporate customers. After significant criticism, Zoom announced that end-to-end encryption would be offered to all Zoom account holders in July.

Other steps a host can take to maintain control include requiring pre-registration, muting some or all of the meeting participants and ejecting unwelcome individuals. The host can disallow muted participants to unmute themselves. Ejected participants cannot reenter that meeting again.

Zoom is popular as it is full featured, easy to use and free for most. However, Zoom security enhancements have, at times, been disruptive. On several occasions, I have been unable to start a meeting, finding that a change had been made since I scheduled the meeting. If you are a meeting host, log in and open the meeting at least 10 minutes early and ensure that everything works.

The widespread use of online conferencing facilities is here to stay. Security will need to keep up with ever more creative hackers. To read more about what Zoom is doing to enhance security, see <https://zoom.us/docs/doc/Ask-Eric-Anything-6-10.pdf>. For a review of Zoom security issues and tips, see <https://www.tomsguide.com/news/zoom-security-privacy-woes>.

#57: Ransomware in the age of COVID-19

Originally published in the August 2020 issue of *Venturing into our Past* (JGSCV)



This is an update to my May 2016 article on Ransomware. Ransomware has shifted over the past four years from locking down data and threatening to keep it locked up or even to destroy it pending receipt of an untraceable payment. Ransomware today does this and also exports a copy threatening to expose the data. This is generally more of an issue for businesses than individuals.

Payments by individuals to release their data continue to run \$300 to \$400. But businesses and government agencies have paid hundreds of thousands. On June 26, UC San Francisco confirmed that it paid \$1.14 million after ransomware locked down several of its School of Medicine servers. Full disclosure: While I recently retired from UCLA, this article is based on publicly available information.

The UCSF ransomware attack used NetWalker. This malware was first noted in 2019 and has been active in attacks at least from March 2020. A number of these attacks have been against medical institutions including those like UCSF heavily involved in COVID-19 research and treatment. NetWalker first exports a copy of the data, then removes shadow copies (also called snapshots) and encrypts the compromised data. So, even if the target organization quickly discovers and halts the encryption, they would not be able to restore it from the now-useless shadow copies and the hackers would already have copies.

The operators of NetWalker then reach out to the victim and demonstrate that they have copies of the data by pointing the victim to a location on the dark web where a partial copy can be viewed. Once payment is received, often using untraceable Bitcoin, the hacker “returns” their copy of the targeted data and provides the victim with the necessary instructions to unlock it. The hackers are generally true to their word as trust is critical to the success of this RaaS (Ransomware as a Service) business model.

While the FBI discourages organizations from paying the demanded ransom, it recognizes that at times when faced with “an inability to function,” payment might be the only option, and “victims should first evaluate all options to protect shareholders and other impacted parties”. For a statement from UCSF on the attack, see <https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf>

In most cases, ransomware gets onto your computer through email attachments or websites that you visit. To lessen the likelihood of becoming a victim, follow standard, safe computing practices, including deleting suspicious emails, not clicking on links unless certain that they are safe, staying away from dangerous websites and maintaining current antivirus software. Do not let your guard down.

Even if careful, you may still be a victim. So, be sure to regularly backup your data to devices physically separate from your computer. Also, create and maintain a recovery drive so that, if necessary, you can reestablish a clean computer onto which you can reinstall your programs and download your backed-up data. While this will not be quick or fun, it is best to be prepared. Not sure how to do this? See <https://support.microsoft.com/en-us/help/4026852/windows-create-a-recovery-drive>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#58: Vishing (Voice phishing)

Originally published in the September 2020 issue of *Venturing into our Past* (JGSCV)



Scamsters are after your personal information and your money. Whether it is phishing on your computer or vishing on your phone, the goal is the same. You likely think that you would never be fooled by such obvious cons. However, more folks than you imagine have been taken and are too embarrassed to admit it. We were brought up in a more trusting time. Scamsters are experts in human engineering. They know how to connect, to build trust and create urgency and fear. They are very good at what they do. Do not underestimate them.

- **Relationship** – Scamsters may use their skills to create an apparent bond. They may share their own fears and hopes. They may share things that they have in common with you. Maybe they have a Jewish-sounding surname or drop a Yiddish expression. The goal is for you to let down your guard.
- **Known Entity** – Scamsters may represent themselves as being from a company, governmental entity or other organization that you know and trust (or fear). They are usually quite convincing. Anyone may say that they are an IRS or postal investigator or from the fraud alert group at your bank.
- **Fear** – Scamsters “from the IRS” may threaten you with a huge penalty or jail. Scamsters “from the power company may threaten to cut off your power. Scamsters from “the police of a foreign country” may threaten to jail, or not to release, a friend or relative. The goal is to rattle you.
- **Greed** – A scamster may inform you that you have a government payment on hold, that you have a package at FedEx, that you will be paid \$100 to complete a survey or help them catch a bank employee who has been stealing. or of course, that you have won some prize.
- **Urgency** – Scamsters almost always rely on urgency. Action must be taken immediately or there will be dire consequences or an amazing opportunity will be lost. By creating this urgency, they hope you will not stop and question things.
- **Immediacy** – Scamsters demand payment now, using purchased cash cards, debit cards, wire transfer or bitcoin. Credit cards, checks and the US Mail are too slow. Of course, the alternatives they require mean that your money will not be recovered and they will likely not be caught.
- **Identification** – Being asked to identify yourself by providing information such as birth date, account number, address, social security number, “your secret word”, or any other personal information should alert you that you are being reeled in. Do not fall for it.
- **Verification** – Scamsters know that you may be suspicious and want to check them out. So, they may provide you a phone number to call. The automated call tree and eventual “representative” sound legitimate. They are not. Always verify by looking up the number yourself.
- **Confidentiality** – You may be informed that this is a special, delicate situation that demands confidentiality. If you bring anyone or any organization into the picture, the opportunity will be gone or there will be dire consequences. They want to be your only source of “truth.”
- **Repetition** – Once a scamster has taken you, they may well return in the guise of an official to help you recover what you lost or as the same person with a convincing story as to why things did not work out before but with some more effort, and money, they are guaranteed to work out now.

The scamsters are experts at manipulation. They have done this successfully with uncounted smart and sophisticated people. Be careful. Step back and whatever you do, do not provide personal information or money. Do not try to outsmart them. Just focus on not getting reeled in.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#59: We are holding a package for you
Originally published in the October 2020 issue of *Venturing into our Past* (JGSCV)

I just received the following two texts on my smart phone (these are the exact texts)...



I immediately went to my browser and Googled, “urgent alert for your USPS package” and “we came across a parcel from June pending for you.” You can likely guess the results.

“HORRY COUNTY, S.C. (WMBF) – The Horry County Fifteenth Circuit solicitor is advising residents to be on the lookout for a text scam circulating to get their information. According to a post on the solicitor’s Facebook page, the text message appears to be from the U.S. Postal Service with a link saying a package is being delivered. Solicitor Jimmy Richardson said he reached out to the USPS fraud investigators after he received a text four times about a package being delivered to him. USPS officials said the text is a phishing scheme to get information from individuals as soon as they click the link. According to the USPS, they will not send text messages to people unless they had previously signed up for such messages about a particular package delivery.”

There have been several similar stories from newsrooms around the country. People routinely fall for these postal, FedEx, or UPS delivery scams. Once you go to the link, you will be asked to identify yourself by providing things like your full name, mailing address, driver’s license, date of birth and a major credit card “for identification purposes only.”

You might be instructed to call a legitimate looking number, which may even appear to be in your own area code, subtly gaining your trust. The person you speak to is friendly, sympathetic and very believable. When you say that you were not expecting a package the caller convincingly explains to you that it looks like a gift.

With your personal information they are able to start making charges in your name, steal your identity or sell your personal information on the dark web. They may have even downloaded a virus. As you wait for the delivery it dawns on you that this might not be on the up-and-up. Trust that inner voice.

Today, we order more and more for home delivery and may even forget exactly what we ordered and when. Scam artists depend on it. Google the text you just received. You will almost always learn that it is a scam. Verify legitimacy before providing your personal identifying information, not after.

If you do fall for this scam, take immediate action. Freeze your account and carefully watch all charges. See previous articles for additional steps that you can take. Reporting the scam is promoted as your civic duty. But, better not to have been taken in the first place.

[Go to Index](#)

#60: Misleading Google Results

Originally published in the November 2020 issue of *Venturing into our Past* (JGSCV)



When you search with Google, the first few links shown are often paid ads. Placement below is based on secret and ever-changing criteria. Some sites may suddenly disappear or are pushed down off the top page as Google's criteria change. Sites pay to be at the top of the list because they know that folks most frequently choose the top one displayed. This can be an expensive mistake.



AnnualCreditReport.com is a free service that permits you to view your credit reports from Equifax, Experian and TransUnion. By law, these

agencies are required to allow one free annual download of your credit report. Recently all three agreed to permit one download each week through April 2021.

Being able to obtain your Credit report for free pretty much as often as you would like is great – even if this may be a marketing ploy to get folks hooked on frequent access. In preparing to share this, I typed “AnnualCreditReport” into Google. The first three items returned were entitled:

1. “Annual Credit Report - Official Credit Report” and linked to freescoreonline.com,
2. “Annual Credit Report - 3 Bureau Credit Report” and linked to freescoreonline.com
3. “Annual Credit Report.com - Home Page” and linked to AnnualCreditReport.com

The first two take you to the same commercial site that requires your credit card and will start charging a monthly fee of \$29.95 if you do not cancel within the 7-day free trial period. While they are labeled as “Ads”, they expect that many will not pay attention. Some will then decide to purchase their services or accept the free trial and neglect to cancel in time to avoid being charged.



To pay a bill from QuestDiagnostics I searched for “QuestDiagnostics bill”. The top site displayed was, “QuestDiagnostics.com Bill - Pay Bill Online” and linked to a page within doxo.com that looked very much like a QuestDiagnostics payment page. doxo.com is a legitimate third-party payer that is not associated with QuestDiagnostics.

The actual QuestDiagnostics site, questdiagnostics.com, is the second one listed. It would be easy to mistake the first site as the official one. In checking out the doxo site I found that they would add \$3.99 to my bill as a service fee and take three days to process my credit card payment. I paid the bill at the actual QuestDiagnostics site where payment was immediate and there was no service fee.

doxo has been sued for trademark infringement for deceptively appearing to be the company's official payment site. Customers, would then complain to the companies about the service fees. doxo displays advisories that they are a third-party payment site. But folks often do not pay attention.

Take care when selecting a link from among those returned by Google. Be certain that it is the site you actually want. In considering a third-party payer site be sure to review its terms and conditions to be sure it is your best option - it certainly was not for me! It is easy to make an expensive mistake.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#61: “Ten Software Fixes

Originally published in the December 2020 issue of *Venturing into our Past* (JGSCV)



If you are experiencing a computer problem like a function that is no longer working, a page that you cannot access, a website that is acting strangely, or a program that is frozen, one of the following ten fixes may resolve the problem.

1. If you have a more than a handful of windows open, close those that you do not currently need. Each open window reserves a portion of memory and problems sometimes result from a lack of available memory.
2. Clear the cache related to the browser you are using. Recently used data is stored in cache. Sometimes this creates problems when the cached data is out of date. For more see, <https://www.pcmag.com/how-to/how-to-clear-your-cache-on-any-browser>.
3. Close the browser and open a different one, say Chrome to Firefox or Firefox to Edge. Each browser has its own cache. Additionally, a specific browser may become corrupted and need to be reinstalled. Having an alternate browser is free and easy to install.
4. If a specific application is frozen, press CNTL-ALT-DEL and select “End Task” for any application that you would like to force to close.
5. Restart your PC. This resets all transient values. Cache that is stored on disk is not deleted. Restarting your PC solves a multitude of problems and so often is the first thing that support folks suggest.
6. Clear your cookies. They contain data used by websites that you visit and are generally not cleared when you close your browser or restart your computer. The link to instructions for clearing cache above also provides instructions for clearing cookies.
7. Run a virus scan to see if it identifies any malware that might be lurking in your PC and creating problems. Your anti-virus software likely has the ability to run an immediate scan at your request. If not sure how to do this, check with your anti-virus vendor.
8. If the problem seems specific to a particular application, uninstall and reinstall it. This will result in a clean copy, reset to default values. Search “Programs” to uninstall. Be sure to retain the application’s installation key so that you can reinstall the application.
9. Check for any displayed alert symbols indicating that access is being blocked. Click on the symbol. It may inform you that the site does not appear to be a trusted one and ask you to confirm whether it can be trusted always, just this once, or not at all.
10. When the computer is running well, take a snapshot of its security settings. If you are having problems, see if the settings have changed. Sometimes they are adjusted behind the scenes. To view these settings, search “Settings” and then select “Security”.

Cache hint: If you suspect that the web page you are viewing is out of date, you may be looking at an older version in your cache. To load the current page, press the F5 key.

#62: Reducing the Impact of Data Breaches

Originally published in the January 2021 issue of *Venturing into our Past* (JGSCV)



On Monday, November 30th, the “blackShadow” group revealed that it had hacked Shirbit, an Israeli insurance company. “blackShadow” tweeted photos of ID cards, driver’s licenses and forms containing private information. The next day the Jerusalem Post quoted a leading hacking expert that “there have been multiple successful cyberattacks against Israeli infrastructure in the past year that have not been revealed to the public.”

“blackShadow” demanded payment of 50 bitcoin (\$961,110) or it would continue to release hacked data. Each day, it posted significant amounts of data and doubled its price. Shirbit publicly refused to pay and the Israeli government acknowledged it was unable to stop the release of data. It encouraged Israelis to obtain new ID cards and driver’s licenses. Then, on December 6th, the reporting abruptly stopped. One wonders what might have taken place behind the scenes.

U.S. laws require that organizations report data breaches to the impacted individuals and in larger breaches to the government. You can scan a list of 500 significant 2020 breaches of Personal Health Information (PHI) at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. How many organizations actually comply and how many quietly pay off the hackers is anybody’s guess. But, be assured, eventually, your data will be exposed. Take these steps to lessen the impact of the inevitable breach.

1. Use different IDs and passwords for your accounts. Hackers know that many use the same IDs and passwords. So, when they discover this information at one site, they will try it on others.
2. Use dual authentication where offered and consider shifting from organizations that do not offer it. In dual authentication, a message is sent to your smartphone for your confirmation. So, a hacker would also need to have your device to be able to access your account.
3. Monitor your credit report and review your credit card, investment and bank statements to ensure that no unauthorized transactions have occurred. Notice any missing credit card or utility bills.
4. If notified that your data was part of a breach, update your password and change it at any other site where you have used that password. Redouble your efforts to monitor your credit reports. Accept any offer by the organization to pay for credit or identity monitoring services.
5. Check <https://haveibeenpwned.com> to see if your email and password can be found for sale on the dark web. The results will only be meaningful if you use strong passwords that others are not likely to have used as well. Change compromised passwords.
6. Consider placing a credit freeze with the three credit reporting agencies. This restricts access to your credit report, which makes it more difficult for identity thieves to open new accounts in your name.
7. Consider signing up for a credit or identity monitoring service that will alert you if your data has appeared on the dark web or someone has used your information to open a credit account.

For additional guidance, see <https://www.gao.gov/assets/700/697985.pdf>.

[Go to Index](#)

#63: Using Zoom to Create a Personal Video Message

Originally published in the February 2021 issue of *Venturing into our Past* (JGSCV)



Recently I was invited to create a short video tribute for a cousin who had passed away. The funeral home would be live-streaming the service. I used Zoom to create a 90-second tribute to be shared at the memorial service.

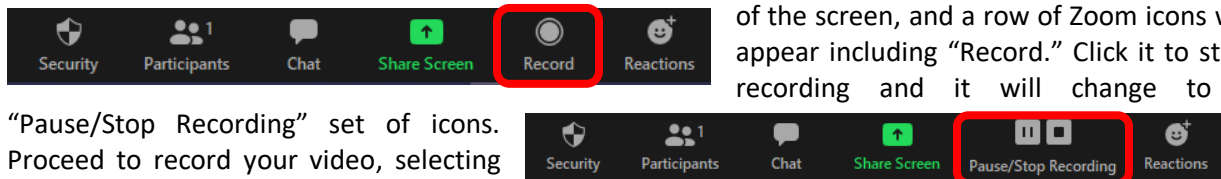
You have certainly seen the “Record” button on the bottom of the screen when in a Zoom session. If you clicked on it, you were likely informed that only the host can record. You can host your own one-person Zoom session to create a self-video.

Sharing the video will generally require you to upload to the cloud, say to a [Dropbox](#) folder and provide a link to the person or persons with whom you would like to share. These video files are typically too large to email. My 90-second video is 22 MB.

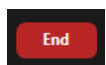
To get started, go to the <https://Zoom.us> website. If you do not have a Zoom account you will need to create one. Click on “SIGN UP, IT’S FREE”. If you have a Zoom account, log in. Now, hover over “HOST A MEETING” in the upper right corner of the screen. Select “With Video On”. Click “Open Zoom Meetings” in the dialog box that will appear at the top center of the screen. If the dialog box fails to show, click “Launch Meeting” in the center of the screen.

Select “Join with Computer Audio” and you are in a Zoom session alone. Bring your cursor to the bottom of the screen, and a row of Zoom icons will appear including “Record.” Click it to start recording and it will change to a

“Pause/Stop Recording” set of icons. Proceed to record your video, selecting “Stop Recording” when done.



Once you click on “Stop Recording”, a message will be displayed in the upper-right corner of the screen letting you know that an MP4 will be created “when the meeting ends.” To record another video, select “Record” again. You can do this as many times as you like. So, if you are dissatisfied with a recording in progress, you can quickly terminate it and start over.



When you are finished, bring your cursor to the bottom of the screen to reveal the Zoom icons again and click on the “End” button, selecting “End meeting for all.” A pop up will alert you that “Recording is in Progress.” Zoom is now creating the MP4 video file(s). Once it completes, you will be given the option of selecting a folder for the video(s). If you just press the “enter” key it will default to the Documents folder, Zoom subfolder.

In the destination folder you will find two files for each time you started and stopped recording, an M4A audio file and an MP4 audio/video file. A 90-second MP4 will take a couple of minutes for Zoom to build. A 45-minute video could take 30 minutes. Be patient. For more help see <https://support.zoom.us/hc/en-us/articles/201362473-Local-recording>.

#64: Private Browsing

Originally published in the March 2021 issue of *Venturing into our Past* (JGSCV)



You purchase a product and almost immediately see pop-up ads for similar products. “If the product is free, you are the product.” You are certainly aware that free Internet browsers monetize your use by selling information about your online habits. Per Statistica, Google Chrome has 48% U.S. market share, Apple Safari has 35%, Microsoft IE and Edge have 7% and Mozilla Firefox has 4%. All are free because your information is a valuable commodity.

This article from the Electronic Frontier Foundation explains how Google monetizes your browsing habits while being able to legally assert that it is not selling your information, <https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and>

There are things that you can do to reduce your exposure while browsing. First, always use the “private” mode when on a shared or public computer and close the browser window or session when done. Otherwise, the computer may retain information that others might be able to access. Generally, you would not want to use private mode on your own computer. This will clear your cookies and cache removing preferred Internet settings and may even slow future access.

Second, if available, turn on the “Do Not Track” option in your browser. This simply requests websites not to gather data on you. It is voluntary and ignored by many websites. However, as some websites still respect it, it affords some protection.

Third, choose the most secure browser that you can. RestorePrivacy rates FireFox number one, calling it “a great all-around browser for privacy and security.” But, don’t get too comfortable. You need to configure its security settings. They advise, “Be sure to disable telemetry in Firefox, which collects ‘technical and interaction data’ and also ‘install and run studies’ within your browser.” Here is their step-by-step configuration guide: <https://restoreprivacy.com/firefox-privacy/>

Fourth, run your browser within a Virtual Private Network (VPN). This will make it more difficult for others to track your online activities by masking your Internet ID and location.

Additionally, if your browser has a pop-up blocker turn it on. If it does not, consider installing one. This will not stop browsers from tracking you and using your information. But it will suppress at least some of the annoying ads that are displayed as you browse.

Browsers must pay the bills. They do this by providing advertisers with access to you for a fee, a multibillion-dollar business. Additionally, when you use a search engine (like Google or Bing), a social network (like Facebook or YouTube) or any other application on the Internet, they may, and likely do, collect information on you, your activities at their site and potentially even well beyond their site.

Too invested in Chrome? Consider adding Firefox, configuring it for security, and using it when you do not want Google tracking your every move. No browser can guarantee 100 percent privacy protection. But you can take steps to reduce your exposure. Read the security policies, choose wisely, configure privacy settings on whatever browser you use, and do consider installing a VPN and a pop-up blocker.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#65: Looking your best while on Zoom

Originally published in the April 2021 issue of *Venturing into our Past* (JGSCV)

We have all observed others on Zoom sessions who look awful, their face is so dark you can hardly make them out, the camera is pointed at their chin or forehead, or way too much of their fingers are shown as they adjust the camera. Here are some tips to look your best while on Zoom.

**Good lighting**

- Your face should be well lit from the front. Try to arrange things so that the windows are in front of you rather than behind you. If you cannot do this, consider a blackout curtain.
- Set up lighting so that it brightens your face and does not cast shadows across it. Shadows on your face are unflattering and may make it difficult for others to see you.

Camera angle and distance

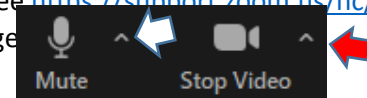
- Set up the camera so that it is slightly above your face. Angles from below are rarely flattering. If using a laptop or smartphone consider setting it on top of a few books.
- Select a distance from the camera so that your image is well sized. Avoid being so far away that you are lost in the furniture and background.

Avoid distractions

- Ask members of your household to avoid doing things behind you. As you are looking at the screen, you may not realize what is happening behind your back.
- Consider setting up a virtual background to minimize distractions. Not sure how? Refer to <https://support.zoom.us/hc/en-us/articles/210707503>
- Mute your microphone when you are not speaking. We all know how annoying dogs barking, phones ringing, whispered side conversations and background noise can be.

Settings and technical considerations

- Adjust the video settings (➡) to improve your image. For ideas, see <https://support.zoom.us/hc/en-us/articles/115002595343>. This is also where you can add or change your profile picture.
- Test the audio (🔊) to ensure that you can hear and be heard.
- Set a profile picture to display when you turn off your video. Not sure how? Refer to <https://support.zoom.us/hc/en-us/articles/201363203> (Remember to sign into Zoom before clicking on the meeting invite so that your profile picture will be displayed when your video is turned off.)
- Ensure adequate bandwidth to avoid an unstable connection. Ask others in the house to put off streaming videos or otherwise eating up bandwidth while you are on Zoom.

**And, never forget that you are on camera!**

- Check yourself out in the mirror before the Zoom session.
- Display your own image while in the Zoom session and occasionally glance at it.
- Feeling drowsy? Turn off your video and mute your microphone.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#66: Yet Another Data Breach!

Originally published in the May 2021 issue of *Venturing into our Past* (JGSCV)



A huge security breach occurred in December 2020 and January 2021 that puts you at risk and you have probably never even heard of it! Accellion is a data security company whose software is used by thousands of universities, government agencies and private companies to safely transport their most critical and sensitive data.

Hackers discovered a flaw in the software and quietly copied massive amounts of data. They have since posted portions of it on the dark web, demanding payment to stop the release of more. The stolen data includes personal information, like social security numbers, medical records and financial records.

Accellion quickly created patches and distributed them to organizations using its software. They encouraged clients to shift to its replacement product which they claim is more secure. They brought in outside experts who confirmed that all “known” flaws had been fixed. But the damage had already been done with the data in the hands of the hackers.

Organizations are slowly realizing the extent of the breach. On March 31, 2021, The University of California posted, “UC has learned that it, along with other universities, government agencies, and private companies throughout the country, was recently subject to a cybersecurity attack....in which an unauthorized individual appears to have copied and transferred UC files by exploiting a vulnerability in Accellion’s file-transfer service.” UC offered free credit-monitoring services to those impacted. <https://ucnet.universityofcalifornia.edu/news/2021/03/uc-part-of-nationwide-cyber-attack.html>

How many of Accellion’s clients were impacted is anyone’s guess. However, I would encourage anyone to act under the assumption that their medical, banking, employment and tax records may have been compromised. As I have written in previous articles, there is not much you as an individual can do to avoid being a victim of such breaches. But you can take measures to minimize the damage.

1. Be cautious if contacted by any bank, insurance company, the IRS or other entity and satisfy yourself that the contact is actually from the organization before taking any directed action.
2. While you will need to make your own decision, I would simply delete any email that demands money stating, “Your personal data has been stolen and will be published.”
3. Never click on the link in an email that you did not explicitly request, no matter how legitimate it appears. You do not know where it is really taking you.
4. Carefully monitor your credit card and other financial statements for signs of fraud and promptly take action if you find anything that you did not authorize.
5. Periodically access your three credit reports at <https://www.annualcreditreport.com> and satisfy yourself that all accounts and balances are legitimate.
6. If you are using the same ID and password for multiple accounts, change them so that a breach in one does not put the others at risk. Use an automated password manager.
7. Accept an offer of a free year of credit monitoring services that will often come from the entity you trusted to protect your data.

[Go to Index](#)

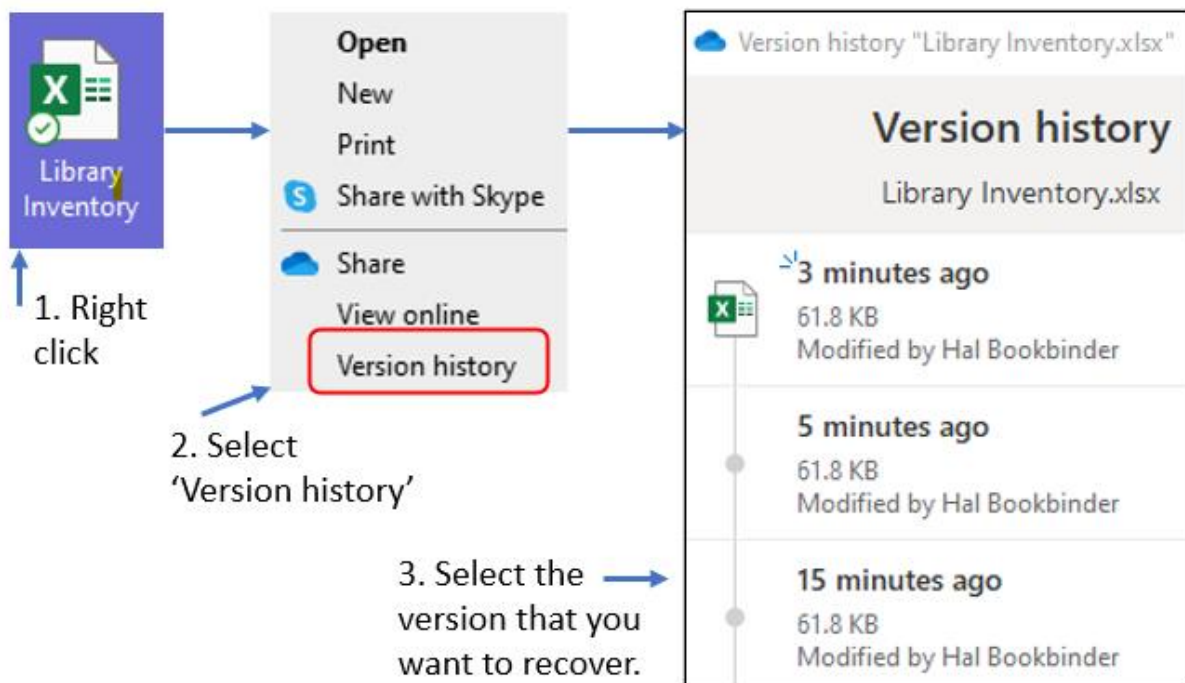
#67: Recovering files using OneDrive

Originally published in the June 2021 issue of *Venturing into our Past* (JGSCV)

File backups typically take copies of files that have changed since the prior backup. The new backup replaces the prior one. While This supports recovery of deleted files, it does not provide for restoration of earlier versions of files that you still have and have since overlaid. Windows 10 OneDrive supports such restoration.

If OneDrive is active and a file is stored in the Documents folder, the Pictures folder, or on your Desktop a copy is taken each time you update the file. These copies are saved in the cloud. To recover one of these prior versions, right click on the file name or icon and select “Version history”. Each of the prior versions, including the one you saved 5 minutes ago that has now been overlaid by a version from 3 minutes ago, can be restored. If you move your cursor to the right of the version that you want to restore, three dots will appear. Click on them and you will be given two choices, “Restore” and “Download”. The first will overlay the current version. The latter will download a copy.

Recovering an earlier version of the Library Inventory file on my Desktop is as easy as 1 – 2 – 3.



OneDrive is included with Windows and so you likely have it on your PC. It currently includes 5 GB (5 billion bytes) of storage at no cost. Of course, Microsoft hopes that you will buy additional storage. Five GB has met my needs for version backup. Try the above with a file on your Desktop to verify that OneDrive is running on your computer. If it is, you will see the above sequence. If you would like to learn more about OneDrive, including activating it, pausing it, changing which files are synchronized and removing it, see <https://support.microsoft.com/en-us/onedrive>.

As OneDrive synchronizes the files on your computer with its cloud backup, deleting a file on your computer results in all prior versions being deleted from OneDrive. However, OneDrive will permit you to recover deleted files for up to three months before permanently scrapping them.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

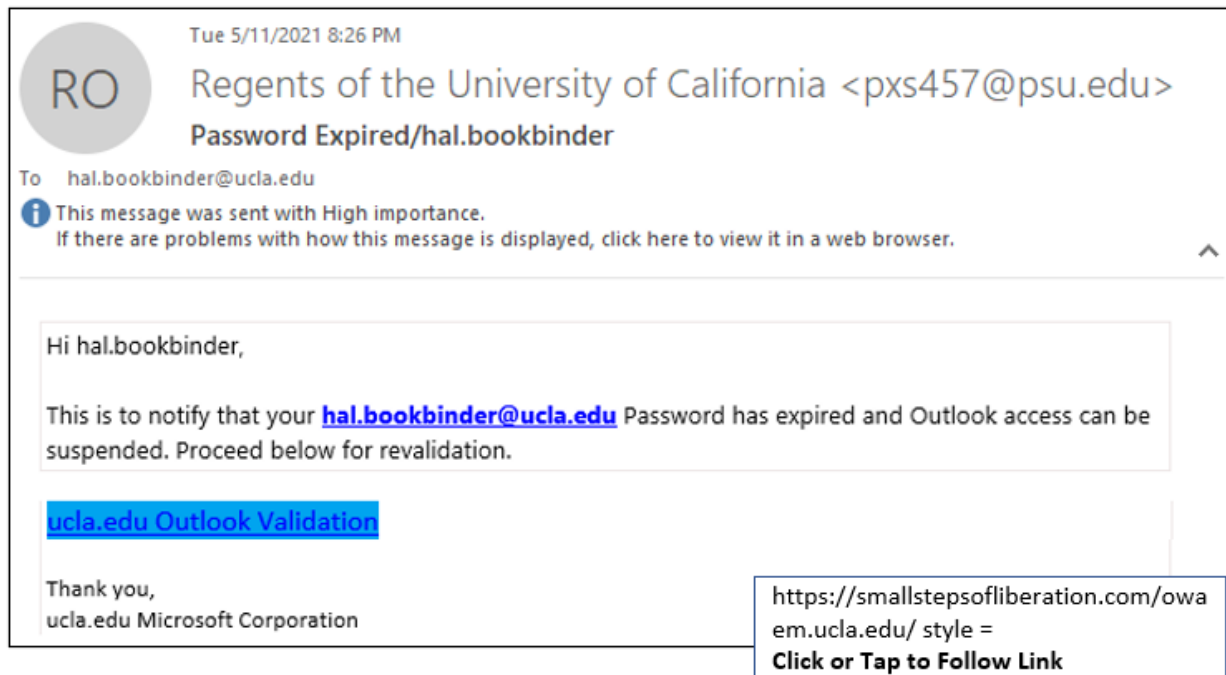
#68: Protecting your credentials

Originally published in the July 2021 issue of Venturing into our Past (JGSCV)



Be cautious when notified that your password has expired or has been compromised and that you must immediately change it.

Having worked for UCLA for 24 years and as a retired UCLA employee, I routinely receive emails from the University. However, this email from the “Regents of the University of California” is bogus. ‘psu.edu’ is not even a University of California domain. In fact, the domain ‘psu.edu’ belongs to Penn State University. It appears that a cybercriminal found an exposed Penn State email address and spoofed it.



When I hover over the link, [ucla.edu Outlook Validation](#) this is what pops up.



If I had gone to the link, I would have been presented with an official-looking page to update my UCLA credentials. I would be asked to identify myself by first entering my current ID and password. Likely, it would then display an “error message” letting me know that my request could not be processed and to try again later. All this would look quite official.

You know the punch line; cybercriminals now have my actual ID and password. Be suspicious of any link in an email you did not request. Before you click on it, hover over it to see where it will actually take you. Then, DO NOT DO IT! If you feel it might be legitimate, close the email and log into the site as you would normally do so and only then update your credentials.

If you do fall for it (and you are not the first and will certainly not be the last), immediately go the site whose credentials you just gave away and update your password. If you use that password on any other sites, update them as well. Don’t wait for the criminals to sell your credentials on the dark web!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#69: Even an 8-year-old Yahoo breach can bite!

Originally published in the August 2021 issue of Venturing into our Past (JGSCV)

Really bad passwords	
123456!	iloveyou
qwerty	15May1951
passw0rd	Mary&Joe

Michael Hiltzik, a columnist for the LA Times, wrote an article on July 11 about Fran Finnegan and his company, SEC Info. This company provides quick access to financial documents filed with the SEC. Just before the July 4 weekend, his system was breached by Russian hackers who encrypted all of its data.

The hackers did not use some newly discovered software flaw to accomplish this. Rather, they used Finnegan's Yahoo email password which had been exposed eight years ago in a massive breach. He used that same password in managing his website. The lesson here is that an old breach can still bite.

Most of us have Yahoo email accounts. We may not have used the account in years and may have even forgotten that it exists. I did. I searched in my password wallet and saw that at some point I had updated my Yahoo password. However, I could have as easily neglected to do so.

If you have unique, strong passwords on each website, you will only be exposed if cyber criminals successfully hack that website. If you reuse the same password or variants of it, ("Mojave6!", "Mojave7#", "Mojave8%") you are at risk if hackers breach any one of your sites.

If you cannot remember when you last changed your Yahoo password, do it now. If you used it, or a variant elsewhere, change it there as well. Hacking software may attempt millions of variations and so changing the number and symbol is not enough.

Ensure that you have unique, strong passwords on your social media and email accounts as well as your financial and health accounts to avoid having your email hijacked, the information you want to share only with family and close friends exposed, your financials compromised, or your data encrypted with a bill to unlock your system from the cybercriminals to be paid in bitcoin or gift cards.

Folks reuse easy-to-remember passwords to make their lives easier. However, when cybercriminals get hold of them the impact can be severe. Better to be inconvenienced with different, strong passwords along with a password manager to keep track of them all.

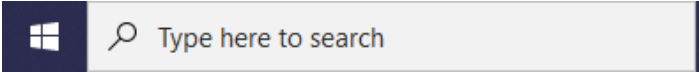
Password managers remember your passwords and will typically generate strong ones on request. I have used the free version of LastPass for years. I will continue to use it even though it did not make PC Magazine's 2021 list of the best free password managers. To read their assessment see: <https://www.pcmag.com/picks/the-best-free-password-managers>

You can read Hiltzik's article at <https://www.pressreader.com/usa/los-angeles-times-sunday/20210711/281560883794400>

[Go to Index](#)

#70: Windows Ease of Access – Vision Support

Originally published in the September 2021 issue of Venturing into our Past (JGSCV)

Ease of Access Vision Display Mouse pointer Text cursor Magnifier Color filters High contrast Narrator	Windows provides features for individuals with sight and hearing limitations to better access their computers. In this article I will focus on vision support. To start type “Ease of Access” in the Windows search box at the bottom left of the screen and press enter. The options shown to the left will be displayed.  Select Display to adjust the size of text or the size of everything. Note that not all text is recognized by Windows as text, including text in a picture or in a PDF and such text will not be increased by simply adjusting text size. Adjusting the size of everything, however, will increase the size of such imbedded text. Select Mouse pointer to adjust the size and color of the cursor and so make it easier to find and control. A slider bar is provided to adjust the size and options are provided to display a white, black or color cursor. Select Text cursor to adjust the size and color of the cursor which displays as you type. It is typically a thin black vertical line that can be easy to misplace. You can adjust its size, color and thickness. You do not need to adjust the Magnifier settings. By default, this powerful tool is available. To invoke it, at any time press Win and +. A pop-up will display. Select + in the pop-up to magnify the screen and - to return to normal size.
--	---

The **Magnifier** can also launch **Narrator** to read aloud text on the screen. Select the text to be read by dragging the mouse across it while holding down the left button. Select **►** in the magnifier pop-up and the text you identified will be read aloud. You can click on the **⚙** to change the voice or reading speed.

The **Color filters** permits you to reverse text and so display white text against a black background. Settings are also available to assist with red-green or blue-yellow color blindness.

Turning on **High Contrast** makes applications easier to see by using more distinct colors. So, if you find it difficult to distinguish subtle color shifts, this may help to see what is on the screen. The default high contrast is dramatic and may be more than you want. This can be adjusted to meet your needs.

Use **Narrator** to tailor the way selections are read aloud and whether to bring it up automatically. You can even set it to enunciate the keys as you type. Numerous other features are available. You can invoke Narrator through **Magnifier** or bring it up directly by pressing **Win** + **Ctrl** + **Enter**. I prefer to invoke it through the Magnifier as I find I have more control as to the precise text is to be read aloud.

#71: Keeping email contacts up to date

Originally published in the October 2021 issue of Venturing into our Past (JGSCV)



Holidays provide a great opportunity to send mass mailings to friends and relatives, both to stay in touch and to verify that the emails that you have are current.

When I recently sent out my annual Rosh Hashanah emails, a few that had worked, bounced. Some did not, but also did not elicit expected responses. Possibly the recipients are no longer receiving email at the addresses I had used.

A work email might bounce if the individual has retired or changed jobs. A personal email might bounce if the individual switched their email provider. It might seem to work and yet elicit no response if the person simply stopped using that particular email account.

Once you have checked that you have typed the address correctly, you might phone the person or contact a mutual friend or a relative for a current email.

Here are a few other ideas for finding working emails (The first may avoid the problem entirely):

1. Ask for and record an alternate email, especially if all you have is a work email.
2. Check the 'sent from' address on the person's last email to you.
3. Recheck your contact list for an alternate email address that you may have saved.
4. Find the person on Facebook and use Messenger to ask for their current email.
5. Google "Directory" and the person's company or organization. You may be surprised.
6. Or, one of my favorites, Use FastPeopleSearch.com to find another email that might work.

If you have not used FastPeopleSearch.com I strongly recommend it as it shows physical addresses, land line and cell phone numbers and often email addresses across the U.S. It may show nicknames and even maiden names along with birth month and year. I have used it to identify close adult relatives of the person. Some of the information is out of date and sometimes it misidentifies a parent as a spouse. But enough is accurate to make it a terrific, free tool.

For more ways to find emails, see the July 13, 2021 article, "13 Ways to Find Someone's Email Address (Level Up Your Outreach Game)" at <https://kinsta.com/blog/find-email-address/>. While the target audience is sales professionals, many of the suggestions are free and useful for general searches.

A final thought on holiday greetings: Some that I receive are sent to a hidden list of recipients with no salutation. I find this to be somewhat cold. But, sending personal emails can be tedious and time consuming. My solution is to use Microsoft's "mail merge" to rapidly send individual emails to hundreds of relatives and friends, each with a personal salutation and, occasionally, even a unique comment.

[Go to Index](#)

#72: Contingency Planning

Originally published in the November 2021 issue of Venturing into our Past (JGSCV)



In early October, Facebook, Instagram, WhatsApp and Messenger experienced two outages totaling eight hours. These outages do not appear to have been the result of malware or hacking. Rather, they appear to have resulted from internal system changes. As we become increasingly dependent on the Internet, such outages, whatever the cause, can be more than a minor inconvenience.

The Facebook outages highlight the importance of having a backup plan for the various services on which we rely. If you do not already have alternatives in place for the communication apps you use, like Messenger, Twitter and Gmail, now might be a good time to think about this.

Here are ten other contingency planning actions to consider:

1. Download an alternate browser (Firefox, Chrome, Safari, Edge, Tor). It is easy and free to have a ready backup to invoke when your regular browser isn't functioning properly.
2. Have an alternate driving directions app in your car or on your smart phone so that you can still find your way when the primary app is down (physical maps, anyone?)
3. Download the passwords stored in your cloud-based password manager. Keep this, and a copy of your master password in a password-protected file and in a secure physical place.
4. Have alternate emails and phone numbers for friends and family. We have all experienced emails that bounce and phone numbers that no longer work.
5. Back up your picture and data files automatically BOTH to the cloud and to a local device. Either should provide 99%+ protection and availability. But 99.99% is better.
6. Consider having a second device available to replace your primary computer. When my desktop's sound would not function, I switched to my laptop and was able to teach an online class
7. Most smart phones offer "hot spot" functionality. Be sure you know how to turn yours on so that you will still be able to connect to the Internet during an Internet disruption or power outage.
8. In a disaster, local phone lines can be overloaded. Have a disaster plan with someone hundreds of miles away to receive and relay calls between you and local members of your family.
9. Agree on an alternate physical location for the family to gather if a fire, flood or earthquake blocks access to your normal gathering location and jammed phone lines restrict communication.
10. While I lived most of my life without a cell phone, I would feel isolated and vulnerable today without one. Consider having an inexpensive backup phone on a different service.

Contingency planning weighs the likelihood of an occurrence, its impact should it occur and the cost of reducing the risk. Events, such as Facebook's outage, bring this need into focus.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#73: Charity Review Websites

Originally published in the December 2021 issue of Venturing into our Past (JGSCV)



This updates my December 2018 article, "[Practicing Safe 'Tzedakah' \(Charity\)](#)" on doing your homework before donating. Some charities are evasive as to where the money goes. Others have fundraising, executive salaries and other overhead significantly above the norm. Some are simply scams.

Tools to check before you donate include Charity Watch (<https://www.charitywatch.org/>), Charily Navigator (<https://www.charitynavigator.org/>), and the BBB's Wise Giving Alliance (<https://give.org/>). They all provide quick, unbiased, information.

If you would like to drill deeper, you can review the IRS "990" filings required of most large 501(3)(c) charities. These filings can provide a wealth of information as to the purpose, the total revenue and how much goes into fundraising, executive salaries and overhead.

I have even used these filings to aid my genealogical research. On Googling a relative with a fairly common name, I found he had a family charitable foundation. The IRS form 990 showed his address and phone number!

In my previous article I cited the Foundation Center's "990 Finder." I now find this tool to be dated, lacking current 990s for a sampling of charities I queried. I recommend use of the IRS search facility for nonprofit filings at <https://apps.irs.gov/app/eos/>. *(link updated December 2024)*

Consider Googling the name of the charity plus "complaint", "review", "rating" or "scam." While not everything one reads on the Internet is valid, obtaining critical information as well as material published by the charity may help you make the best choice.

If you simply Google "Best Charities", "Charity Reviews", or the like note that the first few links tend to be paid ads in which listed organizations pay for placement. Objectivity is questionable.

A few more considerations:

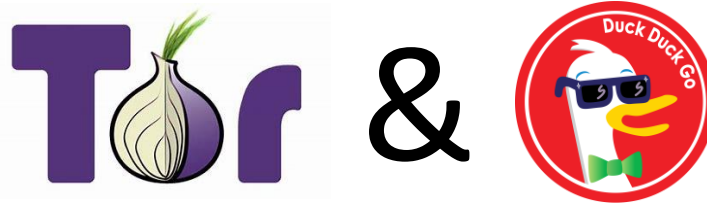
- Don't let anyone rush you into making a donation. This may be a sign you are being scammed.
- Never send cash, gift card or wire money. These are also typical of scammers.
- Monitor bank and credit card statements to ensure that a one-time donation is not recurring.
- Be especially careful before donating to a crowdfunding site. Many are not legitimate.
- Solicitors are often intermediaries who take a fee. Consider donating directly to the charity.
- Ask for written assurance, before you donate, that personal information will not be shared.
- Scammers sometimes choose charity names that sound like real ones. Pay attention!

For more, see, <https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#74: A Browser that will not track your every move
Originally published in the January 2022 issue of Venturing into our Past (JGSCV)



In response to an email from the X-CHAIR folks about a \$500-off special, I clicked on the link to read more. Now, I am receiving regular X-CHAIR pop-ups. No doubt, you have had similar experiences. Google Chrome, Mozilla Firefox and Microsoft Edge track your visits and provide these interminable ads. As you have undoubtedly heard, “If the product is free, you are the product!”

If you do not want to be tracked and do not want these pop-ups, use the Tor browser and associated DuckDuckGo search engine. They protect your privacy by routing you to a distant location (I often get routed as if I were in Germany). While some ads are displayed (they have to pay the bills), They do not track your searches and do not generate ongoing pop-up ads. You are also hidden as you surf the net.

There is no cost to the Tor browser or DuckDuckGo search engine. They were developed and maintained by folks who take privacy seriously, almost as a religion. I am no zealot. I use four browsers on my computer, Microsoft Edge, Mozilla Firefox, Google Chrome and Tor/DuckDuckGo. When I do not want to be tracked, I use Tor (“The onion router”), from The Tor Project, a 501(3)(c) organization.

Download Tor and DuckDuckGo at <https://www.torproject.org/download/>. Versions are available for Windows, MacOS, Linux and Android. In three years, I have encountered no issues with the Windows version. It takes a few extra seconds each time you invoke it as it creates a random hard-to-trace network routing. It then works like any other browser and search engine.

If Tor has routed you through Germany, you may see some results in German. If Holland, you may see some results in Dutch. Don’t let it throw you. It is working to anonymize you! As with any browser, once you connect to a site you run the risk of malware being transferred to your computer directly from that site. So, do not look at Tor as a way to safely visit risky sites.

If you think Google’s Incognito mode or Firefox’s Privacy mode are sufficient, consider this; while they claim not to record the sites you visit on your computer and to delete any cookies created at the end of your session, they do not make any commitments regarding whether your accesses are tracked for sale to their advertisers.

If you want to read more about Tor see [https://en.wikipedia.org/wiki/Tor_\(network\)](https://en.wikipedia.org/wiki/Tor_(network)) and if you want to dig deeper, see <https://vpnoverview.com/privacy/anonymous-browsing/tor/>. Along with protecting your privacy, Tor can be used to access “onion” addresses on the dark web. For a quick overview of the dark web, see my November 2017 article, “[What is the Dark Web?](#)”

#75: Cyber warfare, 2022

Originally published in the February 2022 issue of Venturing into our Past (JGSCV)



On January 14, 2022, Reuters reported a massive cyberattack on Ukrainian government websites. While Russia has denied responsibility for cyberattacks in Ukraine in the past, it is seen as the most likely perpetrator. See <https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/>.

Also on January 14, 2022, the AP reported a cyberattack on the schools in Albuquerque, NM resulting in 75,000 students being sent home for a second day. See <https://apnews.com/article/education-new-mexico-albuquerque-000a615feacd4e4d5bd0f8538689b023>

China, Russia, North Korea and Iran have been investing heavily in cyber and are capable of causing severe disruptions anywhere in the world. America is rich in potential targets as we have an enormous number of discrete governmental and commercial networks, many with weak cybersecurity.

President Biden has stated that he will take strong, non-military, action in the event of a Russian invasion of the Ukraine. Presumably, he would punish Russia economically. Putin has made clear that he will not stand for this. The response may be a cyberattack. Such attacks can be accomplished at minimal cost, have significant impact and even permit deniability.

Iran has yet to make good on its promise to avenge the killing of Qasem Soleimani, “at a time and place of its choosing”. Some are predicting cyberattacks later this year against U.S. targets. Iran and Israel have repeatedly traded successful cyberattacks against one another.

Should we continue to stand by Taiwan, as the President has committed us to do, or further challenge China in the South China Sea, China could respond with a cyberattack. And North Korea is always the wild card. In 2014 they launched a successful cyberattack against Sony Pictures when it released “The Interview” which they felt insulted Kim Jong-un.

The Jerusalem Post predicts that, “Cyber warfare 2022 will be 2021 on steroids”. See <https://www.jpost.com/cybertech/article-691438>. This may sound like science fiction. But it is all too real. While we, as individuals, can do little to prevent this, we can take some precautions. My November article on “[Contingency Planning](#)” provides 10 steps to consider.

In addition, consider having extra cash on hand if our financial infrastructure is disrupted and credit cards cannot be processed or banking is otherwise impacted. Have back up plans for utilities that might be impacted, including water, power and Internet. Back up your data locally as well as to the cloud. And, maintain different strong passwords for your various online accounts.

We have seen repeated successful cyberattacks against hospitals, schools, businesses and entire communities. Although we may not be able to avoid such attacks, we can be aware and prepared.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#76: Upgrading to Windows 11

Originally published in the March 2022 issue of Venturing into our Past (JGSCV)



If you have a Windows 10 PC running a recent Intel (or other manufacturer) processor, Microsoft should offer you a free upgrade to Windows 11 during the next few months. If Intel, this means generation 8 (gen 8) or higher. You can view the Windows version and processor generation by entering “system information” to the right of the Windows symbol: 

“OS Name” shows the Windows version. “Processor” will include something like “i5-9400” or “i7-12700”. The one or two characters after the dash is the generation; so, these are a gen nine i5 processor and a gen twelve i7 processor. Windows 11 is not intended for gen 7 or earlier as some features require components that were not included until gen 8.

Most PCs sold during the past three years are gen 8 or higher. Note that Windows 11 is only free for those already running Windows 10. Microsoft offers a tool to verify that a PC meets Windows 11 minimum requirements. It can be downloaded at:

<https://www.microsoft.com/en-us/windows/windows-11#pchealthcheck>.

You may choose to accept or defer the upgrade. Some prefer to defer for six months or so to give Microsoft the opportunity fix bugs that escaped extensive testing. New releases typically have potentially disruptive bugs. Others opt to pass as they prefer Windows 10, and can choose to upgrade later. Microsoft has committed to supporting Windows 10 through 2025.

Windows 11 emulates some of the Apple Mac’s look and feel. It also supports a growing suite of Android apps (like those on a Samsung smartphone). Here are a few of its features:

- It will let you set up, and toggle between, virtual desktops in a way that is similar to Macs. You could switch between desktops set up for work, home and genealogy.
- It includes features called Snap Groups and Snap Layouts allowing you to simultaneously bring up multiple tasks that you typically want to run at the same time.
- It integrates Teams, which includes video conferencing, directly into the Windows 11 taskbar, making it easier to access (similar to Apple’s FaceTime).
- For tablets, it improves the experience for touch screen, key typing, voice typing and consistency of commands across the system.
- It includes certain features found in Xbox consoles, like Auto HDR and DirectStorage, to improve the gaming experience on a Windows PC.
- And a decision to upgrade is not final. Once you have installed Windows 11, you have ten days to freely fall back to Windows 10.

For more on Windows 11 see, <https://www.pcmag.com/reviews/microsoft-windows-11>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#77: “Nothing is certain but death and taxes” (Ben Franklin)
Originally published in the April 2022 issue of Venturing into our Past (JGSCV)



Have you considered what will become of your online presence after you die or become incapacitated? Many of us have wills and trusts to direct what is to become of our financial accounts and physical assets. But, what about our online presence in Facebook, LinkedIn, Ancestry, MyHeritage, FamilyTreeDNA and many more?

If Facebook becomes aware of your passing, and you have not provided settings to delete the account on your death, it will be “memorialized”, or frozen. If your settings allow, friends may be able to share memories on a memorialized timeline. Facebook will only remove a memorialized account if they receive a valid request from your “Legacy Contact” or from an individual to whom you have granted legal power to act on your behalf.

If you choose to designate a Legacy Contact in your Facebook settings, that person may update your profile picture and cover photo, view posts, including private ones, authorize who can post tributes and request deletion of your account. The Legacy Contact, who must be a Facebook friend, may not log into your account, read your messages, remove any of your friends or make new friend requests.

For more information on what a Facebook Legacy Contact can and cannot do, see <https://www.facebook.com/help/1568013990080948>. For more information on what will happen to your Facebook account if you pass away, and instructions for setting up a Legacy Contact, see <https://www.facebook.com/help/1506822589577997?ref=tos>.

FamilyTreeDNA permits you to designate a “Beneficiary” who can control your account in the event of your death. See <https://help.familytreedna.com/hc/en-us/articles/360004731636-Beneficiary-Information-Tab>. Ancestry requires documents from your designated successor showing that they have been appointed to take over your account. See https://support.ancestry.com/s/article/Managing-a-Deceased-Person-s-Account?language=en_US.

MyHeritage requires a death certificate for the deceased webmaster and only permits a first-degree relative to take over the account. See <https://faq.myheritage.com/en/article/the-webmaster-site-creator-has-passed-away-how-can-i-delete-or-take-over-the-account>. If you have a personal genealogical website, have you arranged for what will become of it on your death?

Consider what you wish done for each of your online accounts. Do you want them cancelled, temporarily continued or transferred should you die or become incapacitated? Update settings where available and memorialize your preferences in a will and/or trust, designating an online executor. Store a list of your online accounts, with access codes and passwords in a separate, safe location accessible by your online executor after your death or incapacity. Periodically review this list and instructions.

I have long advised against sharing passwords and do not recommend it as your succession plan. Shared passwords may be further shared, misplaced or misused, especially if your relationship with your backup changes over time. Provide these only when needed by your designated online executor. For additional guidance, Google “planning for your digital presence after death”.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#78: 1950 Census Search Tips

Originally published in the May 2022 issue of Venturing into our Past (JGSCV)

The 1950 Census was released on April 1, 2022 after a 72-year hold. Months before, I had used the “Unified 1880-1950 Census ED Finder” on <https://SteveMorse.org> to identify the enumeration district (ED) for my address in Newark, New Jersey. I then found other relatives searching by name. Here are a few tips and tricks for searching the Census.

One can search by name within a city or county, across a state or the entire nation. After selecting the state, select the city or county from an alphabetical list. First check to see if

your target city is shown. If not, only then select the county. For example, Newark, New Jersey was enumerated separately from Essex County. So, one would select “Newark, Essex” rather than “Essex” in the alphabetical list. Selecting Essex will not retrieve any records for Newark.

Artificial intelligence (AI) was used to transcribe the Census. It transcribed my dad as “Book Binder Jack”. Recognizing that there are many such transcription errors, the name search includes near matches. Searching for “Bookbinder” did, in fact, find my dad, even with the break in the surname. It also found my widowed great-grandmother, Mollie, who was erroneously transcribed as Moller.

You can request corrections by selecting [Help Us Transcribe Names](#) above the sheet image. I used it to ask that my dad’s surname and great-grandmother’s given name be corrected. Ancestry and MyHeritage currently provide limited access to the 1950 Census as they work on its indexing. For the present, you will likely have more luck going directly to <https://1950census.archives.gov/>.

The search returns images of the full census sheets. Each image is followed by a searchable listing of the names found on the sheet. Although the Census search permits you to enter given name and surname, it returns any matches of either. Searching for “Bookbinder” in Newark, NJ returned three hits. Searching for Jack Bookbinder returned 899! Quotation marks around the name make no difference.

I recommend you search for the surname (within city or county, if possible). Once you have retrieved the sheet images containing the surname, use the Windows Find command (Ctrl-F) to search for the given name or the full name in the listing of names immediately after each sheet image. To minimize the number of screens to search, change the button in the upper right from “Show 25” to “Show 100”.

My wife’s birth surname is Newmark. By searching for “Newmark” in Illinois, and then “Ctrl-F” for “Newmark Louis”, I quickly found them in Broomfield, Cook County. (Note that the search is surname followed by given name.) This worked because Louis, my wife’s father, was head of household. As surnames were generally not shown for other family members, Ctrl-F them by given name only.

Again, access the 1950 Census for free at <https://1950census.archives.gov/>. Happy hunting!

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#79: Phishing text messages

Originally published in the June 2022 issue of Venturing into our Past (JGSCV)

Phishing emails come directly to your inbox, describing a problem, an opportunity, a windfall, or a pending Amazon delivery. They require your immediate action. Most of us have received any number of such emails and recognize them for what they are, schemes to get our personal information and money. Cybercriminals are now directly targeting mobile devices, like your smartphone.

Per a recent ZDNet article (<https://www.zdnet.com/article/phishing-attempts-against-smartphones-are-on-the-rise-and-those-small-screens-arent-helping/>), 75% of phishing websites now target mobile devices with both email and text messages. Cybercriminals count on people clicking on the links displayed on smartphones and responding to texts without critically considering whether the message is real.

All phishing attempts, no matter the device, are designed to take advantage of your trusting or helpful nature, fears, curiosity, or greed. If you connect, you will be dealing with individuals who are skilled in separating you from your money and personal information. They are very good at what they do.

During a recent two-day period, I received three phishing texts on my iPhone. If I felt that there might be something to these alerts, I would have called Wells Fargo or Verizon directly. I would certainly not call the number, respond to the email or click on the links shown in, or above, the text message.

Received on 5/3/2022	Received on 5/4/2022	Received on 5/4/2022
+1 (301) 418-9134 Text Message Today 7:20 PM wells: the amount for \$654.39 has been declined, to block unauthorize purchases please click link below http://bemywells.zapto.org/r/DS8sFGT	Wellsfargo-33246@... Text Message Today 6:10 AM (ALERT) 3324 - WellsFargo: Your online access is suspended, restore now: 8dmdw.app.link/yy6h	899000 Text Message Today 1:40 PM Verizon Alert: There's a request to authenticate from the Verizon website. Please confirm or deny here: https://govzw.com/BnmkZJIQ

The links shown above are clearly suspicious. Yet, people often click without thinking. I would not click even if they started with <https://wellsfargo.com> or <https://verizon.com>. The display may not reflect the actual link, which may take me to a legitimate-looking page set up to scam me. To demonstrate, click on "Wells Fargo", "Verizon" or any of the other links above; you will find that they all bring up CNN.com.

Cybercriminals may attempt to hook you by voice, text, emails, or even IM (instant messaging). For more on avoiding phishing scams, please see these previous articles in the Practicing Safe Computing series: [Vishing \(Voice phishing\)](#), [Top 10 Tips for Detecting Phishing](#) and [Phishing email from your Bank](#).

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#80: Take care what you share

Originally published in the July 2022 issue of Venturing into our Past (JGSCV)



The Los Angeles Times of Sunday, June 19, 2022, page 20, carried the story of a woman who received a call, purportedly from her son, sobbing, “Mom, momma, please come get me. Mom, please. Please Momma.” Another person took over the call letting her know that her son had witnessed an illegal transaction and had interfered, spoiling it. The man had lost \$15,000 due to this and she needed to make him whole or she would never see her son again.

Her son had been living on the streets and she had no good way of reaching him. She was told that if the police were to be involved her son would be gone forever. Nonetheless, she did call in the police and after four harrowing days they were able to locate her son. The “kidnapping” had been a hoax.

The woman in the LA Times article may well have shared on social media her worry about her son living on the streets and that she had difficulty reaching him. While a criminal might be directly aware of her son’s situation, he might have picked this up through social media chatter.

How many times have you seen Facebook posts about an exciting upcoming trip to Turkey, Mexico or Zimbabwe? How many posts have you seen about upcoming travel to Chicago to attend a family wedding or bar mitzvah? How many posts have you seen that provide personal information about the person, their family members, or friends?

While you may think that your social media postings are only seen by trusted friends, this is not always the case. Presume that whatever you post on social media will be seen more broadly than you intend. A friend may innocently pass on your plans; a scamster may have somehow become one of your 247 “friends”; a cybercriminal may be following your every social media post.

Here is how the scam might unfold: A friend posts that he will be vacationing in Turkey. You get a call that he has been jailed for drug possession and needs \$2,000 immediately. You post that you will be traveling to Chicago for a wedding and your house is burglarized by thieves who know you will be away. Scamsters convince you that they are IRS agents by referring to personal information that you shared on social media.

While we might think that we would quickly recognize such scams, in the heat of the moment, and with experienced scamsters who well know how to play on our emotions, we may not. The woman in the Los Angeles Times story had the presence of mind to not fall for the scam. Hopefully, we all will. While you would never post on your front door that you are away in Chicago for the weekend, are you as careful in your Facebook posts?

We should all be sensitive that unintended folks may, and likely are, paying attention to what we “privately” publish on social media. For more on the risks of posting personal information on social media see, <https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media>

[Go to Index](#)

#81: Free Online Databases Courtesy of Your Public Library
Originally published in the August 2022 issue of Venturing into our Past (JGSCV)



Several different searchable historical newspaper databases are available online and for free through local libraries. We are all aware of Newspapers.com, an excellent fee-based resource. This article discusses resources that are freely

accessible online using your library card and not requiring a trip to the library. Virtually all California public libraries offer library cards to any California resident. You need not live in that library's community. However, you may need to go to the library to pick up your card.

"Newspaper Archive" includes literally thousands of searchable, historical U.S. and international newspapers. I wanted to search the Philadelphia Jewish Exponent in my research into the Bookbinders of Philadelphia restaurant fame. It is not to be found in Newspapers.com but the Exponent (1877-1977) can be found in Newspaper Archive.

Some of the other Jewish newspapers in Newspaper Archive include Seattle Jewish Transcript (1924-1975), The Cincinnati Israelite (1856-1879) & The American Israelite (1899-1997), The Miami Jewish Floridian (1928-1977), and The Atlanta Southern Israelite (1929-1977). It also includes The Sydney Hebrew Standard of Australasia (1895-1953). You can access it online with your LAPL card.

"NewsBank" similarly includes thousands of searchable, historical and international newspapers. Most of the libraries in the LA/Ventura County area offer access to NewsBank, though the scope of newspapers varies. They also provide access to the historical LA Times, the historical NY Times and Data Axle Reference Solutions' nationwide phone and address lookup.

The T.O. and Ventura County libraries provide online access to Heritage Hub's collection of newspaper obituaries and death notices. The Camarillo, LA County, LA City and T.O. libraries provide online access to HeritageQuest. The LA City Library provides online access to MyHeritage (Library Edition), The San Francisco Chronicle (1865-1922), Encyclopedia Judaica, Jewish Data and A to Z Maps Online. The Long Beach Public Library offers access to the Newspapers.com California Collection (1852-2009).

While there is no guarantee it will continue, the LA City and the Ventura County libraries continue to provide free access to Ancestry Library Edition. I verified this on July 18th. I have a personal subscription to the U.S. edition of Ancestry.com and find the library edition a valuable addition. The library edition includes international information as well, which helps in my Canadian and British research.

Finally, I found a relative in the Massachusetts State Penitentiary in the 1910 census! I subscribed to the Boston Globe for just \$1/month for six months, and found extensive coverage of the trial as well as birth, marriage and death information on a host of Boston relatives. I canceled before it converted to a regular subscription. Many newspapers offer bargain introductory online and print deals.

While I focused on Southern California libraries, if you are in another area and have not checked out local online library resources recently, you may be surprised at what you find.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#82: Cyber warfare 2022, a midyear update

Originally published in the September 2022 issue of Venturing into our Past (JGSCV)



My February article, "[Cyber warfare, 2022](#)", shared The Jerusalem Post prediction that, "Cyber warfare 2022 will be 2021 on steroids". I just reviewed "[Cyber Attack Trends](#)", a mid-year report by Check Point Research, an Israeli firm that is a major player in network security. Here are some of its highlights.

In February, just one day before Russia's invasion of Ukraine, Russian cyberattacks were carried out against hundreds of Ukrainian government targets, financial, IT and energy institutions. These attacks were geared to not only disrupt services but to destroy underlying data and applications and so make restoration all the more difficult. Ukraine was better prepared than Russia had expected.

On March 1, Russia took down a Kyiv TV tower with both missiles and a cyberattack. Russia has also repeatedly attacked utilities in various parts of Ukraine, cutting services to hundreds of thousands. In response, Ukraine has recruited an international army of hackers to act on its behalf. Ukraine hacked into the Russian TV platform and beamed live antiwar messages into homes across Russia.

While Russia has far more advanced cyberwarfare capabilities, this voluntary army of international hackers, numbering in the tens of thousands, has blunted the Russian advantage, has helped protect Ukrainian infrastructure, and has launched occasional counterattacks. This has included the leaking of hundreds of thousands of Russian government documents.

Bold cyber-attacks are growing Worldwide. The Conti Ransomware group, which operates out of Russia, launched a cyberattack in April that crippled essential services across Costa Rica. In May, it launched an attack that disrupted services in Peru. Neither country would pay the demanded ransom and opted for the painful process of restoring services on their own. The Conti website posted the following:



Wars have always provided laboratories for testing and improving weaponry and tactics. Cyberwar is no different. State actors and private cyber warriors are likely to come out of this war more capable and dangerous. Russian cyberwarriors are certainly learning ways to circumvent the defenses that Ukrainian volunteers are able to create and so will be better prepared to overcome our cyber-defenses.

Expect the future to include temporary government, utility and financial disruptions. Expect data dumps of sensitive information, including medical, financial and security information. While we, as individuals, can do little to prevent this, we can take precautions. See my November 2021 article on "[Contingency Planning](#)" for ten steps to consider to prepare for a range of cyber-disruptions.

In addition, consider having some extra cash on hand to ride out a temporary disruption to financial services, including credit card processing. Back up your data locally as well as to the cloud to ride out a cloud disruption. Maintain different strong passwords for your various online accounts so that a breach in one area does not leave your other accounts exposed.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#83: Your wallet has been stolen, now what?

Originally published in the October 2022 issue of Venturing into our Past (JGSCV)



Recently, a thief broke into my gym locker and stole my wallet and iPhone. I had to cancel and replace credit, debit, medical, professional and membership cards, my driver's license, my iPhone and more. I was also concerned about identity theft.



Do you need to carry all the cards that you have in your wallet? Better to have fewer to replace if your wallet is lost or stolen. A social security card and the street address on a driver's license can provide a thief with valuable information to steal your identity. I do not carry my social security card and my driver's license shows my post office box rather than my street address.

Do you keep one or two credit cards in reserve and not in your wallet? By doing so, you will continue to have active credit cards to use while awaiting the reissuance of the cards that were in your wallet. Consider limiting the cards in your wallet to those that you routinely use.

Do you know specifically what cards are currently in your wallet and the numbers to call to report them stolen? I periodically copy the front and back of all the cards in my wallet. This ensures that I handle them all and provides necessary card and contact information.

Are you taking appropriate physical precautions? Use a sturdy padlock on your gym locker. I did not, but now do. Carry a wallet in a briefcase, in an inside coat pocket, or front pants' pocket. Purses are especially at risk. Here is an article from AARP to consider, [How to Keep Your Purse Safe, Secure \(and Germ-Free\)](#)

Do you have a password or other secure method to open your cell phone? Most of us have personal information, contacts, and pictures on our cell phones. The slight inconvenience of locking the screen when not in use may keep a thief from obtaining this treasure trove of information.

Do you keep a list of PINs, IDs and passwords in your wallet or purse? Consider keeping them in a password manager. See <https://www.pcmag.com/picks/the-best-free-password-managers> for an article assessing the best free ones. As I have shared, I continue to use LastPass even though it did not make the 2022 list.

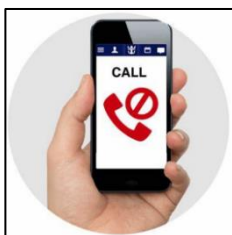
Do you have a backup cell phone? I survived most of my life without a cell phone. But now it is a key part of my existence. Along with staying connected, web site authentication often includes validation via a code sent to your cell phone. Consider having an inexpensive back-up cell phone.

If you think that you may be at risk of identity theft, consider placing an alert or freeze with the three credit agencies. This will reduce the ability of a thief to obtain new credit in your name. My 2015 article, [Credit reporting agencies](#), remains current and accurate.

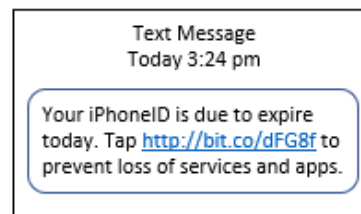
[Go to Index](#)

#84: Stopping Text and Voice Spam

Originally published in the November 2022 issue of Venturing into our Past (JGSCV)



I regularly receive unwanted calls offering Marriott and Hilton timeshares, extended automobile warranties, amazing investments, and fund-raising appeals. I have also received phishing texts like the one to the right. Blocking the caller or sender does not work as they continue with ever-changing numbers.



Several of the mobile carriers offer apps to block spam. Generally, the basic version is free and the enhanced version costs several dollars a month. Others refer you to apps you can download. Typically, these also offer a free-version and an enhanced version for a monthly fee.

See the PC Magazine article, [How to Block Robocalls and Spam Calls](#) for an overview of AT&T Call Protect, Verizon Call Filter, and T-Mobile Scam Shield. The article also describes the Hiya, RoboKiller, Truecaller, and Call Control commercial apps. They all rely on lists of spam numbers which are continuously updated. However, a spammer displaying a number not on the list may still get through.

No app is needed to block ALL calls from unknown numbers, routing them directly to voicemail. Most spam callers will then disconnect. You can return legitimate voice messages and add them to your contact list if you wish. Similarly, no app is needed to tag or block text messages from unknown senders.

For iPhones

- To send unknown calls directly to voicemail: 1) Tap Settings (the gear symbol), 2) tap "Phone", and 3) toggle "Silence Unknown Callers" to green. *Incoming calls will ring from people in your contacts, recent outgoing calls, and Siri Suggestions (phone numbers in recent emails)*
- To allow only calls from your contacts to ring: 1) Tap Settings, 2) tap "Focus", 3) toggle "Do Not Disturb" to green (ON), 4) toggle "Turn on automatically" to clear (OFF), 5) tap "People" under "Allowed notifications", and 6) toggle "Calls From" to "All Contacts".
- To tag unknown texts: 1) Tap Settings, 2) tap "Messages", and 3) toggle "Filter Unknown Senders" to green. When accessing messages, tap "Filters", and "Known Senders" to only see messages from your Contacts. *Apple permits you to block individual senders, but not all unknown senders.*

For Samsung Androids (*the steps may vary for other Android manufacturers*)

- To only allow calls from your contacts to ring: 1) Tap the phone icon, 2) tap the three dots at the top of the screen, 3) tap "Settings", 4) tap "Block numbers", and 5) toggle "Block unknown/private numbers" to green.
- To block unknown texts: 1) Tap the messages icon at the bottom of the screen, 2) tap the three dots at the top of the screen, 3) tap "Settings", 4) tap "Block numbers and spam", 5) tap "Caller ID and spam protection", and toggle to green.

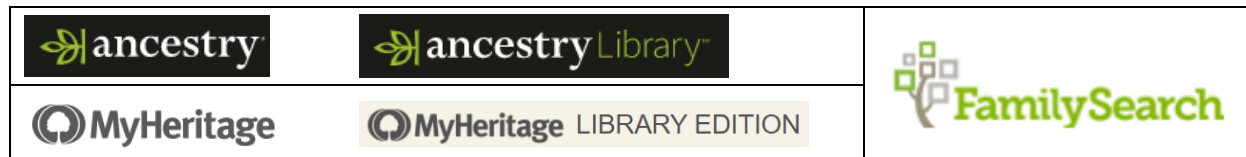
If you are expecting a call from a number that is not in your contact list and you wish it to ring to your phone, temporarily turn off call blocking. As I tend to forget the steps if I have not done them in a while, I record them in a Note on my iPhone for quick reference when needed.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#85: Search tips for selected genealogy websites

Originally published in the December 2022 issue of Venturing into our Past (JGSCV)



Congratulations on finding a document in Ancestry, MyHeritage, or FamilySearch. Be sure to check the pages to the right and left. I found a Declaration of Intent (DOI) in Ancestry for Julius Bookbinder, filed in Denver in 1910. When I looked to the right, I found 16 pages of supporting documents. Occasionally, I have found documents on other relatives filed next to the located document.

Before finding him, I had no awareness that this Julius Bookbinder even existed. My Bookbinders came from Dubno in northwestern Ukraine. Ancestry has a “**Keyword**” field that is compared to the contents of all transcribed fields in the record. I searched for the surname “Bookbinder” and entered “Dubno” in the “**Keyword**” field and up popped Julius. MyHeritage has a similar field called “**Keywords**.”

In this case, “Dubno” was Julius’ place of birth. However, it might have been his last location before emigrating or the town of his closest relative in the old country. Finding a “Bookbinder” associated with “Dubno” is a lead that I would want to pursue. I was able to identify a collateral line and take my research back another generation to my sixth great-grandfather, Itsko, likely born around 1730.

Search criteria and results may differ between Ancestry, MyHeritage, and FamilySearch. Consider repeating searches in all three. For example, MyHeritage indexes the name of the person to whom a passenger is traveling; Ancestry does not. So, searching my grandfather’s name in MyHeritage returned links to the passenger lists of a niece and a nephew who were traveling to him.

In another instance, Both Ancestry and FamilySearch found a couple of relatives in an index of naturalizations from Essex County, New Jersey. However, FamilySearch had images of the Petition for Naturalization, while Ancestry did not. I have found differential information often enough to make the extra effort of replicating searches to be worthwhile.

In addition to my subscription to the U.S. version of Ancestry, I use AncestryLibrary. It provides access to worldwide records. Some libraries provide only in-library access to commercial genealogy databases such as AncestryLibrary; some offer remote access. To maximize my chances for remote access, I have signed up with various library systems, most recently, Las Vegas. (local residency is not required)

Finally, don’t overlook Ancestry’s card catalog. This is a searchable list of all of Ancestry’s collections. Click on “**Search**” or “**Begin Searching**” after you log in. Then, click on “**View all in card catalog**” at the bottom of the right column. I searched for “Canada” and “Passenger” and 12 collections were listed. I searched for, and found, a great-grandfather in “**Canada, Ocean Arrivals (Form 30A), 1919-1924**”.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#86: Package delivery, banking, and Social Security scams
Originally published in the January 2023 issue of Venturing into our Past (JGSCV)



I have recently received a spate of package delivery and banking spam texts. The common denominator is a link that can be misleading and dangerous. Once you click on the link you might be asked to approve the installation of software on your device or to disclose personal or financial information under the guise of identifying yourself. Don't fall for this!

Your package delivery failed because of the wrong address, please modify the address information to deliver again.

<https://www.us.ialla.us>

US Mail Service: Issue with your recent delivery, go to <http://uspxstech.com> for more.

Free Msg Wells Fargo: Recently, we discovered unusual activity or updates on your account that we believe may be unauthorized. For your security, Wells Fargo monitors all transactions to protect your account from misuse; You will not be able to use ATM/Debit/ Credit Card linked to this account for withdrawals or purchases until you verify your information. Visit us at <https://bit.do/VerifyWellsAccount> to secure your account.

Don't let your guard down because a link starts with "https". http or https messages such as these are almost invariably scams. Don't let curiosity cause you to click on the link, just to see what happens. Just doing so may authorize the installation of malicious software (malware) on your device. Never click on any link contained in a text or email unless you are confident that it is legitimate.

Most of these spams now come to your iPhone or Android as texts rather than emails to your computer. Cybercriminals know that we are more apt to click on links in texts. Once on their site they will likely ask you to identify yourself with your ID and password or other personal information. These fraudsters are experts at reeling you in. These scams continue because they work!

If you think that the message might be real, contact Social Security, Wells Fargo, FedEx, Amazon, or the U.S. Post Office directly and not by clicking on the displayed link or calling the displayed phone number. If you have relatives who might be more trusting or impulsive than you, help them to avoid such scams before they become a victim.



Check out these two Social Security Administration alerts. They are quick reads and well worth your time: <https://blog.ssa.gov/helping-you-avoid-scams-this-holiday-season> and <https://faq.ssa.gov/en-us/Topic/article/KA-10018> (What should I do if I get a call claiming there's a problem with my Social Security number or account?)

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#87 - Cybersecurity Tips

Originally published in the February 2023 issue of Venturing into our Past (JGSCV)



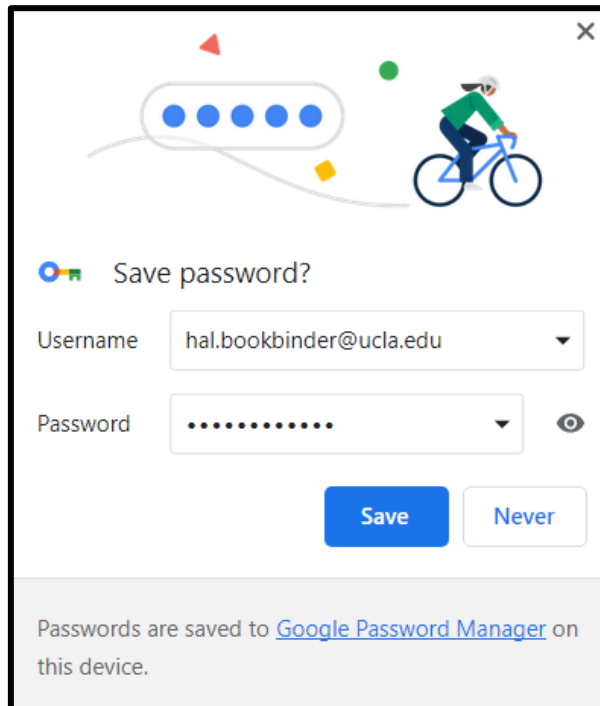
There is no single cybersecurity silver bullet. A comprehensive approach is needed: complex passwords, a password manager, multi-factor authentication, thinking before clicking on attachments and links, minimizing social media sharing, restricting app permissions, and keeping software current.

- **Use complex passwords and do not re-use them for different websites:** Passwords that you can remember are generally guessable. Cybercriminals have automated tools that will try hundreds or thousands of likely passwords. If you re-use passwords and one site is compromised, those for which you use the same password are also at risk.
- **Use a password manager:** Since there is no way to remember your different complex passwords, you must record them somewhere. Password managers are designed to do this, securely. Choose one that also generates complex passwords on request. Of course, you will need to remember the one, presumably complex, password for your password manager.
- **Use Multi-factor Authentication (MFA):** An ID and password alone are not enough. If a site is hacked, your ID and password may have been exposed. With MFA, the cybercriminal would require more. An example of MFA is texting or phoning you with a code for you to enter before access is granted. MFA is a necessary tool in protecting your critical online accounts.
- **Think before opening attachments or clicking on links:** As pointed out in my January article, they may take you to fraudulent websites that have been designed to look like the real thing. Once you enter your ID and password, they have it, and you may not even know that you have been scammed. See, <https://www.aura.com/learn/how-to-identify-fake-websites>.
- **Minimize what you share on social media:** Such information can be used to impersonate you, provide clues as to your IDs and passwords, convince you that a caller is legitimate based on their knowledge of you, and even put your home at risk if they know you are away on vacation. See, <https://www.aura.com/learn/how-to-protect-your-personal-information-on-social-media>.
- **Review which apps have access to your photos:** You may have unwittingly given full access to your photos to various apps. Photo tags show when and where they were taken. This, along with the photos themselves, can be revealing. I checked my iPhone settings for “Photo” and found that Siri has unrestricted access “to make suggestions.”
- **Review which apps have access to your location:** Apps can track your location, and not only when you want this. On your iPhone in Settings, select “Privacy & Security” and then “Location”. You may be surprised when you view the list of apps with whom you are sharing your location.
- **Keep software up to date:** Updates frequently contain “patches” to fix newly uncovered security exposures. It is generally best to remain current.
- **Even a password manager may be hacked:** In August 2022, LastPass, the password manager that I have used for years was hacked. They have been transparent about this and have advised users to change their passwords. I have done so (and plan to continue to use LastPass). See, <https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/>.

[Go to Index](#)

#88: Dangers of saving passwords in your browser

Originally published in the March 2023 issue of Venturing into our Past (JGSCV)



You sign into a website and your Chrome, Firefox or Edge browser asks if you would like to save the username and password. While it will make logging into sites easier, it puts you at increased risk that cybercriminals might steal your credentials.

Verizon's 2022 Data Breach Investigations Report shows that attackers are increasingly successful in using a combination of phishing and malware to steal user credentials. This is especially so when you opt to store your credentials in your computer's browser.

A cybercriminal might send you an email that piques your interest. You click on a link to get more information or press a button to access a special offer. You have just been phished!

Once you click on a link, select a button, or sometimes even when you simply open the email, you may be permitting the sender to execute a set of

instructions on your computer. This may include the installation of malware that discovers the master password for your browser and then uses it to download the IDs and passwords that are saved in the browser. The master password in Chrome is simply your Windows login PIN (the series of digits you enter to unlock the screen). Using a "keylogger", installed malware could easily discover this.

It is more difficult for cybercriminals to steal your credentials if they are stored away from your computer in a commercial, cloud-based password manager. To make it even more difficult for cyberthieves to access your credentials, set the password manager to automatically shut down when you close the browser and then to require you to reenter your master password when you re-open the browser.

I've used the free version of LastPass password manager for years and, for convenience, set it as an extension to my Chrome, Firefox, and Edge browsers. In LastPass, I selected 'Account', 'Extension Settings', and 'Log out when all browsers are closed'. This automatically shuts down LastPass when I close any of my browsers. Your password manager certainly offers a similar setting.

To clear passwords that you have already saved in Chrome, click on your picture icon in the upper right and then on the 'key' symbol. A list of the sites for which you have saved passwords will be displayed. Click on the three dots to the right of each and then on 'Remove'. For Firefox, click on the three bars in the upper right, select 'Passwords', and select 'Remove' for each saved password.

Given the risk of your credentials being compromised, and the impact if it happens, be sure to opt for multifactor authentication for critical financial, health and business websites. With such authentication, you must confirm that it is you by responding to a text or voice message sent to your smartphone.

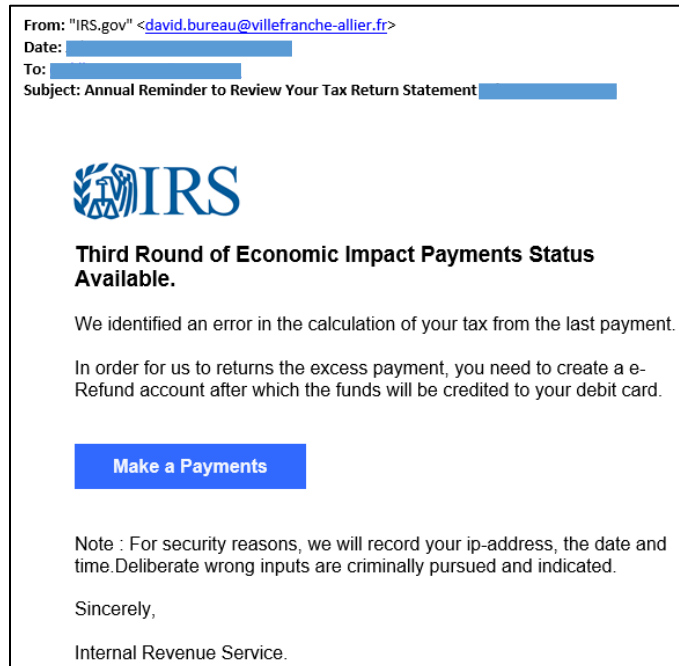
[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#89: IRS Scams

Originally published in the April 2023 issue of Venturing into our Past (JGSCV)

As it is now tax season, one can expect various scams related to property, state, or federal taxes. Often these come in the form of emails or text messages. Below is an email a buddy shared from the “IRS”.



While there are clues that it is not legitimate, including the ‘from’ address and some fractured English, some will fall for it. When they click on the link, it will ask for their banking information so that the refund can be credited.

However, once provided, the cybercriminals will instead drain the account, transferring funds to a location beyond the reach of American law. The link may also ask for other identifying information that can be used for criminal activity.

While the bank may eventually restore the funds, they may charge a fee up to \$500, based on how long it took to report the theft. Even if your funds are restored, you are in for a serious hassle.



If you click on a link and are asked for personal information, including the routing number and account number for your bank account, see this as a giant red flag. Government agencies will never contact you this way regarding a refund. Such contact will always be by U.S. Mail.

When you pay by check you are sharing all the information needed to take funds out of your bank account. Think about all the checks you have written that are floating through different hands. Similarly, your debit card information can be used to steal from you. Carefully review your monthly statements to quickly reverse unauthorized charges.

Bank statements may now be online and not mailed. Your diligence in reviewing them has not changed. Some scams involve returning deposits “made in error”. The “deposit” is reversed when the funds are not received. By then, the funds that you sent are gone. Carefully verify all withdrawals, checks and charges and deposits. If you wait too long (typically 60 days), you may be out of luck.

Never try to outsmart a cybercriminal via phone, email, or text. They have successfully swindled many educated and intelligent people who thought that they would never be taken. Rather, if called, hang up. If emailed or texted, do not call the number displayed or click on the link, no matter how curious you might be. Rather, call or email the agency directly.

Check out <https://www.irs.gov/newsroom/tax-scams-consumer-alerts> for more on the latest tax scams.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#90: Artificial Intelligence

Originally published in the May 2023 issue of Venturing into our Past (JGSCV)



The dangers of artificial intelligence (AI) are increasingly in the news. AI is the ability of computing to emulate human thinking, with instantaneous access to an almost limitless supply of information. Often, when interacting through email, text, or voice, we are not sure whether we are dealing with a human or a machine. This has enormous potential for both good and for harm.

The one sure thing is that this is part of our future. Governments are starting to show interest in legislating controls for artificial intelligence. Italy recently banned ChatGPT until it is satisfied that it does not violate EU privacy rules. Ireland has expressed support for Italy's action. The CEO of ChatGPT, Sam Altman, said that he intends to fully address Italy's concerns.

ChatGPT can create original written material, including poetry, fiction and more. As a college instructor, I recently took part in a discussion with my peers about how to deal with students' use of ChatGPT to create written assignments that conform to the professor's instructions, appearing to be original work and yet are not the original work of the student.

We agreed upon methods for detecting the use of ChatGPT which, while workable now, will quickly become outmoded as this technology advances. Cheating on educational assignments is just the beginning. The ability of AI to mislead and to scam people is almost limitless and will be a challenge to control. It is imperative that society implement adequate controls for this wondrous technology.

I call it wondrous as it may vastly speed scientific discovery, replace a huge part of the analytical work currently done by humans, and even help us improve sustainability of the planet. But, until we get a handle on it, we could be in for a wild ride. My focus for this article is its ability to scam us through emulation that is personal, responsive, and believable.

With AI, the days of misspelled, grammatically incorrect, and illogical spam may be ending. We can no longer rely on these red flags to detect cyber-criminality. We each need to be ever more careful before we share personal information or take actions no matter how plausible the request. If asked for personal information, stop; if you feel pressured to act, stop. Check, independently, before you act.

The Federal Trade Commission is alerting consumers about a next-level, more sophisticated family emergency scam that uses AI which imitates the voice of a family member in distress. There is a panicked voice on the line. It is your grandson. He says he is in deep trouble — he wrecked the car and landed in jail. But you can help by sending money.

You take a deep breath and think. You have heard about grandparent scams. But darn, it sounds just like him. How could it be a scam? You have experienced voice cloning. You cannot even trust the sound of a familiar voice! Using a short clip of his voice, say something he posted on social media, AI could construct a message, and even scarier, respond to questions that you might ask in real time.

Click here to read more about this scam on the FTC website: <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#91: Your own Internet access point

Originally published in the June 2023 issue of Venturing into our Past (JGSCV)



If you are one of the 95%+ of folks who carry a mobile phone, you likely are also carrying a mobile hotspot, permitting you to connect your laptop or other Wi-Fi enabled device to the Internet, even when out of range of a functioning and accessible Wi-Fi connection.

At 5:40 pm, I discovered that my home Wi-Fi was not functioning, and I was to teach a class at 6:00 pm. I did not know whether my wireless router had failed, or if my Internet Service Provider (ISP) was down and I did not have time to find out. Instead, I activated the “hotspot” on my iPhone, connected my desktop through it to the Internet, and was able to teach the class.

The hotspot feature on your iPhone or Android device uses the phone’s data plan to connect to the Internet, and provides a Wi-Fi connection that your laptop, desktop, or other Wi-Fi enabled device can use. This then allows for connectivity from any location where there is no Wi-Fi, or where you prefer not to use an available but potentially unsafe Wi-Fi.

To turn on the mobile hotspot on your iPhone, click “Settings”. If “Cellular” is off, click it and turn it on. Then, choose “Personal hotspot” and “Allow Others to Join”. You will notice that your iPhone’s name (in the form of “xxxxx’x iPhone”) along with your Wi-Fi Password are displayed. Although you may want to do so, you need not turn off your phone’s Wi-Fi connection.

To turn on the mobile hotspot on your Samsung Android, click “Settings”, choose “Connections” and then “Mobile hotspot and Tethering”. Now, turn on your “Mobile hotspot”. It will note that you must turn off Wi-Fi. Acknowledge this and tap “Mobile hotspot” once more to see the Network Name and Password.

Display available networks on any nearby desktop, laptop, or other Wi-Fi enabled device and you will see the Network Name that is displayed on your iPhone or Android. Select it and enter the password. The device will connect via Wi-Fi to your smart phone and through it to the Internet. Practice this to ensure you are ready when needed.

Once you no longer need to provide Internet access through your smartphone, it is good practice to turn off the hotspot. It is also good practice to have a complex hotspot password that is not easily guessable. Since it will display on your smartphone, you need not remember it. Be aware that you may be charged for data usage that exceeds your monthly limit.

 [https://](https://www.pcmag.com/news/google-to-kill-chromes-lock-icon-now-considered-outdated-and-misleading) Separate topic: The lock symbol provides a false sense of security. It only means that encryption is turned on and not, as many believe, that the site is safe. Read this article about Google’s plans to retire the lock symbol, and why encryption does not equal safety. <https://www.pcmag.com/news/google-to-kill-chromes-lock-icon-now-considered-outdated-and-misleading>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#92: Computer Cache and Cookies

Originally published in the July 2023 issue of Venturing into our Past (JGSCV)



You may have been advised to clear your cache or delete your cookies to resolve an online problem. Indeed, clearing them can solve a variety of issues. And, clearing them rarely causes much computer grief. So, understanding cache and cookies and being ready, and fearless, to clear them can be an easy fix to vexing web problems.

Web pages are “cached”, or copied, to fast internal storage in your computer to speed access to the Internet. Retrieving a page from internal storage is significantly faster than downloading it. Your browser has various ways to determine whether the cached page is still current. Sometimes it is wrong. Other times the cached page is broken. Clearing cache forces all pages to be freshly downloaded from the Internet. New copies will then start being cached.

Cookies are small files used to store data to facilitate your use of a specific online site. They might contain your preferences for that website, speed your logging in to the site, and permit you to stay logged in for the duration of your session. But, sometimes, the website might not be able to interpret the cookie; sometimes the cookie is broken. Clearing cookies can provide a fresh start. See: [“What are ‘cookies’ and should they concern you?”](#)

If a page that you are trying to access will not load, looks weird, or is acting funky, the problem might be in your cache and cookies. So, you might try clearing them before calling your favorite techie. You will hardly notice anything different when you clear cache. Temporarily, web pages may load more slowly. This will likely not even be detectable. So, start by clearing the cache.

If this does not resolve the problem, go after the cookies. Since your website-specific preferences are stored in cookies, once cleared, these preferences will be “forgotten”, and you will have to re-enter them. You may need to again tell the site to “remember” you on this computer, that your nickname is Joe, or that you prefer sports stories, rather than politics.

Cache and cookies are specific to each browser and reside in that browser’s storage area. So, if you use Chrome and Firefox, you will have two separate sets of cache and cookies, one for each. Clearing your cache or cookies from within Chrome will not clear your Firefox cache and cookies and vice versa. I periodically clear my cache and cookies, just “to clear the cobwebs” and possibly prevent future problems.

It is only partially true that cache and cookies are “temporary”. They generally have expiration dates. But these dates may be far into the future. The longer they hang around, the more likely they may become dated or broken. This article in PC Magazine provides instructions for clearing cache and cookies for all common browsers. Read it and practice so that you are ready. <https://www.pcmag.com/how-to/how-to-clear-your-cache-on-any-browser>

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#93: Ten Commandments to avoid AI scams

Originally published in the August 2023 issue of Venturing into our Past (JGSCV)

Thou shalt not

- ⌚ Succumb to pressure to act now.
- ⌚ Share personal data when contacted.
- ⌚ Pursue unsolicited opportunities.
- ⌚ Download unverified AI utilities.
- ⌚ Try to outsmart AI.

Thou shalt

- ⌚ Keep up with the news.
- ⌚ Limit sharing in social media.
- ⌚ Remain aware, remain vigilant.
- ⌚ Independently verify before acting.
- ⌚ Trust your gut.

While I believe that Artificial Intelligence (AI) will provide amazing advances in science, medicine, analytics, and productivity, and prove a boon for humankind, it will also be disruptive. Significant effort will be required to limit its potential for harm. While the Government is now scrambling to catch up, reviewing the Federal Register shows [numerous studies](#) on the benefits and challenges of AI.

My May article, [Artificial Intelligence](#), discussed the use of AI to make the existing grandparent scam more believable and more dangerous. I also noted that with AI, some of the easy clues in scam emails and texts, will become a thing of the past. While we do not yet fully know how AI may be used to perpetuate scams, some of the ways can be readily imagined.

There is a vast amount of personal information that is available on the Internet, including entries in public and semi-private databases. Using this data, AI will be able to better guess the passwords we use (few of us use truly random ones) and to personalize scams. It will be able to fashion communication that is so knowledgeable about each of us that we are more likely to believe in its legitimacy.

By scanning the Internet, including our postings on Facebook, LinkedIn, and Twitter, AI may learn that we are avid genealogists, are in job search mode, have suffered a loss, are ready to invest, are preparing to retire, or are on vacation in Europe. While scams today find and use this information, it can be costly and time consuming. AI can gather, analyze, organize, and use such information on an industrial scale.

AI might reach out to us as a distant relative trying to connect or a genealogical database offering new finds. It might offer an opportunity that is exactly what interests us right now. It could seemingly come from our specific bank, brokerage, grocery, utility, or doctor. It might even include specific knowledge about our accounts or medical history, and even ask about our spouse or children by name.

AI may be able to contact us in a way that shows knowledge that could only be coming from a relative or friend. Contact may be by email, text, or phone. Similarly, it might assume your identity and attempt to scam family and friends. You might first learn of this when someone reaches out to you asking how you could recommend this worthless stock to them, or otherwise set them up.

Folks have been fooled into downloading free, or low-cost, AI tools, only to be infected with a virus or sustain a ransom attack. Be sure to regularly scan your system for viruses. Trust that cyber criminals will keep pushing the envelope and coming up with new AI-driven scams. While there will likely be controls put in place, in the end, you need to primarily rely on yourself to avoid being scammed.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#94: Spear phishing messages

Originally published in the September 2023 issue of Venturing into our Past (JGSCV)



Had a terrific experience in Great Britain, both at the London Conference and afterwards travelling with my family from Stonehenge to Inverness. One of the more memorable sites was Linlithgow, Scotland, where we stayed while visiting the Edinburgh region. The ruined Linlithgow Palace was the birthplace of Mary, Queen of Scots and climbing among its many levels, with amazing views, both inside and out, provided great exercise and was a special treat.

I gave three talks at the conference, with my final one, “Practicing Safe Computing in the Age of Artificial Intelligence (AI)” scheduled for the very last time slot, 10:30 am on Thursday, August 3. I was worried that by this time, the attendees would be weary of presentations and ready to move on. Undoubtedly, many were. However, there was a good turnout for my presentation, and with questions, we ran well past the closing bell of the conference.

After my talk, my Venezuelan/Israeli friend and possible relative, Daniel Horowitz, (my mom was a Horwitz) shared a recent experience with WhatsApp in which he received a message, supposedly from a relative which was unexpected and had a slightly strange tone. He figured that it was a scam and quickly deleted the message. This provided a reminder that we need to be wary of messages we receive, whether email, text, Facebook Messenger, WhatsApp, or from any other application.

We tend to let our guard down when we believe that we have been contacted by a friend or relative. We might reveal personal information, provide money, purchase something, or take actions that may not be in our best interest. With the rise of Artificial Intelligence (AI), scams of this nature are sure to rise. AI’s access to massive amounts of information, its speed and analytics will permit it to send an enormous number of personalized messages and then follow up in a most realistic and engaging manner.

We must maintain our guard and not accept messages, whatever the source, at face value. Rather, if anything seems odd, trust your gut, and check with the supposed sender to see if they were the actual source. Don’t respond directly to such a message. This only confirms that your contact information is real and permits the false dialogue to continue. Scam artists are experts at reeling you in and with AI, the threat increases exponentially.

Spear phishing messages, targeted to you and intended to reel you in are nothing new. We have all received them. By now, you likely recognize them for what they are and do not respond. However, with AI, expect that they will seem much more real. Instead, of simply, “Hi” with no salutation, expect personalized messages with content “only” the other party should know. As genealogists, we know that there is a tremendous amount of personal data out there to be found.

All the best for the upcoming High Holidays and for all of 5784. Some years ago, I wrote an article about my experience as a fill-in Rabbi and USAF officer during the 1973 Yom Kippur War. Click here if you would like to read, [“My Most Memorable Yom Kippur.”](#)

I look forward to next year’s conference in Philadelphia and to seeing many of you there.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#95: Internet Relationship Scams

Originally published in the October 2023 issue of Venturing into our Past (JGSCV)



Relationship (or romance) scam victims are not just the young and naïve. Anyone seeking connections, including those who have lost their mate, are at risk. The FTC reports that in 2022, nearly 70,000 people reported losing \$1.3 billion in relationship scams. Since many likely do not report, the actual losses are likely higher. This is a nine-fold increase over the reported losses of just four years ago. Increased isolation due to the pandemic may have contributed to this.

A typical online relationship scam quickly progresses from a contact out of the blue, to strikingly similar interests, to professions of admiration and love, to immediate need of financial help or “can’t lose” investment opportunities, to ghosting, with your money and the phantom admirer gone forever.

Relationship scammers’ techniques

- Sending friend requests to people in your network, expecting some to accept, making it appear that you have friends in common.
- Amazing coincidences, in which the scammer’s passions, politics, and interests seem to closely match yours.
- Seeming to take a genuine interest in you, flattering you, and even expressing their love for you relatively soon after making contact.
- Wanting to move the conversation from the relationship app to email, WhatsApp, Telegraph, or another private messaging site.
- Telling you that they are unable to meet you in person. Common excuses are inability to travel and offshore or international work.
- Trying to convince you to invest, send money to resolve a problem, pay gift fees, or pay for transportation so that they can join you.

How to avoid becoming a victim

- Be careful about accepting new friendship requests. Don’t share personal information, including phone numbers and addresses.
- Suspect it’s a scam if the new admirer has excuses, no matter how plausible, for not meeting you in person.
- Share that you are in an online relationship with family and friends and listen to their feedback.
- If the online admirer shares suggestive, or even explicit, photos and asks you to do the same, **don’t do it!** and **block the admirer!**
- Do a reverse image search on any photo they send. You may find it on the web. Here is a recent [Forbes article](#) on how to do this.
- Never send money, crypto, gift card numbers or wire funds to a person you have met online, or act on their investment tips.

Artificial intelligence (AI) will make relationship scams even more potent. AI will likely be used to identify potential targets, gather personal information, compose convincing messages, and even keep the dialogue going with multiple targets simultaneously. To read more, Google, “[Relationship Scams](#)”.



Separate issue: You need to be on iOS 16.6.1 on your iPhone and iPad. To update, open “Settings”, select “General”, and then “Software Update”, and if not up to date, tap to begin installation of iOS 16.6.1 Here is a [write-up](#) from Apple on this security update. And, here is a more informative [article](#) from the *Times of Israel*

#96: 23andMe personal data exposure

Originally published in the November 2023 issue of Venturing into our Past (JGSCV)



On October 6, 2023, 23andMe announced, “We recently learned that certain 23andMe customer profile information that they opted into sharing through our **DNA Relatives feature**, was compiled from individual 23andMe.com accounts without the account users’ authorization.” [Read more here.](#)

On October 9, 2023, they issued an update noting that their investigation continues and, “We are reaching out to our customers to provide an update on the investigation and to encourage them to take additional actions to keep their account and password secure. Out of caution, we are requiring that all customers reset their passwords and are encouraging the use of multi-factor authentication (MFA).”

The announcement did not share specifically what data was compromised, or that this data is now available for sale on the dark web. Possibly, a further update from 23andMe by the time you read this will include this. The updates thus far have neither been forthcoming, nor complete. The tone of the updates seems to shift blame to the user, rather than taking any corporate responsibility.

According to Bill Toulas at *bleepingcomputer.com*, “Late last month, a threat actor leaked 23andMe customer data in a CSV file named 'Ashkenazi DNA Data of Celebrities.csv' on hacker forums. The file allegedly contained the data of nearly 1 million Ashkenazi Jews who used 23andMe services to find their ancestry info, genetic predispositions, and more.” [Read more here.](#)

The threat actor apparently obtained passwords that were exposed on other sites and reused on 23andMe. They were then able to retrieve publicly available personal information that users share to facilitate links, including full name, year of birth, city and state, and ancestry information. I have 1,504 DNA “relatives” in 23andMe and so if any of them were hacked, my public information could be seen.

My password on 23andMe is long, complex, and unique. However, this does not protect me from exposure of my publicly available information as others among my 1,504 “relatives” likely reuse passwords and may have been hacked elsewhere. While I considered hiding my public information, or even turning off the DNA Relatives feature, in the end I decided against this.

As genealogists, we know that the publicly facing information in 23andMe is easily found elsewhere on the web. Look yourself up in <https://www.fastpeoplesearch.com/> and you will likely find your name, contact information, even month and year of birth. However, I am disappointed with 23andMe for its lack of internal mechanisms to catch such mass extraction of data, and for its lack of transparency.

In the end, we may learn that the issue with 23andMe goes deeper than the reuse of passwords. At this point, it is too early to speculate. This situation does highlight, however, the need for each of us to use unique, complex passwords for each site that we access, to employ MFA, and to be conscious of the information we share publicly, recognizing that once it is out there, where it will end up is anybody’s guess.

As can be expected in our litigious society, several class-action lawsuits have already been filed against 23andMe. [Read more here.](#)

[Go to Index](#)

#97: Translation tools

Originally published in the December 2023 issue of Venturing into our Past (JGSCV)



&



My Bookbinder / Buchbinder (Бикбиндер) ancestors lived for hundreds of years in Dubno, a town in Rivne Oblast, Ukraine, that was part of historic Volhynia. While my immediate ancestors left prior to WWI, scores of relatives were murdered there in the Holocaust. One of the few who survived was Sheva Beinstock. With her blond hair and Arian looks, she passed as a Christian farmworker.

In 2018, I visited Dubno with my cousin, Boris Fradkin, the son of Sheva. Erna, a friend of his who lives in Dubno served as our guide. I continue to exchange regular emails with Erna. As she does not read English, we communicate in Ukrainian. At first, I used [Google Translate](#) to convert her emails to English and mine into Ukrainian. I have since switched to [DeepL Translator](#).

While most of Google's translations were reasonable, a few were laughably garbled. I found that DeepL provided more consistently credible translations. Google, however, handles 133 languages, including Hebrew and Yiddish; DeepL handles 31. Both provide for translation from images as well as text. So, either can be used to translate a photo of a gravestone or an image of a printed page.

On October 7, a heroic Israeli nurse was severely wounded by rampaging terrorists as she tended to wounded soldiers in Zikim, near Gaza. Controlling the bleeding with a tourniquet, she continued to direct first aid. I used Google Translate to read an image of the Hebrew news article that her mother shared. Here is the [amazing story](#) of my cousin, Michal Elon, as covered in the Times of Israel (in English).

To use the text translation version of [Google Translate](#) or [DeepL Translator](#), copy or type the text to be translated into the left panel and the translated text will appear in the right panel. To use the image translation facility of Google, select "Images"; for DeepL, select "Translate Files". Then, drag and drop the image file into the indicated window. Either may have difficulty translating unclear or fuzzy images.

I even challenged Google Translate to handle the following, carefully written, cursive Cyrillic:

Переплетчики

and, it correctly translated, "Periplichek," as "Bookbinders"

This appears at the top of the entry for my family members in the 1850 Russian Revision List (Census) for Dubno and is apparently a translation of the surname, which would be meaningless to the Russian ear.

At this time of year, charities ramp up their efforts. Please exercise care in selecting charities to which to donate. Some are out-and-out scams. Others spend an obscene amount on fundraising and administration. Still others do not explain how donations will be spent. "[Charity Review Websites](#)" provides considerations and tools to see that your donations make the most difference. Note that the link for IRS charity filings in that article is out of date. Please use <https://apps.irs.gov/app/eos/>.

Happy Channukah, Merry Christmas, and a most Happy, healthy, and especially peaceful 2024.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#98: Password Managers, a 2024 update
Originally published in the January 2024 issue of Venturing into our Past (JGSCV)



When I speak on “Safe Computing”, I typically ask the audience whether they use a password manager. About two-thirds respond that they do. So, about one in three rely on memory or a printed list. If you can remember a password, a hacker can figure it out, and lists can fall into the wrong hands.

Hackers may discover your password by compromising a system in which that password is used. They may discover your password by trial-and-error, using information they uncover about you, like your child’s name, your birthday month, or favorite color. If you reuse the same password, or variations of it, once a hacker discovers it on one site, all other sites where you use it are not at risk.

Steps that you can take to reduce the risk include (1) using a different password for each site that you visit, (2) [strong passwords](#), and (3) [multifactor authentication](#). In the age of artificial intelligence and superfast computing, you are more at risk than ever. So, wherever you can do so, use all three of these techniques to best protect yourself.

As there is no way any of us can remember dozens of strong passwords, we need a password manager to remember them. Password managers can typically enter your ID and password when you are logging in, create strong passwords on request, warn you of weak or potentially compromised passwords, and automatically record passwords that you create or update.

Browsers, like Chrome and Firefox, offer password management. You see this when you are asked by your browser whether you would like it to remember your password. I do not recommend browser-based password management as passwords stored directly in your browser are more easily hacked than those stored in the cloud. See [Dangers of saving passwords in your browser](#).

Many password managers offer a free version along with fee-based versions including additional features. About ten years ago, after evaluating various password managers, I selected LastPass. I found that the free version was easy to use, rich in functionality, and did not constantly dun me to upgrade to a paid version. Recently, LastPass has experienced several breaches, the most serious one in August 2022.

Articles, like this one in [Forbes](#), and LastPass’s own [blog](#), sufficiently concerned me so that I decided that I would no longer use it. After evaluating several free alternatives, I recently switched to Bitwarden, which PC Magazine rates as the “Best Overall” free password manager. Here are links to PC Magazine’s current “best-rated” [free](#) and [fee-based](#) password managers.

Bitwarden has some catching up to fully compare with LastPass. For example, LastPass recognizes when a new password has been created or an existing one updated. Bitwarden does not and so such updates must be manually entered. I expect that Bitwarden will add this important feature as it matures. Review the best-rated password managers and select one that works for you. Don’t delay until you are hacked.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#99: Finding your iPhone, Android, and more

Originally published in the February 2024 issue of Venturing into our Past (JGSCV)



Apple
"Find My"



Google
"Find My Device"



Apple
AirTag tracker



Pebblebee
card tracker

Some months ago, I had a pleasant picnic lunch with a cousin in a local park. When we got up to leave, I inadvertently left my iPhone on the picnic table or bench. A half-hour later, I realized that I did not have my phone and raced back to the park. However, it was gone.

Logging into iCloud on my home PC, I tried to locate it using Apple's "Find My" tool. It did not show the location of my iPhone. I tried for several days and then proceeded to purchase a new iPhone. After setting it up, I decided to give "Find My" one more attempt, from my new iPhone.

It indicated that my iPhone was at a specific address. I drove there and knocked on the door. A lady answered. I politely, but firmly, requested my iPhone. She claimed that she did not know anything about it. My body language communicated that I was not satisfied. She then stepped back and made a phone call, proceeding to whisper in Spanish. I knew enough Spanish to follow the conversation.

The lady was speaking to her son, querying him about the iPhone. She then went to his room and retrieved my iPhone, none the worse for wear. I thanked her and left with a terrific sense of accomplishment. I was able to return the new iPhone to Costco for a full refund. Although I was successful, on reflection, it might not have been the wisest thing for me to go up to a strange house and demand the return of my property.

While I cannot recommend this approach for retrieving lost property, I do strongly encourage Apple and Android users to turn on "Find My" (Apple), or "Find My Device" (Google/Android), and then periodically practice using the feature from another device. Had I not activated, and exercised, the "Find My" feature on my iPhone, it would not have been available when I needed it.

For instructions on setting up the "Find My" feature on your iPhone (or another Apple device), go to: <https://support.apple.com/en-us/102648>. For instructions on setting up the "Find My Device" on your Android, go to: <https://support.google.com/android/answer/6160491?hl=en>. Here is another helpful article: <https://www.foxnews.com/tech/how-find-your-lost-iphone>.

I have a long-standing habit of misplacing things. So, I purchased a set of [Apple AirTag](#) trackers, placing one on my keyring and one in my laptop computer bag. [Pebblebee](#) offers similar trackers, including one shaped like a credit card, fit for a wallet. Pebblebee trackers work with both Apple and Android devices. I am now able to locate my wallet, keys, and laptop from my iPhone, and my iPhone from my PC.

When I was a child, my mother would tell me that I should thank G-d every day that my head was attached (or I would surely lose it). Little has changed. But technology can now help.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#100: Data breach awareness

Originally published in the March 2024 issue of Venturing into our Past (JGSCV)

In prior articles, I have shared the free <https://haveibeenpwned.com/> website to check whether your email address has been exposed in a data breach. If it has not, the site will return:

Good news — no pwnage found!

No breached accounts and no pastes ([subscribe](#) to search sensitive breaches)

When I entered one of my addresses, bookbndr@g.ucla.edu, I got the response above. I was not surprised, as I have never used it as an identifier in any website. However, when I entered hal.bookbinder@ucla.edu, I received the following:

Oh no — pwned!

Pwned in 11 data breaches and found no pastes ([subscribe](#) to search sensitive breaches)

The site goes on to describe each of the eleven breaches, what data elements were captured, and whether the information is for sale on the dark web. Most captures are annoying, but relatively harmless. However, some demand attention, especially if passwords have been exposed.

Rather than checking the site, one can enter their email address into 'Notify me' found at the top of the home page. They will then receive alerts when an email address shows up in a breach. I recently received this alert. →

While I have not used Trello in years, I never deleted my account. My data was waiting to be exposed.

Expect breaches to continue. While you cannot stop them, you can:

- ✓ Limit what you share.
- ✓ Stay aware of known breaches.
- ✓ Delete outdated credentials.
- ✓ Avoid reusing passwords.
- ✓ Update passwords periodically.
- ✓ Use multi-factor authentication.
- ✓ Create an email just for logon IDs.

';--have i been pwned?

You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	hal.bookbinder@ucla.edu
Breach:	Trello
Date of breach:	16 Jan 2024
Number of accounts:	15,111,945
Compromised data:	Email addresses, Names, Usernames
Description:	In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum . Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses. Trello advised that no unauthorised access had occurred.

[Go to Index](#)

#101: Even if you do everything right...

Originally published in the April 2024 issue of Venturing into our Past (JGSCV)



You take reasonable precautions to protect your personal data. You avoid risky sites; you do not click on unknown links; you minimize the sharing of personal information; you have a password manager to support your use of complex and varied passwords; and you opt, wherever possible, for multi-factor authentication. Yet, with all your precautions, your personal data may still be at risk.

Even the largest and most respected organizations get hacked. With advances being made in hacking technology, with bad actors sponsored by hostile governments, and with the use of ever more sophisticated Artificial Intelligence (AI), this will assuredly get worse. Widely used behind-the-scenes software is sometimes compromised, simultaneously impacting multiple organizations.

Typical claims in tech journals include, “92% of Fortune 500 companies rely on ... software”. When one of these widely used products is hacked, the exposure can be enormous. Software companies are generally quick to respond and fix exposures. But, by the time they do so, substantial damage may have already occurred. This is referred to as a “Zero-day exploit”.

Thousands of organizations use Progress Software’s MOVEit Managed File Transfer Software to move data quickly, efficiently, and securely within the data center and across the World (*The illustration above is from the progress.com/moveit website*). This includes a significant number of the most trusted healthcare, government, financial, corporate, and educational organizations.

In May 2023, the ransomware gang, Cl0p, found a Zero-day exploit in MOVEit. 2,000 organizations reported being attacked with data thefts affecting more than 62 million people across the U.S. If you are like me, you received at least one letter from an organization in November or December, letting you know that your data had been exposed by the MOVEit hack.

The letter may have offered free credit monitoring services for a year. It may have recommended that you change your password. It certainly reassured you that the organization takes your security seriously and that they had quickly remedied the exposure. These letters try their best not to unduly alarm. Notwithstanding their reassuring tone, it is important to act.

Consider updating your password for the site, even if this is not specifically recommended. If you are using the same password elsewhere, update them as well. Avoid sharing personal data which may later be exposed. I’ve seen user IDs containing names and birth year. A hacker can use this to obtain an enormous amount of personal information from publicly available databases.

The volume of notices that we get is often daunting. Follow-up notices that we think are simply duplicates may provide additional details and recommended actions. For example, the first alert that I received from 23andMe regarding its 2022 breach claimed that no client data was involved. Later alerts, as they learned more, acknowledged that client data had been extracted.

To reduce the impact of breaches, remain alert and, as needed, act promptly.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#102: Avoiding payment app theft

Originally published in the May 2024 issue of Venturing into our Past (JGSCV)



A 2023 survey by NerdWallet found that 80% of Americans use mobile payment apps, such as Cash App, PayPal, Venmo, and Zelle. Half say that they use these apps at least once a week. Payment apps are a convenient way to send money to a friend, a relative, pay a bill, or donate to a charity. These apps typically offer capable security options. But you may need to turn them on.

In most cases, the fraudster steals your money by gaining control of your unlocked iPhone or Android device. A common tactic is to ask to use your phone to make a quick call. A skilled fraudster can quickly discover your payment app and send money to himself or an accomplice.

Be certain to turn on the app's biometric security feature, so that it checks your Face ID, Voice ID, or Touch ID, before permitting a money transfer. If it does not offer such verification, consider switching to a payment app that does. Check if it can stop, slow, or flag money being sent to unknown parties.

Apple Cash claims, "Your transactions are authenticated with the security of Face ID or Touch ID. Apple Cash will even alert you if you're about to send money to someone that's not in your contacts." Review and turn on the available security features in your payment app. If the app sends alerts, especially for unusual transactions, pay attention to them.

A restaurant server, salesperson, or solicitor for a charity, may offer to help you by entering the payment on your behalf. Generally, this is not a problem. Fraudsters, however, are skilled at gaining your trust. Once they have your phone, they might key in a transfer to their partners in crime. If you are not comfortable entering the transaction yourself, the app does not belong on your phone.

A thief that steals your phone may then attempt to use your payment app. If the phone and app are unlocked or their security codes are easily guessable, you may find your bank account drained. Biometric authentication, on both your phone and your payment app may be the difference between simply replacing your phone and also finding your bank account drained.

If you have an iPhone with iOS 17.3 or later, you can help prevent thieves from accessing your payment apps by enabling Stolen Device Protection. Per Apple, this adds a security delay "designed to prevent a thief from performing critical operations so that you can mark your device as lost and make sure your Apple account is secure."

Review the security settings in your payment app and set them to maximize protection, including biometric verification; ensure that you know the steps to lock down and disable your phone if it goes missing; remove unused payment apps from your phone; don't let others enter payment transactions on your behalf; and be careful to whom you lend your phone.

#103: One of the biggest breaches that you never heard of
Originally published in the June 2024 issue of Venturing into our Past (JGSCV)



On May 14, I received an email from “Have I been Pwned?” alerting me that my information had been exposed in a data breach of “The Post Millennial”. I had never even heard of The Post Millennial. On checking, I learned that this is a conservative Canadian news site. I am certain that I had never accessed it. Yet, my data is currently for sale on the Dark Web!

Per “Have I been Pwned?”, the database that was hacked was consolidated from a variety of mailing lists, not all of them controlled by The Post Millennial. On May 2, 2024, it was breached. Data on 56,973,345 accounts was exposed and quickly made available for sale. The compromised data included some or all of the following: Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses, and Usernames. There was no mention of passwords.

It appears to me that this was a database used for advertising and so I expect to see even more spam than I already get. If I had an account at ThePostMillennial.com, I would have immediately changed my password. But not knowing the actual source of the data, I have no idea what password or passwords to change. To limit damage from any such breach, I use different [strong complex passwords](#) for all websites on which I have accounts, and [multi-factor authentication](#) where I can.

Several days after being notified by HavelBeenPwned.com (note that there is no “a” in Pwned), I was notified by Experian that my data had been exposed. The information provided by Experian was not as specific nor informative as that provided by HavelBeenPwned.com. I was notified because I had entered my email address into the “Notify me” feature at HavelBeenPwned.com. There is no charge for this service.

Check it out by going to the site and entering your own email address to see if it is for sale on the Dark Web. If you prefer, enter my email, hal.bookbinder@ucla.edu. Scroll down and you will see that my data has been exposed in a dozen breaches. Oddly, they are in alphabetical, rather than chronological order, with the seventh being The Post Millennial breach.

You will also notice that I was part of the Twitter breach in 2023, the LinkedIn breach in 2021, the MyHeritage breach in 2017, and the Dropbox breach in 2012. To date, HavelBeenPwned.com has recorded over 13 billion exposed accounts. Your email and associated data have likely already been exposed. I encourage you to sign up with HavelBeenPwned.com for quick, meaningful, notifications.

If the summary for the breach indicates that passwords have been exposed, change the password on the affected site(s) immediately. If you have used that password elsewhere, change it there as well. Most breaches are used to feed advertising spam operations and are more annoying than dangerous. By reading the explanation at HavelBeenPwned.com, you can determine whether to act or just to be annoyed.

#104: Free product trials

Originally published in the July 2024 issue of Venturing into our Past (JGSCV)



Online services, subscriptions, and applications often provide a free trial period. You understand that if you do not cancel prior to the end of the trial period, your credit card will be charged, and the charges will continue until you cancel. Typically, once a charge is made, the company will not reverse it simply because you neglected to cancel on time.

They count on some finding the product well worth the cost and consciously deciding to continue their subscription. They count on others procrastinating, forgetting, or simply giving up on cancelling before the trial period has ended. It is up to you to understand clearly how to cancel and to do this prior to the end of the trial period.

While this is fair and reasonable, the cancellation process is not always easy or obvious. You might expect that if you log into the site, there would be a button to cancel. However, this is not typically the case. You may have to search for it. And, sometimes, it cannot be found at all. Don't wait till the trial period is about to expire to discover this.

Recently, I signed up for the trial period of a popular suite of applications, providing my credit card and agreeing to be charged a monthly fee starting at the end of my trial. If I had agreed to an annual renewal, the price per month would have been considerably less. As I did not want to be on the hook if I somehow missed the deadline, I opted for the monthly option.

As the deadline for the trial period approached, I decided that, while I liked it, I did not find sufficient value in the product to pay \$29.95 each month. I logged into the product and tried every conceivable link to cancel my subscription. Finally, I gave up and searched my emails for the subscription confirmation to see if it had cancellation instructions.

The confirmation provided a link to cancel the subscription. I clicked on it and none of the displayed links seemed to relate to cancellation. I tried the various links and found the one which took me to the cancellation option. I clicked on it and was presented with a screen that highlighted the great features of the product, encouraging me not to cancel.

I paged down and found the button to confirm my cancellation. Once I chose it, I was presented with yet another page that let me know that they were sorry to see me go and again touted the great benefits of keeping my subscription. Had I assumed that I was through, I would have remained subscribed. However, when I paged down, I found yet another, and final, cancellation confirmation button.

The lesson here is clear. When you sign up for a trial period, read the materials carefully to be clear on the cancellation process. If the confirmation email includes a cancellation link, be sure to keep it handy. If you must call a phone number, be wary. If you get through, you are sure to be speaking to a most convincing agent whose employment is based on their ability to keep you as a customer.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

#105: Accidental and criminal cyber disruption

Originally published in the August 2024 issue of Venturing into our Past (JGSCV)



Two events during July foreshadowed the cyber-World to come. One was the Worldwide computer disruption that impacted air travel, hospitals, government agencies, and more. This was reportedly due to a faulty update to CrowdStrike's "Falcon"

cybersecurity software. The irony is that the purpose of this software is to protect CrowdStrike's customers from disruption.

CrowdStrike's Falcon software is used by thousands of organizations to guard against cyberattacks. As cyberattacks are constantly morphing and new ones appear hourly, CrowdStrike is constantly sending updates which are immediately installed by these organizations on upwards of 500,000 individual computers across the World. So, when something goes wrong, it can be hugely impactful. What made this one so disruptive was that it was not quick or easy to uninstall.

Although the faulty update was remedied within 90 minutes, each machine that had the upgrade had to be fixed manually, including stripping the faulty update and performing several machine reboots. Today's upgrade and fix processes tend to be highly automated with few staff maintaining hundreds, if not thousands of machines apiece. Airlines, and especially Delta seemed to be the most impacted, though a number of hospitals had to cease all but critical care for several days.

Common software is used across industry and government for managing and moving data, for cybersecurity, for operational monitoring, for communications and much more. The challenges of a fast-changing and dangerous world require that updates be installed immediately, without individual testing by each receiving organization. Since time is of the essence and staff is expensive, companies have tended to shift to trusting suppliers and reducing internal testing staff.

We will undoubtedly experience more widespread disruptions due to such shared software and the need to rapidly deploy updates. Some of this will be due to human error, as was apparently the case with CrowdStrike. However, I expect that cyberterrorists working for enemy states have already implanted time bombs in shared software that they will be able to wake up when they wish to create maximum worldwide disruption, akin to "sleeper cells", of years past.

The other event, which did not get nearly as much publicity, was a ransomware attack on the Los Angeles County Court System, the largest such system in the nation. Scores of courthouses had to close for several days after which they quickly returned to full operation. Such a rapid recovery likely indicates that the cybercriminals were paid to unlock the Court System's data. However, as is often the case, the County has refused to comment as to whether a ransom was paid.

Ransomware is highly profitable for cybercriminals. Establishing and maintaining a security infrastructure to protect from ransomware attacks is expensive and technically challenging. Sadly, it may be cheaper to simply pay off the criminals. Typically, this is done with as little publicity as possible. Ransomware cybercrime is hugely profitable, and many organizations are easy prey. Significant ransomware comes from criminal operations in Russia, beyond the reach of U.S. law.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

Your password has expired

Originally published in the November 2024 issue of Venturing into our Past (JGSCV)

Your UCLA password has expired. You must update it now.

Have you received notices that your password has expired or will shortly expire? These notifications claim to be from your employer, bank, brokerage, or even the government, and make it clear that action is required, or you will be locked out.

Don't fall for it. Invariably, these are bogus notices designed to steal your identity. Once you click on the link you will be asked to identify yourself by entering your current ID and password, along with the new password. It might even ask for additional information like your email and cell phone. The screen appears legitimate with appropriate wording, layout, and graphics for that institution.

Once you enter the information, it will display an error screen with something like, "We are unable to process your password reset at this time. Please try again later."

You have just provided your ID and password to cyber criminals who will now use it themselves or sell it on the dark web. You should, of course, ignore and delete any such message that you receive. If you do fall for it, immediately go to the actual login site for the institution and update your password, before a cyber thief has the chance to use it.

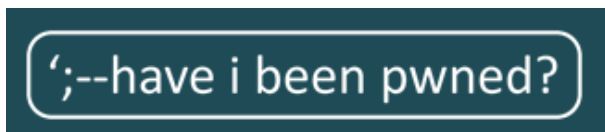
Since we tend to reuse IDs and passwords, or variations of them, you must also log in to any other sites for which you use these, or similar credentials, and update them as well. I know of folks who repeatedly use the name of their dog, and simply append a number or a special character. (for example, Rover, Rover1, Rover2, Rover!, Rover1!, etc.).

Once the cyber criminal has a version of your password, they can use automation to try out variants on different sites, counting on the fact that many of us recycle them.

Legitimate institutions do sometimes require you to update your password. However, I have never heard of one sending out emails requiring you to do so. Rather, they will notify you once you actually log into their site that you must update your password and will typically take you directly to the security or profile page to do so.

While two-factor authentication does provide an extra level of security, and should be used where possible, any personal or credential information that cyber criminals are able to gather puts you at risk.

ON ANOTHER TOPIC



My March 2024 article, [Data breach awareness](#) discussed the [Have I been Pwned?](#) website. This site will alert you when it finds your email or password on the dark web in a major data breach. I encourage you to avail yourselves of this valuable free service. I was just notified my information was included in a 9/28/2024 breach of over 31 million accounts from the Internet Archive. The faster you are aware of a breach that exposes your data, the quicker you can take action to protect yourself from cyber harm.

[Go to Index](#)

© 2015-2024 by JGSCV and by Hal Bookbinder, permission to copy granted with appropriate attribution.

Hal Bookbinder bio



Hal is originally from Newark, NJ. His family then moved to the “Catskills” of New York State where his great-grandfather had settled in 1917. He experienced the heyday and decline of the “Borsht Belt” working as a waiter in the resorts. Hal earned his bachelor’s degree from New York University majoring in Math and Physics, remaining at NYU to earn a master’s degree in operations research.

He then spent four years on active duty with the U.S. Air Force, tracking satellites from within the Cheyenne Mountain Complex in Colorado Springs. His unit continues with this function as a component of the U.S. Space Force. See the [November 2016 issue of *Venturing into Our Past*](#) for an article on Hal’s experience there during the 1973 Yom Kippur War. While on active duty, he

earned a master’s degree in business. After active duty, Hal remained in the USAF Reserves, achieving the grade of major.

On leaving active duty, Hal settled in Los Angeles, first working as an IT professional for ARCO and then for UCLA Health. His final position at UCLA Health before his retirement in July 2020 was as Director of IT Strategic Finance. He remains on the faculty of the University of Phoenix, where he has taught courses in business, project management, mathematics, and information technology. As a volunteer, Hal created and directed a transition-to-work training program for individuals in recovery at the Los Angeles Midnight Mission and at its associated Homelight Family Living Center.

He continues to research eight family lines (Bookbinder, Barenberg, Horwitz/Milstein, Sacharow, Newmark, Yvelson, Biller, and Schwartz), identifying over 4,000 relatives. His direct male line extends to his 5th great-grandfather in Dubno, Ukraine. See the [March 2024](#) and [April 2024](#) issues of “Venturing into Our Past” for articles on how he used the 1850 Russian Revizskie skazki in his Bookbinder family research.

Hal has served as president of the JGSLA and of the IAJGS. He has been a member of the JewishGen Board of Governors and currently serves on the JewishGen Ukraine Research Division Board of Directors, and as town leader for Dubno. He has co-chaired several IAJGS Conferences, first in 1990 and most recently in 2014. Hal received the IAJGS Lifetime Achievement Award in 2010.

Hal has spoken at most IAJGS conferences over the past 30 years. His current presentations include:

- Bookbinder’s Restaurant, Philadelphia
- The Changing Borders of Eastern Europe
- Jewish Fraternal Organizations of the early 20th Century
- A Murder in Boston’s West End
- Obtaining, losing, and regaining American citizenship
- One Family’s Shoah Survival Stories
- Practicing Safe Computing in the time of Artificial Intelligence (AI)
- The Rise and Decline of the Catskills
- Ships of Our Ancestors
- Why did our Ancestors Leave a Great Place like the Pale?

Hal, his wife, Marci, their four adult children and four grandchildren reside in the Los Angeles area. He can be contacted at hal.bookbinder@ucla.edu.

[Go to Index](#)