By Joanna F. DeFranco

Teaching Internet Security, Safety in Our Classrooms

"HERE IS THE WAKEUP CALL: **THE FBI HAS MADE CYBERCRIME ITS NUMBER THREE PRIORITY, FOLLOWING TERRORISM AND COUNTER-INTELLIGENCE."**

PHOTO BY STOCK.XCHNG.COM

THERE IS A MISCONCEPTION: "KIDS KNOW MORE than We Do About the Internet." Do teens know more than their parents and teachers about how to *use* the Internet? Teens may be more familiar with the latest blog or social networking site; however, with 56 percent of teens posting personal information (McAfee, 2010) on the Internet and child predators and criminals looking for this information—I think not.

Here is the wakeup call: The FBI has made cybercrime its number three priority (fbi.gov, 2010), following terrorism and counterintelligence. In addition, cyber criminals are scraping the social networking sites, using the automated free tools available on the Internet, to collect the personal information posted by social network users so they can more easily commit crimes. On the bright side, many of the issues can be mitigated with a few simple steps to increase the difficulty of criminals gaining access to our personal information, and potentially us.

Educators Need to Take the Lead

Internet security is an important topic for educators due to curriculums now incorporating tools such as the Internet, Google docs, e-portfolios and course management systems. Those tools require students to spend more time online, where they are susceptible to manipulation or intimidation if they do not stay on task. Kids of all ages lack emotional maturity. They also need attention and validation; combine that with their extreme lack of caution, and a broadband connection, and we now have a big problem.

The problem is best described with terms coined by Marc Prensky (2001). He referred to people who did not grow up with the Internet as the *Internet Immigrants* (over 30 years of age), and the *Internet Natives* are those who grew up with the Internet (under 30 years of age). The problem is that the *immigrants* are raising the *natives* and assume the natives know what they are doing because they have so much interest in the latest technology. Unfortunately, the focus is on obtaining and using the bells and whistles of the new technology, rather than the dangers that come along with it.

Immigrants raising natives is not a new situation. For example, in the early 1900s when immigrants arrived from other parts of the world, they needed to focus more on feeding their families than educating their children. They accomplished this by sending young children to work instead of school—obviously dangerous, but probably necessary. Laws were then created to make sure all children attended school. Our society cannot wait for Internet safety to be a required part of the curriculum or depend solely on parents who may not have the knowledge to teach Internet safety.

Why is it Suddenly OK to Talk to Strangers?

Technology has allowed us to obtain knowledge in a most efficient way. However, utilizing that technology is also leaving us vulnerable to exploitation. We tell our children not to talk to strangers, yet that is exactly what they are doing on the Internet. As mentioned earlier, more than half of teens are posting personal information such as name, age and address, and are chatting with people they have met in chat rooms and social networking sites. The Internet is misleading in that people use it in seclusion, feeling somewhat anonymous and safe when they post their personal accounts and photos. People are posting where they live, not only with text, but with the photos taken from their smartphones. Taking pictures using mobile phones with GPS capability will embed the longitude and latitude of where the photo was taken. Therefore, if you post a photo on a social networking site taken in front of your house using your smartphone, and mention you are going on vacation next week or that you work every day—you have just sent an open invitation to a burglar.

Online Predators

There are not enough FBI agents to locate and arrest every online predator. Therefore, it is important for educators to teach young people of all ages about the dangers of the Internet. A great resource for educators to teach kids of all ages about Internet safety is *netsmartz.org.* This Web site contains content (videos, PowerPoints and activities) for parents, teachers and children of all ages that helps to stress important issues such as: never meet someone in person that they have met online, or give out personally identifying information. Monitoring a child's technology use can be overwhelming. The FBI suggests a few signals to determine if a child is a target of an online predator:

- Child spends large amounts of time online.
- Child receives phone calls from people you don't know.
- Child turns monitor off when you come into the room.
- Child becomes withdrawn from the family.
- Child receives gifts through the mail (bus tickets, mobile phones, Web cams).

PHOTO BY ISTOCK.COM

> "INTERNET SECURITY IS AN IMPORTANT TOPIC FOR EDUCATORS DUE TO CURRICULUMS NOW INCORPORATING TOOLS SUCH AS THE INTERNET, GOOGLE DOCS, E-PORTFOLIOS AND COURSE MANAGEMENT SYSTEMS."

The FBI suggests keeping computers in a common room. Think hard before buying a device that has Internet capabilities. Set ground rules for use if purchased. Communicate with kids about the potential dangers on the Internet. Use real examples that will resonate with kids. A suggestion specifically for parents is to maintain access and randomly check their children's activities on any social network and e-mail accounts.

Teens and Mobile Phones

The two main problems that are in the limelight right now regarding kids and mobile phones are sexting and texting while driving. LG Mobile Phones sponsored a study surveying 1,017 teens. The study showed that 45 percent of teens admit to texting while driving, and 41 percent admit to some form of sexting (sent, received, or forwarded a text with sexual content). Eight students from a Pennsylvania high school recently learned a tough lesson about sexting. The teens, who all knew one another, were accused of using their mobile phones to take and send nude photographs of one another, resulting in a felony pornography charge for each of the teens (Miller and Hirschkorn, 2010). Some teens do not realize sexting is against the law. Even if they are familiar with the law, they may not think they will get caught. They need a reminder that once you send something out, you can't take it back; there is also a chance that whatever they are sending can become viral (each person sending to another and so on).

No one would argue that texting while driving is an extreme problem. There are laws in some states outlawing texting while driving. However, laws are not enough, since people can hide the phone while they are texting—or again, do not think they will get caught. Granted, once an accident occurs, texting can be verified simply by analyzing the mobile phone. Obviously, at this point it is too late; the accident has occurred. It would be beneficial for parents to install software on their children's mobile phones that either prevents texting while driving, or redirects phone calls and texts (using GPS to determine speed). A number of companies have already announced various solutions to prevent texting while driving (Purdy, 2010).

Another solution is setting expectations and rules for cell phone usage; sometimes the teens engage in this behavior because they think mom and dad aren't checking the phone. Talk to teens about the legal ramifications of sexting and texting while driving.

Viruses

Viruses are not a new problem, but they are certainly a bigger problem than ever before. In the past, hackers needed a high skill level even to create a relatively simple virus. Now, due to the extensive knowledge base on the Internet, very sophisticated viruses can be created with a relatively low skill level. Users can mitigate this problem just by being cognizant of the latest scam. One way to avoid a virus is don't be so quick to click! Pop-up windows that prompt users to download antivirus software or claim that they will scan your computer for malware are probably scams. Clicking on them could install the malware on your computer. Sometimes these FakeAV (Fake Antivirus, Rogue Antivirus, ScareWare) are sent directly to the victim as an attachment or as a link in a spam e-mail message (SOPHOS, 2010). The e-mail message will prompt a user to visit a Web site where they will be asked to pay for the elimination of the nonexistent virus.

Phishing Scams

Another danger to Internet users is phishing scams. Users are lured to provide personal information, typically through e-mail and instant messaging. Criminals use *botnets* (robot networks), to perpetuate phishing scams. Botnets are multiple computers that are infected with a virus that enable a single hacker to remotely control the infected computers to send out

“INTERNET SAFETY SHOULD BE TAUGHT AS PROACTIVELY AS OUR WOOD AND METAL SHOP TEACHERS TAUGHT US SAFETY IN JUNIOR HIGH BEFORE WE USED THE CIRCULAR AND TABLE SAWS; THE PREDATORS AND CYBER CRIMINALS ARE JUST AS DANGEROUS.”

e-mails. The botnet will enable thousands of e-mails to be sent out appearing to come from a legitimate source. The e-mail will ask for sensitive personal information that some victims will provide. For example, if you receive a message from what appears to be a bank, you should avoid replying to the e-mail and avoid clicking on any links. This is a common phishing scam designed to convince you that your money is at risk. Other scams attempt to trick you into clicking on links by promising huge profits for little or no investment.

These are all forms of online “social engineering,” a term popularized by hacker turned consultant Kevin Mitnik. Social engineering is a non-technical intrusion that relies on manipulating people into divulging confidential information. Cyber criminals find ways to trick users into providing sensitive information such as passwords via e-mail, instant messaging and social networking sites. Another example of a social engineering scam is e-mail messages imitating a network administrator attempting to fix your e-mail or bank account.

“Free” Applications

As we should know—nothing is free. The applications you can get on social networking sites or on the Web for your smartphone may be costing you your personal information. Even if you are using social networking with the strictest privacy settings, your information is not safe. Recently it was discovered that Facebook apps have been providing user personal information to dozens of advertising and Internet tracking companies (Steel and Fowler, 2010).

It seems that cyber criminals are also targeting smartphones. This is for a couple of reasons: sales of smartphones have increased over the past year, and it is convenient for users and developers to download and create applications for their smartphones. In addition, the mobile-phone operating systems are unsophisticated in regulating access to private information such as name and location of the phone user (Enck *et. al.*, 2010).

An inter-unversity team of researchers developed an application called TaintDroid that determines if a smartphone application captures users’ private information. The researchers randomly selected 30 applications and found that two-thirds of the applications suspiciously handled the user’s sensitive information. In addition, half of the applications they tested sent the user’s location to remote advertising servers (Enck et.al., 2010). This may make teens think twice about downloading the cute Disney wallpaper for their phones.

Looking Ahead

The technology that is available to students and educators can be a very effective way to enhance curriculum and instruction. However, the educator needs to take a part in the responsibility of teaching the students how to use the technology safely. Our students are the next generation of our workforce, and these are additional life skills that need to be taught. Internet safety should be taught as proactively as our wood and metal shop teachers taught us safety in junior high before we used the circular and table saws; the predators and cyber criminals are just as dangerous.

References

Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., Sheth, A. (2010). “TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones.”

Prensky, M. (2001, October). “Digital Natives, Digital Immigrants,” *On the Horizon*, MCB University Press, Vol. 9, No. 5.

Purdy, J. (2010, March). “Inside Mobile: Using Mobile Technology to Prevent Texting While Driving,” *Enterprise Mobility.*

SOPHOS. (May 2010). “What is FakeAV?” A Sophos white paper.

McAfee. “The Secret Online Lives of Teens.”

Steel, E., Fowler, G. (2010, Oct. 18). “Facebook in Privacy Breach,” *The Wall Street Journal.*

Myers, D. (2010, Sept. 25). “Popularity of Social Networking Sites Leads to More Home Burglaries,” *Bucks County Courier Times.*

Acohido, B. (2010, July 30). “Banks Seek Customers’ Help to Stop Online Thieves,” *USA TODAY.*

Acohido, B. (2010, Aug. 3). “Cybercrooks Use Web Apps to Infiltrate Smartphones,” *USA TODAY.*

Miller, M., Hirschkorn, P. (2010, June 5). “Sexting Leads to Child Porn Charges for Teens.” *CBS News.*

Joanna F. DeFranco, Ph.D.,

is assistant professor of software engineering, Penn State University School of Graduate Professional Studies. She can be contacted at jfd104@psu.edu.