Lesson 7

How to avoid cyberscams

By Jon Swartz
USA TODAY
October 9, 2008

Cybercrooks are exploiting the financial crisis to step up attacks on banks and their customers with malicious software, spam, phishing scams and other online tricks.

Computer-security vendor Proofpoint offers some useful tips on how consumers can best protect themselves:

1. Be aware. View with suspicion any e-mail with urgent requests for personal IDs, financial information, user names or passwords. Your bank, online services or legitimate e-commerce sites are unlikely to ask you for this type of information via e-mail. You should be extremely suspect of similar e-mail that appears to come from an employer. Never send personal financial information or sensitive information such as Social Security numbers via e-mail.

2. Don't click. If you receive a suspicious e-mail, don't click the links in that e-mail to visit the website in question. These links may take you to a fraudulent site that looks similar or identical but is designed to steal your personal information. Never click on a file attachment unless it's from a completely trusted source.

3. Be secure. When you are shopping online, entering important information such as credit card numbers, or updating personal information, make sure you're using a secure website. If you are on a secure Web server, the Web address will begin with https:// instead of the usual http://. Most Web browsers also show an icon (such as Internet Explorer's "padlock" icon) to indicate that the page you are viewing is secure.

4. Don't fill out e-mail forms. Never fill out forms within an e-mail, especially those asking for personal information. Instead, visit the company's website and ensure that the page you are using is secure before entering sensitive information.

5. Keep an eye on your accounts. Check the accuracy of your credit card and bank statements on a regular basis, especially during a time like this. If you see anything suspicious, contact the financial institution immediately. Banks that have gone through a transition are also communicating on their public websites.

Lesson 7

Introduction

The best way to avoid becoming a victim of cybercrime is to learn how to identify it. But how do you know what to look for? Read the article for some quick, practical tips on how to keep your personal information yours alone!

Discussion

1. What information should you never send by email? Why?
2. What file attachments are safe to click on?
3. If a file comes from your best friend, but you weren't expecting it, what should you do with it? Why?
4. How can you tell if a website is secure?
5. One safety tip says not to fill out forms that are inside emails. Why?
6. If you really think that information is legitimate and necessary, what should you do instead of filling out an email form?
7. Why do you need to keep an eye on your accounts?
8. If your account is compromised (whether it be a bank account or online social media account), what should you do?
9. What scams have you seen? Have you fallen for them?
10. What kinds of cybercrimes target youth? Have you known victims? What happened?

Activity

1. Some of the tips in the article apply more to adults. In small groups of three, create a set of tips for students your age on how to spot cybercrime and how to avoid becoming a cybercrime victim.
2. Check what you would consider the five most important tips on your list.
3. Create the content for a wiki, website, podcast or video announcement designed to share your tips with students your age. Remember, your goal is to get students to read or hear all of your tips and then use them, so be creative and persuasive!

Lesson 7

TEACHER'S GUIDE

Overview:

In this lesson, students will:

- Read the article, "How to avoid cyberscams."
- Brainstorm tips to share with classmates on how teens can become more cybersavvy.
- Share these tips through a creative and persuasive presentation.

Grade level:

6-12

Subject areas:

career and technical education, language arts, social studies, advisory classes

Time requirements:

Step 1: Read the article (10 minutes).
Step 2: Discuss the article using the questions provided (15 minutes).
Step 3: Brainstorm cybersafety tips and develop presentation (55 minutes).
Total: 80 minutes in class (Note: Times may vary according to students' grade and ability levels.)

Notes:

1. You may want to preteach the following terms: exploiting, malicious, phishing and vendor.
2. Discussion Question 3: If you receive a file you're not expecting, check with the sender to make sure he/she sent it, and not a hacker or spammer.
3. If you want to provide additional tips for youth on staying safe on social media sites, go to: http://www.staysafeonline.org/blog/staying-safe-social-media-web-sites.
4. If you have time, students can take the cybercrime quiz located at this website: http://www.symantec.com/norton/cybercrime/quiz.jsp. Once they answer the 10 questions and hit "submit," they'll see how many they got right and the reasons behind each correct answer.

Links:

- National Cyber Security Alliance: www.staysafeonline.org
- United States Computer Emergency Readiness Team: www.us-cert.gov
- i-SAFE: www.isafe.org
- Wired Safety Organization: www.wiredsafety.org
- Federal Trade Commission: www.onguardonline.gov
- Multi-State Information Sharing and Analysis Center: www.msisac.org/awareness
- ConnectSafely: www.connectsafely.org/safety-tips-and-advice.html
- iKeepSafe: http://tools.ikeepsafe.org/older-students
- FBI's Internet Crime Complaint Center: www.IC3.gov