PLTW COMPUTER SCIENCE

Activity 2.3.1

The Vulnerable User

Introduction

“Employees must wash hands before returning to work.” Have you ever seen that sign? It’s required by law in many states to be posted in restaurant bathrooms. Why is everyone’s participation required to reduce the population’s risks from disease?

Our nation has a dire need for people – as employees, citizens, and consumers–to practice good cyber hygiene. What does that mean? Why is it so important? What are the worst-case consequences?

Image courtesy of ©2005 CDC

Materials

- Computer with Internet access

Procedure

Part I: Ethics

1. Form pairs as directed by your teacher. Meet or greet each other to practice professional skills.
2. All people are expected to follow ethical standards for computing. These include accessing computing resources only when authorized to do so. Computing professionals are held to strict ethical standards. Even a single attempt to access computing resources without authorization can result in losing a job, being expelled from a university, or being banned from a professional organization.

   Consider the following two scenarios. With your partner, decide if Rob has behaved unethically. If his action was unethical, explain why and describe what you think the consequences might be. If his action was ethical, describe what additional actions would have crossed the line into unethical behavior.

   - Rob is sitting next to Tanya, who is entering a password on a website. Rob watches her type and memorizes her password. He uses it once to see if it really was her password and immediately logs out. He never uses it again.

    - Rob is given access to a computing network. He discovers that the computing system allows him to look at directory listings of other users' files. He wonders if he'd be able to read their email. Without any special effort, he succeeds in listing the titles of other people’s email messages. He decides not to try to read one of the messages. He does not report any of this to the system administrator.

3. The **Association for Computing Machinery (ACM)** is the leading professional organization for computing specialists. Read the text of the ACM’s Code of Ethics, Parts 1.7 and 2.8, at **https://www.acm.org/about/code-of-ethics**. Were Rob’s actions described in the previous step unethical according to the ACM Code of Ethics? Explain your opinion, citing specific wording from the Code of Ethics.

Part II: Impact

4. > Refer to your downloadable resources for this material. Interactive content may not be available in the PDF edition of this course.

While some cyber attacks affect high-level military and commercial targets, the majority of attacks are against consumers and small businesses. These attacks increased more than 40% in 2012 over the previous year (Symantec 2013). Attacks on individual users contribute to attacks on business and government because an attacker uses the individual consumer’s device to stage additional attacks.

Society needs everyone to improve their cyber hygiene!

Brainstorm specific consequences we risk as a nation if we do not attend to cyber security in our own lives. Consider consequences to yourself, your community, your employer, and to the larger infrastructure. Write out your list of ideas. Two have been given to get you started.

- Cyber attackers could steal money from my bank account.
- Cyber attackers could disrupt the electricity grid.

5. As a class, brainstorm stories you have seen, read, or heard about cyber attackers causing or attempting personal or economic harm. Collect separate lists for factual and fictional stories. Optionally, your teacher might ask you to find factual news stories and collect the events on a map or timeline.
6. Why do attackers want to control other people’s computers? Control of your computer gives an attacker data, processing power, and bandwidth to reach other computers. Attackers have their own purposes for each of these categories.
    - An attacker might want data for many reasons. Add one reason to the list.
        - To get your email credentials so they can send spam as you.
        - To get your contact list so that the attacker can trick your friends into trusting them.
    - An attacker might want processing power for many reasons. One reason is to factor large numbers. Why might this be useful to a hacker?

- An attacker might want to use your access to the Internet. An attacker might work through your Internet access to deliver a denial of service attack (DoS), in which legitimate users are prevented from accessing a web site or other service, either by making the service crash or by tying it up with a flood of bogus requests. Why would an attacker work through your computer to do this instead of acting directly from their own computer?
- Cyber attackers also use infected computers for launching a distributed denial of service (DDoS) attack. While a DoS attack overwhelms a server by sending a flood of requests from one source, a *distributed* DoS makes the flood of requests from many senders. Explain why a DDoS attack is harder to defend against.

Part III: Malware and Vulnerabilities

7. The objective of an attacker is usually to install malware, adware, or spyware. The term malware is sometimes used to include all three of these categories. All these categories can be described as the attacker's payload. Various additional terms are sometimes used to categorize types of payloads. Review the presentation **Types of Malware**. Summarize what distinguishes the categories from each other.

   Refer to your downloadable resources for this material. Interactive content may not be available in the PDF edition of this course.

8. Often, a vulnerability in software is exploited to install malware. A vulnerability is an error or oversight in software that allows a hacker to access or affect computing resources. An exploit is particular input or data that takes advantage of the vulnerability.
   - With your partner select one or more (as directed by your teacher) from the following list of attacks and malware families.
     - Ping of death
     - Flame
     - SQL injection
     - Sality
     - MyDoom
     - Man in the middle
     - ILOVEYOU
     - ZeroAccess
     - Samy worm
     - Stuxnet
     - Melissa virus
     - Conficker
   - Spend a few minutes skimming web pages about the attacks or malware families you selected in Step 8a. Describe each of the following as applied to the attack you selected.
     - Identify the vulnerable software or language.

        - If easily determined, describe the vulnerability. In general terms, what is it about the software that allows the malware to get installed?
        - If easily determined, describe the exploit. In general terms, how does an attacker use the vulnerability to deliver a payload?
        - Describe the timeline. When was the malware first observed? If there is a patch, when was it released? A **patch** is an update to software that fixes a bug or vulnerability.
    - As directed by your teacher, summarize one of the attacks or malware families for another pair of students or the class. Record the information from Part b for the attacks or malware described by other students.

Part IV: What You Can Do

9. As part of routine cyber hygiene, you should maintain your privacy. Once digitized, data might linger forever.

    - As a team of two, pick one of the slides in the presentation **Protecting Your Identity**, as directed by your teacher. Each slide is likely to be assigned to multiple pairs.

    Refer to your downloadable resources for this material. Interactive content may not be available in the PDF edition of this course.

    - Prepare a 45-60 second narration to present the slide. Use at least one additional source of information to inform yourself as you prepare. Record your reference source and make a written version of the narration you prepare. Narratives should provide more information than what is on the slide. Do not read from the slide.

10. For cyber hygiene, be conscious of cybersecurity whenever you are using a computer. Most intrusions can be prevented by following simple cyber hygiene guidelines (Wallace, 2013). Most intrusions are accomplished by **social engineering** in which the user is tricked into clicking on a link, installing software, opening a file, or answering questions.

    - As a team of two, pick two of the slides in the presentation **Social Engineering**, as directed by your teacher. Each slide is likely to be assigned to multiple pairs.

    Refer to your downloadable resources for this material. Interactive content may not be available in the PDF edition of this course.

    - Prepare a 45-60 second narration to present the slide as described above.

11. To have effective cyber hygiene, we need to maintain security on our devices.

   - As a team of two, pick one of the slides in the presentation **Software for Cyber Hygiene**, as directed by your teacher. Each slide is likely to be assigned to multiple pairs.

     > Refer to your downloadable resources for this material. Interactive content may not be available in the PDF edition of this course.

   - Prepare a 30-60 second narration to present the slide as described above.

12. Present the slides from Steps 8-11 in collaboration with the full class.
    - You will probably only present one or two of the slides you prepared, as directed by your teacher. When your slide is shown, stand up and give your narrative.
    - Take notes on other students' presentations, and after the presentations are all completed, review with your partner and summarize in writing the advice presented for each slide.

Conclusion

1. Gail Brown wants to use the Internet to pay a bill from CoolStore. She knows her username and password for the CoolStore company’s website for paying bills online. Gail considers each of the following methods for paying her bill. Describe the attack that could be underway in each applicable case.
   - Gail googles the name of the “coolstore” and follows the first link provided. It looks like the familiar website. It is using http. It asks for her username and password.
   - Gail gets an email reminding her to pay her bill and follows the link to https://coolstore.com. That website looks familiar and asks for her username and password.

2. You get an email from a friend:

   Check this out: http://lkjfdg.ru/7gfd9

   What should you do, and why?

3. Suppose you own an iPhone and you get an email from Apple. It says:

   You recently initiated a password reset for your Apple ID. To complete the process, click the link below.

   https://iforgot.apple.com/verify

   This link will expire three hours after this email was sent. If you believe an unauthorized person has accessed your account, you can reset your password at https://appleid.apple.com

Despite what the email says, you haven't visited the Apple Store this week and definitely didn't request a password reset. What should you do, and why?

4. The introduction compared practicing cyber hygiene to washing hands. How are they similar?