Info for educators – Cybersecurity Safety – Fall 2019

Module Description

This module reviews some of the common and typical cybersecurity threats and vulnerabilities for personal computers. Information includes phishing, malware and social engineering. Included is advice for maintain the security of your computer and information when on the internet.

Module contents

1) Recorded lecture (approx. 45 minutes)
2) Slide deck materials (pdf)
3) Discussion topics (below)
4) Suggested assignments and activities (below)

Student Learning Outcomes

- Develop student knowledge of the fundamental threats and vulnerabilities with respect to use of a personal computer to access the internet.
- Understand and recognize phishing – characterize typical phishing messages and be able to identify phishing messages.
- Understand the concept of social engineering and how it is used to gather information or influence actions.
- Understand how malware is delivered.
- Understand actions to prevent becoming a victim and protect one's personal computer from malware.

Time/Effort

- Recorded lecture – approx. 45 minutes
- Activities – approx. 2 hours
- Discussion: 30 – 60 minutes

Suggested Discussion Topics

1) Has your computer ever been compromised by malware? Describe what happened and the steps you had to take to recover from that.

2) One of the reasons that phishing is such a problem is that the criminals can easily create anonymous email accounts at places like gmail.com. *(Those of you who have taken the Privacy & Social Media module: what do you think is the motivation for places like google to give away these "free" services? Are they just "good guys"?)* This makes it hard for providers to block "bad" email addresses. Should there be any restrictions on creating an email address? Is that a practical solution?

Suggested Activities

1) Go research famous or major phishing attacks. Produce a brief paper about the attack with the following sections:
   a) Brief "what happened" summary
   b) Who was/ware the victim(s)
   c) How were they phished? If possible, describe the message they were sent. How were they convinced to click the link, open the attachment, reply with information, etc?
   d) What was the impact of the attack?

2) Visit https://phishingquiz.withgoogle.com/ and complete the quiz.

3) Do an internet search for "password manager". Choose three different applications and compare them. Consider things like cost, if it has a version for your mobile device, whether others recommend it. Choose your favorite and install it. Use it.

4) Go research major ransomware attacks. Produce a breif paper about the attack with the following sections:
   a) Brief "what happened" summary
   b) Who was/ware the victim(s)
   c) How did they get infected with ransomware? What was the delivery method?
   d) What was the impact of the attack? How much did they pay? How long were they down?

Suggested reading:

- https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/
- https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
- https://www.csoonline.com/article/3240364/what-is-a-botnet.html