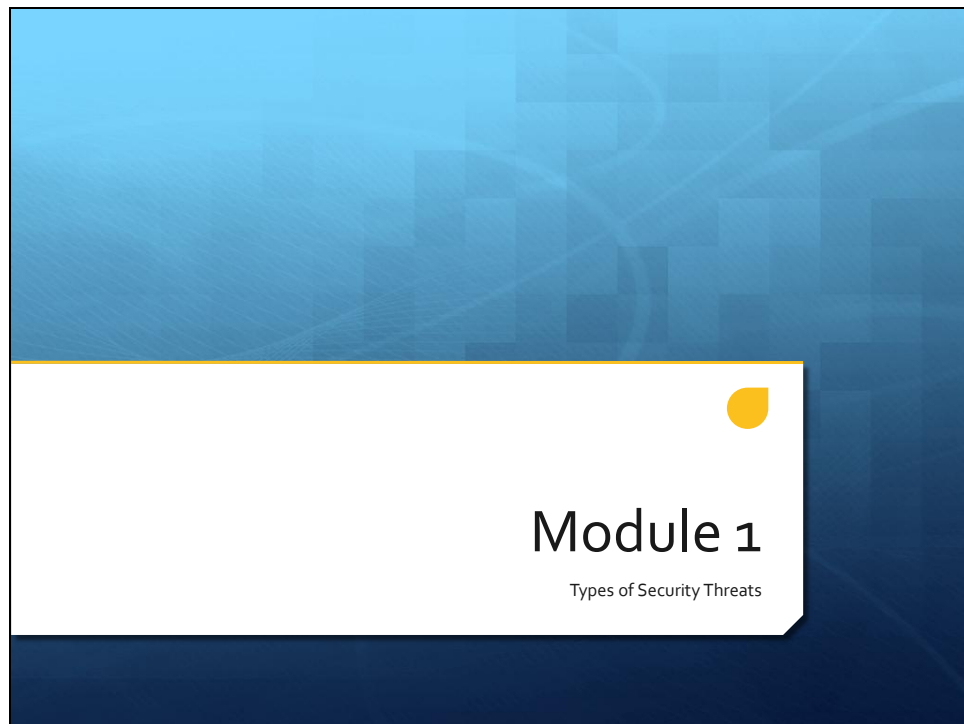


Security Awareness

Module 01 – Types of Security Threats

WORKBOOK

Slide 1



Overview

- + Your Computer
- + Your Internet
- + Yourself
- + Your Words
- + Your E-mail
- + Your Home
- + Your Files

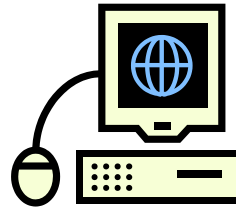
Your Computer

- + There are many attacks that can be done against your computer
 - + Did you lock it?
 - + Did you encrypt it?
 - + Did you scan it?
 - + Did you leave the keys with it?
 - + Did you copy the key?



Your Internet

- + Known bad sites
- + What did you just download?
- + Web site attacks
 - + 0-click attacks
 - + 1-click attacks
 - + 0-day attacks
- + Fake websites
- + Mis-spelled URLs
- + DNS Spoofing
- + Online Profile



Yourself

- + Credit Cards:
 - + At the store register
 - + At the bank
 - + At the restaurant
- + Beware the innocent person on the phone
- + Is online shopping safer?



Your Words

- + Lunch time conversations
- + Phone solicitation
- + Email requests
- + Talking to colleagues



Your E-mail

- + Phishing
- + Signing up for fake sites
 - + Did you just download that?
 - + Where did you just surf?
- + Pharming



Your Home

- + Wi-Fi
- + Visitors
 - + Wanted or not
- + Your systems backup
- + Your decryption



Your Files

- + Backups
 - + Types of storage
- + Encryption
 - + EFS, RSA
 - + Theft of Drive
 - + RMS





QUESTIONS **and** **ANSWERS**

Review Questions:

1. Will putting a cable lock on your laptop protect your data should you leave it unattended?
 - A. Yes
 - B. No
2. What is needed to decrypt your encrypted hard drive or encrypted files?
 - A. RSA
 - B. Decryption key
 - C. Token card
 - D. Username
3. True or False: Most security systems keep a list of websites known for having malware or malicious activities.
 - A. True
 - B. False
4. When you visit a website, as soon as that page is loading, a file is downloaded to your system. You were a victim of what?
 - A. Drive-by download
 - B. 1-click attack
 - C. 0-day attack
 - D. Cross-site scripting
5. True or False: If you accidentally mistype the URL of your website, you could be taken to a fake version of the actual website that you originally intended to surf to.
 - A. True
 - B. False
6. You can be at risk of having your credit card stolen while using it where?
 - A. Restaurant
 - B. Store
 - C. Bank
 - D. All of the above

7. What is the term used for an e-mail being received with the intent of making you believe it is legitimate, yet is designed to convince you to going to a fake website, such as your online banking?
- A. Pharming
 - B. DNS poisoning
 - C. Phishing
 - D. Eavesdropping
8. True or False: You should always use a different password for different applications or websites that require you to register before their use.
- A. True
 - B. False
9. True or False: Your data is safe while you are using your home network.
- A. True
 - B. False
10. How can you protect your data while it's on storage or being transmitted?
(Choose all that apply)
- A. Never give out your password
 - B. Keep your data under a different username/password login
 - C. Encrypt your data while stored on drives
 - D. Encrypt your data while being transmitted

Answer Key:

1. B
Your data is not on the screen or system board, but instead it's on your hard drive. A cable lock will protect your laptop screen and system board from theft, but it does nothing to protect your data.
2. B
Almost all digital encryption is done with a symmetric encryption solution. This type of encryption uses a single key for encryption and decryption.
3. A
True. There is a growing list of known dangerous URLs.
4. A
This is typically a 0-click attack, also known as a drive-by download.
5. A
True. Many hackers will register a domain that is close in the spelling of a legitimate website with the intention of tricking you into providing your username/password to this hacker.
6. D
Your card is at risk anytime you take it out for public use/display.
7. C
Phishing attacks are usually an e-mail that purports to be a legitimate correspondence, but in reality is using fake links to navigate you to the hacker's replica website.
8. A
True. At the very least you should have a different password for all such locations, preferably a different username as well.
9. B
False. Your data is never truly safe, and even at home hackers will attempt to access your data remotely or physically by breaking into the home.

10.C, D

Data should be secured while in motion or at rest.