Final Assessment

PHISHING – Module 1

Ninety-two percent of malicious software is delivered by

1. external devices.
2. an unsecure wi-fi hotspot.
3. email. **T**
4. hackers cracking your password.

If you receive a credible-looking email from your bank requesting information with a link to their website, you should

1. click on the link and provide the necessary information immediately.
2. report the email to authorities.
3. avoid clicking the link and navigate to the bank’s website independently. **T**
4. reply to the email to verify the sender is legitimate.

It is perfectly safe to click on a link or open an attachment if it was sent by someone you know well.

1. True
2. False **T**

What is the purpose of malware?

1. To gain control of your system
2. To collect your personal, sensitive information
3. Marketing
4. All of the above **T**

A good way to avoid falling victim to a phishing scam is to only access your email from your iPhone.

1. True
2. False **T**

PASSWORD STRENGTH – Module 2

One thing that is NOT important when it comes to passwords is

1. encryption.
2. ease. **T**
3. length.
4. entropy.

Of the passwords below, which is the best example of a strong password:

1. H%c!az>.+40rst~=LNE **T**
2. ILoveMyCatSooooooMuch
3. R3m3mb3rM3!!!!
4. 8675309jennysnumber

The best way to remember your passwords is to

1. write them down on paper and keep them near your computer.
2. use software specifically designed to store and protect your passwords. **T**
3. keep them in a file on your computer’s desktop.
4. use the same passwords for all your accounts so they’re easy to memorize.

Of the options below, the best way to create a strong password is to

1. use an online password generator. **T**
2. make it the same as your email address.
3. use a combination of your loved ones’ names and birthdays.
4. repeat the same 4 characters 10 times to make it really long.

You are the only one responsible for protecting your password.

1. True
2. False **T**

PATCHES AND ANTIVIRUS – Module 3

You should install software updates as soon as they’re available.

1. True **T**
2. False

If you always install your patches, then you don’t need antivirus software.

1. True
2. False **T**

Which of the following is NOT a type of antivirus scan?

1. quick
2. on-access
3. full system
4. emergency **T**

What are the two main methods used by antivirus software to detect malware?

1. Heuristics and virus definition **T**
2. Virus definition and virus signature
3. Both a and b
4. Parsing and sweeping

If your patches are up to date and you have good antivirus software, then

1. you can download anything safely.
2. there is no malware on your machine.
3. you are more protected but still vulnerable. **T**
4. you shouldn’t have to install any more updates.

PUBLIC WI-FI SECURITY – Module 4

What should you do before logging on to a public wi-fi network?

1. Verify the name of the network with an employee. **T**
2. Hide your screen from people nearby.
3. Disable your firewall.
4. Do a full-system scan.

What is a VPN?

1. A Virtual Protected Network
2. A Verified Private Number
3. A Verified Protected Number
4. A Virtual Private Network **T**

HTTP is safer than HTTPS.

1. True
2. False **T**

Which of the following is NOT a public wi-fi safety tip?

1. Turn off sharing in your Network Settings in your Control Panel. You can save these settings for public networks.
2. Turn off wi-fi when you’re not using it and disable the “connect automatically” feature so you can control when you’re on a public network.
3. Cover your screen so nearby hackers can’t see what you’re doing. **T**
4. Always log out of your accounts when you’re done using them.

If the public wi-fi network you’re using is password protected, then it is secure.

1. True
2. False **T**