Basic Security I – How to Protect

You are the Target – Q1

Q: What do individuals like you represent to cyber criminals?

Choices:

1. Online Friendship
2. Money
3. Marketing Lead
4. Social Networking

Ans: 2

You are the Target – Q2

Q: What is a common way cyber criminals use your computer to their benefit?

Choices:

1. To send spam emails
2. To track usage
3. To create Excel documents
4. To access illegal webpages

Ans: 1

You are the Target – Q3

Q: Cyber criminals target important information on your computer including credit card numbers, identification numbers and confidential work information. What is another type of information on your computer often targeted by cyber criminals?

Choices:

1. Websites you visit
2. Your IP address
3. Banking Information
4. The software you use

Ans: 3

Email and Messaging – Q1

Q: You receive an instant message from a person called Claudio Kabila informing you that he needs your help to retrieve money that is currently kept in a trust deposit vault in Dubai. He will give you $10,000 to help him. What should you do?

Choices:

1. Offer to help in any way you possibly can; $10,000 is too much money to pass up.
2. Reply to Mr. Kabila via IM and ask him for more information before proceeding.
3. Ignore the scam. You know if it sounds too good to be true, it usually is.
4. Google the name Claudio Kabila to ensure he is not affiliated with a scam.

Ans: 3

Email and Messaging – Q2

Q: What is spear phishing?

Choices:

1. A certain type of encryption algorithm that is used by senior management for high value targets.
2. A customized attack that targets only a few, high value targets, such as senior management or specific employees.
3. An email verification system that targets phishing attack messages and is used by senior management.
4. A technical attack that exploits vulnerabilities in webservers.

Ans: 2

Email and Messaging – Q3

Q: What is the best practice to follow when you receive emails with attachments?

Choices:

1. Only open the attachment if it is from someone you know and were expecting the email.
2. Open the attachment only if it is from someone you know.
3. You can open any attachment you want because all attachments are safe.
4. You can open any .pdf documents, because Adobe .pdf documents are safe.

Ans: 1

Browsers – Q1

Q: From a security perspective, why is it important to install the most current updates to your internet browsers?

Choices:

1. It ensures that you are able to enjoy the most current videos and games available.
2. It makes your computer faster and more efficient.
3. It protects your browser from known weaknesses.
4. It makes internet surfing more enjoyable.

Ans: 3

Browsers – Q2

Q: What should you do when your browser shows you a warning banner saying the website you are about to visit could be harmful?

Choices:

1. Disregard the warning banner and proceed to the website.
2. Do not go to the website.
3. Call the police and explain the situation.
4. Update your computer.

Ans: 2

Browsers – Q3

Q: Which of the following is a preventative action you can take to protect yourself from cyber criminals with techniques for attacking browsers?

Choices:

1. Configuring your browser for auto-updating
2. Installing the most popular plugins for your browser
3. Reformatting your hard drive
4. Reinstalling your operating system

Ans: 1

Mobile Devices – Q1

Q: From a security standpoint, why is it important to only download applications from trusted sources?

Choices:

1. Criminals can create applications that appear to be real, but are actually malicious programs.
2. Applications from un-trusted sources will not put your mobile devices at risk.
3. If you download applications from un-trusted sources, you will not be able to send or receive emails with your smartphone.
4. All of your SMS messages will be sent to your contacts if you download applications from un-trusted sources.

Ans: 1

Mobile Devices – Q2

Q: From a security standpoint, why is it important to keep mobile device operating systems and applications up-to-date with the latest versions?

Choices:

1. Cyber attackers can easily exploit your mobile devices if you are running outdated operating systems or applications.
2. It is not important to keep mobile device applications updated; they update automatically.
3. Mobile devices with outdated applications are immune to security attacks; only operating software updates are needed.
4. Your contact list cannot be stolen regardless of your operating system and application software versions if you use a password to protect your phone.

Ans: 1

Mobile Devices – Q3

Q: How can you increase security of the information on your mobile device in the event that it is lost or stolen?

Choices:

1. Protect your mobile devices with a hard-to-guess PIN and use encryption.
2. Keep your mobile device's battery charged at all times.
3. Uninstall your Bluetooth application at the end of each work day.
4. Protect your mobile devices by installing anti-virus software.

Ans: 1

Basic Security 1 – How to Protect

Passwords – Q1

Q: Which authentication method is the most secure and the option you should use whenever possible?

Choices:

1. A long passphrase that is hard to guess.
2. Two-factor authentication (commonly called two-step verification).
3. A short password that is easy to remember.

Ans: 2

Passwords – Q2

Q: What is a passphrase?

Choices:

1. A type of two-factor authentication.
2. An advanced encryption algorithm.
3. A strong password that is made up of multiple words.

Ans: 3

Passwords – Q3

Q: When is it okay to share your password at work?

Choices:

1. It is never okay to share your password.
2. When your supervisor requests your password.
3. When someone calls you and says they are from the help desk.

Ans: 1