Cybersecurity: Protecting Yourself in the Digital Age

LC Design

Course Outline

Gamification: The learner receives promotions and gifts as they become more knowledgeable about the different types of cybersecurity breaches.

Levels of Promotions w/ Gifts: IT Intern (to start)

(1) IT Technician - coffee mug
(2) IT Manager - box of chocolates
(3) IT Specialist - flowers
(4) IT Expert - certificate of achievement

Scenario: Security Breach!

You are a newly hired IT professional at a technology start-up - Silicon Dreams. In your first week of work, you receive an urgent call from your boss - the company's computer systems have been compromised by a massive cyber attack! As the IT manager, it's up to you to share your knowledge about cybersecurity and save the Silicon Dreams' sensitive data from future damage or theft.

Let's see if we can identify and fix the source of the data breach...

Scene 1: "The Phishing Attack"

Trevor received a convincing email from his bank asking him to update his credit card number. What did Trevor do?

Animation: Email appears in inbox

Sound Effects: mail received, mail opening

Scenario Branches: (learner choice)

1 - Clicked on the link to see if the website is legitimate

This LIKELY was the source of the breach. Clicking on a suspicious link exposes the company to data and identity theft.

2 - Forwarded the email to Maria to ask her opinion

This MIGHT HAVE BEEN the source of the breach. By forwarding the suspicious email, his friend may have unknowingly clicked the link - exposing Silicon Dreams' data.

3 - Reported the email to his bank's fraud department

Trevor made the right decision; this was probably not the source of the cybersecurity attack.

This was an example of PHISHING. Phishing is an attempt to scam individuals to reveal their personal information, such as passwords or credit card details. Typically, this is done by posing as a legitimate organization, such as a bank or an online retailer, and sending emails or messages that look like they come from the real organization. The messages often contain a link to a fake website that looks like the real one, where the user is prompted to enter their personal information.

Scene 2: "The Malware Download"

Maria was browsing the internet when a pop-up appeared, offering her a free download of a cool new computer game. What did Maria do?

Animation: computer pop up on screen

Sound Effects: pop up, game sounds

Scenario Branches: (learner choice)

1 - Downloaded the game

This LIKELY was the source of the breach. Downloading unsafe software can put an entire computer system at risk.

2 - Downloaded antivirus software first and then downloaded the game

This MIGHT HAVE BEEN the source of the breach. Not all antivirus software is fully protective - be sure to do your research before purchasing.

3 - Reported the pop-up ad and closed the window

Maria made the right decision; this was probably not the source of the cybersecurity attack.

Takeaway: This was an example of MALWARE, meaning “malicious software”. It’s designed to damage, disrupt, or gain unauthorized access to a computer system. Protecting against malware involves implementing a range of security measures, such as using antivirus software, keeping operating systems and software up-to-date, and being cautious when downloading and opening files. It's important to regularly backup your files to protect against data loss in case of a malware attack.

Scene 3: "The Social Engineering Scam"

Sherri received a call on her office phone line. It was someone claiming to be a Microsoft technician asking for remote access to her computer. What did Sherri do?

Animation: Phone call, woman answering

Sound Effects: phone ringing

Scenario Branches: (learner choice)

1 - Grant him full remote access to the system

This LIKELY was the source of the breach. You should only give unrestricted access to a verified, trusted source.

2 - Give him partial access just to your individual computer

This MIGHT HAVE BEEN the source of the breach. Only Sherri’s computer was directly affected, but her computer is part of a larger system.

3 - Refuse to give him access and bring it to the company’s attention

Sherri made the right decision; this was probably not the source of the cybersecurity attack.

Takeaway: This was an example of SOCIAL ENGINEERING. Social engineering is a method of manipulating people into divulging sensitive information or performing actions that go against their best interest by exploiting human emotions and trust. It involves the use of psychological tactics to influence or deceive individuals into giving up confidential information such as passwords, bank account details, and personal identification numbers (PINs).

Scene 4: "The Ransomware Attack"

Daniel's computer screen froze! A message was displayed demanding payment to restore access to his super important files. What did Daniel do?

Animation: Frozen screen with message popping up

Sound Effects: pop up

Scenario Branches: (learner choice)

1 - Paid the money

This LIKELY was the source of the breach. Paying the money does not guarantee the files will be restored. What a waste!

2 - Ignored the message and lost access to his files

This MIGHT HAVE BEEN the source of the breach. Without a backup of the files, there's no guarantee to get them back.

3 - He backed up his files and can ignore the message and restore them from his hard drive

Daniel made the right decision. He protected himself and Silicon Dreams with frequent backing up of his files!

Takeaway: This was an example of RANSOMWARE. Ransomware is a type of attack in which malicious software encrypts a victim's files and locks them out of their computer, demanding a ransom payment in exchange for restoring access. This can lead to significant financial losses, data theft, or disruption of operations.