CYBERSECURITY TRAINING

WELCOME TO CYBERSECURITY TRAINING!

- Cyber security is defending computers, servers, electronic devices, data, and networks from malicious attacks.
- Cyber attacks happen daily and the attacks are always evolving
- With the growing cyber attacks, there is an increase to cybersecurity
- We developed this training guide to help our clients (?) understand the risks of the cyberworld

TRAINING PROGRAM MODULE 1

- The first module will introduce the individual to the cyber world with terminology and types of cyber threats

TYPES OF CYBER THREATS

- Cybercrime – an individual or group that target a system for financial gain or to cause disturbance
- Cyber attack – this often includes a political motive
- Cyberterrorism – attacks systems to cause panic and fear

COMMON METHODS OF CYBERATTACKS

- Malware – the cyber-attacker damages the victim’s computer by spreading malware through an unsolicited email attachment or download
    - Virus – a self replicating program that attaches itself to a file and spreads throughout a computer system with a malicious code
    - Trojan – malware that disguises itself as legitimate software, and when the user downloads it onto their computer, it causes damage or collects sensitive data.
    - Spyware – this malware secretly records what the user does so that cybercriminals can use the information (i.e. passwords to bank accounts)
    - Ransomware – malware that locks a user’s file and data and threatens to delete it unless a lump some of money is paid out. It is not guaranteed that the cybercriminal will not erase the data after being paid.
    - Botnets – cybercriminal will infect the computers connected to networks with malware. Once infected, the computers will do any task the cybercriminal asks it to do without the user’s permission
    - Video: https://www.youtube.com/watch?v=ooJSgsB5fIE&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_&index=3

INTERNET OF THINGS:

- The Internet of Things (IoT) is a network of interconnected physical devices, home appliances, and other devices with sensors, software, and connectivity that enable them to collect, exchange, and act upon data.
- It involves connective everyday devices to the internet or to each other in order to enhance their functionality and efficiency.
- Key Components:
  1. *Devices:* physical objects/"things" with components that collect and transmit data
  2. *Connectivity*: this can include Wi-Fi, Bluetooth, cellular networks
  3. *Data Processing*: the large amounts of data are processed on the devices itself or cloud platforms for analysis and interpretation
  4. *Analytics and Services*: the data collected can be analyzed to detect patterns and make informed decisions.
  5. *Applications and Services:* with the wide range of applications and services, the capabilities of these devices improve efficiency and enhance user experience.

INTERNET OF THINGS EXAMPLES:

- Smart home devices such as smart thermostats, smart locks, and smart speakers
- Wearable devices such as smartwatches, fitness trackers, and health monitoring devices
- Vehicles that are equipped with technological functionalities such as remote diagnostics, GPS tracking, and vehicle communication.
- Healthcare devices such as pill dispensers through telemedicine, remote patient care, and remote patient monitoring systems.
- Retail devices such as inventory tracking systems and marketing and customer engagement beacons.

TRAINING MODULE 2

- This second module will discuss some safety tips to help business and individuals safeguard their network(s) and computers

HOW TO PROTECT YOUR SYSTEMS AND ELECTRONIC DEVICES?

- End-user protection - an individual (the user) could accidentally upload malware to a desktop or mobile device, and it could spread to the network.
- Security protocols must be in place
- Cyber security training programs help professionals identify new threats and ways to combat them. Employees need to be educated and up to date on how to protect their devices and network.
- Our training program offers safety tips and tests to help business and individuals guard themselves against cyber threats and attacks

CYBER SAFETY TIPS

- Updating software and operating system is crucial. The user will benefit from the latest security patches. If the user does not update their software or operating system, then they are exposed to the cybercriminals.
- Using strong passwords – using a series of numbers, letters (capital and lowercase), and symbols will make up a great password. Making sure that passwords are not easily guessable. Using hashed passwords are recommended. Aside from using strong passwords, it is also recommended to change passwords every 90-180 days.
- Do not open email attachments from an unknown sender. If the user is unsure of whether it is a phishing or malicious email, then it is important to report it to their IT department. Opening an attachment from an unknown sender is how the malware is spread

CYBER SAFETY TIPS CONT'D

- Just like not opening attachments in emails from unknown senders, do not click on links in emails from unknown senders. This is also how malware is spread. Report the email to your IT department and they will be able to determine whether the email is legitimate or not.
- Avoid using unsecure Wi-Fi networks in public places because unsecure networks leave users vulnerable to attacks – most common one is the man– in – the – middle attack.
  - The man-in-the-middle attack is when a hacker gets in the middle of the communication of the connected device to eavesdrop
  - Another similar attack is the evil twin attack where a fake Wi-Fi network is set up to steal information from connected devices
  - Video: https://www.youtube.com/watch?v=d30n-YxOHo4&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_&index=13

SECURING INTERNET OF THINGS DEVICES:

- Securing IoT devices is crucial due to their emerging presence in daily life.
- Organizations can enhance the security of their IoT device and mitigate the risks associated. Still, it is always recommended to continuously monitor the devices and adapt the security measures accordingly.
- Key aspects to think about when securing IoT devices:

1. *Encryption:* helps prevent unauthorized access
2. *Authentication*: ensures only authorized users and devices can access the IoT system
3. *Authorization*: clearly defined access control policies to specify what actions certain users and devices are allowed to perform within the IoT system
4. *Patch Management*: regularly updating the devices' firmware and software to patch known vulnerabilities and to enhance security
5. *Physical Securi*ty: security measures such as locks and tamper-evident seals
6. *Monitoring and Tracking*: to detect anomalies or security incidents and facilitate forensic analysis in case of security breach
7. *User Education*: educating users and administrators about IoT security, such as creating strong passwords and recognizing phishing attempts, adds an extra layer of protection

TRAINING MODULE 3

- The third module will consist of a mini exam that will test what the individual has learned throughout the program

PHISHING TEST EXAMPLE

1. An email from your boss asks for the company’s credit card information and tells you it’s urgent that you give them the information. They want you to respond right away or you’re fired.

❑ True

❑ False

2. A company vendor sends you a text message asking you to renew password by clicking the link in the text and it will redirect you to their website to change it. You should:

❑ Reply to the text and confirm whether you really need to change your password

❑ Call the vendor using a phone number that you know is correct for them and asking them to confirm the request

❑ Click the link and if it takes you to the vendor’s website, then you know it’s not a scam

PHISHING TEST EXAMPLE CONT'D

3. Two – step authentication, having email as an authenticator, can help protect users against cyberattacks.

❑ True

❑ False

5. If the user falls for a phishing scam, what should they do to minimize the damage?

❑ Nothing, the damage has been done.

❑ Delete the phishing email

❑ Unplug the computer to get rid of any malware

❑ Change any compromised passwords

❑ Break the computer into pieces

PHISHING ATTACK VIDEO:

- https://www.youtube.com/watch?v=PR0c-gJ20kA&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_&index=43

RANSOMWARE QUIZ EXAMPLE

1. What is Ransomware?

   ❑A form of cryptocurrency

   ❑Software used to protect your computer from harmful devices

   ❑A software that infects the computer networks and mobile devices to hold your data hostage until you send the attackers money

2. If you encounter a ransomware attack, the first thing you should do is pay the ransom

   ❑True

   ❑False

RANSOMWARE QUIZ EXAMPLE CONT'D

3. Setting your software to auto-update is one way you can help protect your business from ransomware.

❑True

❑False

4. What is the possible impact of ransomware?

❑Temporary or permanent loss of sensitive information

❑Financial losses

❑Potential harm to an organization's reputation

❑All of the above

RANSOMWARE VIDEO:

- https://www.youtube.com/watch?v=-KL9APUjj3E

OTHER RESOURCES RECOMMENDED:

- Cybersecurity Trivia – spin the wheel! https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html?category=smartphone
- Counter Intelligence Trivia – spin the wheel! https://securityawareness.usalearning.gov/cdse/multimedia/games/citrivia/index.html
- Cyber security Jeopardy - https://securityawareness.usalearning.gov/cdse/multimedia/games/con-jep-gameone/story.html
- Hidden Objects Security Game - https://securityawareness.usalearning.gov/cdse/multimedia/games/hiddenobject/story.html