Assignment -1

General Cybersecurity Awareness

What is Cybersecurity?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Personal Cybersecurity Tips / Best Practices

Use Strong Passwords

Use a VPN When Necessary

Think Before You Click

Update Your Home Router

Update Your Devices

Use Two-Factor Authentication

Threats and Practices

Malware

Spear Phishing

Malicious Links

Passwords

Browsing in Public

Data Compromise

Threat: Malware

- Software designed to compromise a device/network
- Examples:
  - Worm/virus
  - Botnet
  - Banking Trojan
  - Ransomware

Who is Targeted?

Ransomware

- It is estimated that ransomware damages will cost more than $20 billion globally in 2020
- Encrypts/locks files
- Holds files for ransom
- Typically obtained via:
  - Spam & phishing emails
  - Unpatched security vulnerabilities

Best Practices: Malware

- Learn to identify phishing emails
- Exercise caution with links
- Do not download or click suspicious links or files
- Keep software up-to-date
- Back files up regularly

Threat: Spear Phishing

- **Spear-phishing** is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.
- Common cause of data breaches
- Targeted emails
- Sent to small groups or individuals
- Use social engineering tactics
- **93 percent** of incidents/breaches

Threat: Business Email Compromise

- Solicits wire transfer
- Impersonates executive, vendor, or supplier
- Resembles spear phishing
- Targets financial officers

Best Practices: Spear Phishing

- Check the sender
- Look out for warning signs
- Think before you click or take action
- Never hand over sensitive info

Threat: Malicious Links

- Anchor may hide true destination
- Hacked landing pages
- Copycat domains (exampel.com)
- Shortened links

Threat: Password Security

- Susceptible to:
  - Brute force
  - Hacking
  - Malware
  - Phishing
  - Data breach

Best Practices: Password Security

- Effective passwords are:
  - Long
  - Complex
  - Unique
  - Rotating
- Enable MFA where possible

Yes 9@kj*YbM25nGnl

No p@ssw0rd12

Threat: Browsing in Public

- Unsecured networks
  - "Man in the Middle"
- Visual hacking
- **44%** of stolen devices were left in a public place [3]

Best Practices: Browsing in Public

- Avoid public wireless networks
- Use reputable VPN
- Be mindful of surroundings
- Precautionary apps
  - "Find my phone"
  - "Remote wipe"

Threat: Data Compromise

- May result from:
  - Spear phishing
  - Hacking or malware
  - Simple negligence
- Average cost: **$3.86 MM** [4]

Best Practices: Data Compromise

- Storing sensitive information:
  - **Yes** to encrypted devices
  - **No** to removable media (flash drives)
- Sharing:
  - Who is authorized?
  - Check email CC's
  - Secured network?
- Destruction:

Cybersecurity Basics Checklist

- Keep all your software up-to-date
- Install a reliable antivirus solution
- Enhance your security with a product that can block attacks antivirus can’t detect
- Use strong passwords and change them often
- Activate and use two step verification where available
- Avoid oversharing information on social media
- Back up your data. Do it often. Back up in several places

- Never open emails from unknown senders
- Never download or open attachments sent by unknown senders
- Keep your financial information safe and don’t share it with anyone
- Avoid untrusted websites and don’t click on suspicious banners or links
- Adjust the privacy and security settings in your browser and apps

THANK YOU