KACo Cybersecurity Training

Cybersecurity Threats

- Phishing Attacks
- Malware/Ransomware
- Hacking
- Imposter Scams

KACo Cybersecurity Training

BEWARE OF Phishing

- Phishing attacks steal personal information by tricking you into doing something, like clicking a link or entering your username and password.
- Phishing comes in many forms: emails, phone calls, website downloads. These phishing attempts may look like they are from someone you know—but don't fall for the tricks!

KACo Cybersecurity Training

Tips to Avoid Phishing Scams

- **Be skeptical** of messages that require "immediate action" or threaten that you will lose something.
- Instead of clicking, **type website addresses** in your browser to access sites directly.
- Before clicking, **hover over a link** to display the true URL and see if it is linking to a reputable website.
- **Think before clicking** email and website links and never click a link that you don't trust.
- **Do not open attachments** you aren't expecting—especially ZIP files—and NEVER run .exe files.
- **Avoid providing personal information** over the phone, especially from an unsolicited call.
- **Never send credit card** or other sensitive information via email.
- **Use common sense**. If it looks like spam, then it probably is spam.
- **Look at the full email address** – just because the name looks familiar, doesn't mean it is coming from someone you know.

KACo Cybersecurity Training

Imposter Scams

- Someone "official" calls or emails to report a crisis situation
- They represent the IRS, a bank, the lottery or technical support
- There will be a sense of urgency and a dire penalty or loss if you don't act

Example:

IRS scams – You receive a phone call claiming to be the IRS, reporting you owe money and need to pay or else get hit with a fine.

KACo Cybersecurity Training

Malware/Ransomware

- Type of software with malicious intent and a threat to harm your data
- The author or distributor requires a ransom to undo the damage
- No guarantee the ransom payment will work
- Ransom often needs to be paid in cryptocurrency

Example:

WannaCry was one of the most devastating ransomware attacks in history, affecting several hundred thousand machines and crippling banks, law enforcement agencies, and other infrastructure.

KACo Cybersecurity Training

Avoiding malware/ransomware

- Be wary of invitations to download software from unknown sources; even clicking advertisements can result in malware downloads like ransomware, spyware, and adware.
- Ransomware is a type of malware that prevents or limits users from accessing their system—either by locking the screen or encrypting the user's files—unless a ransom is paid
- Spyware records your actions and keystrokes to steal your passwords, credit card numbers, and other confidential information
- Adware not only slows your computer, but can track the sites you visit

KACo Cybersecurity Training

Hacking

- Unauthorized access to systems and information
- Website attack such as DDOS
- Access denied to authorized users
- Stolen funds or intellectual property

Example:

Newspaper kiosk's point-of-sale system was hacked; malware installed. Every customer's credit card information was sent to criminals.

KACo Cybersecurity Training

Protect passwords

NEVER share your passwords with anyone!

- Create strong passwords that are difficult to guess
  - Avoid dictionary words
  - Do not use common passwords, such as *password1*, *abc123*, *qwerty1*, *letmein*, *yourname1*
- Change your passwords periodically and when creating a password
- Use at least eight characters
- Mix uppercase and lowercase letters, numbers and symbols
- Use different passwords for different sites
- Store passwords in a safe place
- Never keep passwords on a sticky note near your computer

KACo Cybersecurity Training

Prevent identity theft

- Don't give out Social Security numbers, driver license numbers, bank account numbers or other personal information unless you know exactly who's receiving it
- Protect other people's information as you would your own
- Avoid sending personal or confidential information via email, text message, or instant message
- Every year, order a copy of your credit report from each of the three major credit bureaus—Equifax, Experian and Trans Union

KACo Cybersecurity Training

Back Up important Files (Personal)

- Create offline back-up copies of your files to reduce the risk of losing important files to ransomware, a virus, computer crash, theft or disaster
- Save copies of your important documents and files to a flash drive, external hard drive or online back up service
- Test your back up files periodically to make sure the files are accessible and readable

KACo Cybersecurity Training

Everyday Tips

- Be careful of email attachments, web links and voice calls from unknown numbers.
- Do not click on a link or open an attachment that you were not expecting.
- Use separate personal and business computers, mobile devices, and accounts.
- Use multi-factor authentication where offered.
- Do not download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management application to store your passwords for you.