EMAIL SECURITY

Email messages are the number one mechanism for delivery of malicious software and other harmful computer infections. They are also used to trick employees into revealing sensitive or secure information. It is the responsibility of every employee within an organization to be aware of the threat and to follow email security best-practices. One crucial component to email security is to always verify that your computer’s anti-virus software is active and current.

Many email security threats can seem legitimate. Being aware of and following your company’s email security policy is the best way to avoid falling victim to a scam and finding sensitive information compromised.

THE THREATS TO EMAIL SECURITY:

☐ Email attachments can deliver malware and other security threats.
☐ Links within email messages can take you to unsecure and/or malicious websites.
☐ Email messages that as you to provide sensitive or personal information are almost never legitimate. If in doubt, contact the sender using a verified method.
☐ Don’t fall for scams that warn of an imminent threat and ask you to click on a link, update your password, or provide identifying information.
☐ Email messages that appear to come from friends or co-workers asking you to “check this out” or click this link are often bogus and can infect your computer.
☐ Email messages can be intercepted, so use caution when sending sensitive information—especially using public Wi-Fi networks.
☐ Electronic invitations (e-vites), job postings, special offers, even photo attachments can all deliver harmful programs or malware.

PROTECT YOURSELF FROM EMAIL SECURITY THREATS:

☐ Always make sure your computer is running the latest anti-virus and anti-malware software and update it regularly.
☐ Maintain your computer’s software and system updates, including for any applications you are running.
☐ Always question the legitimacy of requests for information, even if they look like they come from a trusted source. Cyber thieves can design websites that look identical to the real ones.
☐ Never click on a link or open an attachment unless you know the sender and are expecting the information.

Key Points

- Email messages can deliver viruses and other malware.
- Up-to-date and active anti-virus software is crucial.
- Adhere to company email security policies.