CYBER SAFETY

Protect Yourself from: Malicious Email

A malicious email can look just like it came from a financial institution, e-commerce site, a government agency or any other service or business.

It often urges you to act quickly, because your account has been compromised, your order cannot be fulfilled or there is another urgent matter to address.

If you are unsure whether an email request is legitimate, try to verify it with these steps:

- Contact the company directly – using information provided on an account statement, on the company's official website or on the back of a credit card.
- Search for the company online – but not with information provided in the email.
- Send it to the Information Security Department to check it out. Forward to Email Security with the subject: *Attention Suspicious Email.*

Be aware of phishing emails, which are attempts to gain access to employee usernames and passwords.

- Don't click on a hyperlink to complete a task you weren't requesting instructions for (hyperlinks are used frequently, however, you should know what is behind the link before clicking anything)
- NEVER PROVIDE YOUR USER NAME OR PASSWORD IN RESPONSE TO AN EMAIL OR ANY REQUEST.

Tips for Avoiding Being a Victim

- Don't reveal personal or financial information in an email, and do not respond to email solicitations for this information. This includes following the links that were sent in the email.
- Before sending or entering sensitive information online, check the security of the website and verify that the URL is correct.
- Pay attention to the website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g, a .com versus a .net)
- If you are unsure whether an email request is legitimate:
  - Try to verify it by contacting the company directly. Contact the company using information provided on an account statement, not information provided in an email.
  - Check out the Anti-Phishing Working Group (APWG) to learn about known phishing attacks and/or report phishing.
  - Send it to the Information Security Department to check it out. Forward to Email Security with the subject: *Attention Suspicious Email.*
- Keep a clean machine. Keep all software on internet-connected devices – including PCs, smartphones and tablets – up to date to reduce risk of infection from malware.

What to Do if You Are a Victim

- Report it to the Information Security Department so that they can be alert for suspicious or unusual activity.
- If you believe that your User ID or accounts may be compromised, contact the Help Desk immediately.

Safety 1st *It's everyone's job!*