Cybersecurity and Plant Operations

Did You Know?

- Cybercriminals use sophisticated malware (i.e., malicious software) to take advantage of system vulnerabilities.
- Cybercriminals are increasingly using ransomware attacks, in which they hack a system and block access to it unless a ransom is paid.
- More employees are working remotely, increasing opportunities for cybercriminals. According to a 2017 study, a cyberattack occurs every 39 sec. The frequency of cyberattacks is expected to increase to every 11 sec in 2021 (www.embroker.com/blog/cyber-attack-statistics).
- Phishing is when an attacker sends emails, supposedly from reputable sources, to dupe individuals into revealing personal information. These attacks are a primary entry method for malware.
- Cyberthreats can enter company systems through emails, links, attachments, and portable storage devices (e.g., flash drives).
- 90% of cybersecurity breaches are caused by human error (www.cybintsolutions.com/employee-education-reduces-risk).

What Can You Do?

- Verify automated requests to update software with your IT department before completing any requests. Only install approved updates, and do so in a timely manner.
- Ensure firewalls and other network security software are up to date and turned on.
- Make sure to regularly back up your systems and data.
- Use strong passwords and change them often. Do not share passwords or accounts.
- Do not save passwords on browsers.
- Do not click on links or attachments in emails sent from an unknown address.
- Never install unapproved software on any company computer. Ensure access keys and other physical security devices are properly secured.
- If you use remote access software, follow company requirements. Be especially vigilant when using public internet sites.
- If something on your computer seems odd or different, ask for help. It could be a hacker trying to gain access.

Cyberattacks are real, and you are a vital part of the defense.