Cyber Safety

Helping and empowering employees to recognize common cyber threats is beneficial to the organization's computer security. Security awareness training teaches us to understand threats to the business. Every employee is responsible and accountable when using a computer on the business network and should be able to recognize security vulnerabilities.

Cyberattacks cost the U.S. Billions every year and pose a threat to individuals and organizations. Small businesses are easy targets due to some vulnerabilities. Learning basic internet usage best practices can prevent cyberattacks. Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through fraudulent solicitation over the phone, in email, text, or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Spotting Phishing emails

If an email goes to your junk email, then it’s probably junk and might be a phishing email. Phishing emails appear as though they’ve been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code or ask for company documentation. Be very cautious about opening links from unknown sources. If something seems suspicious from a known source, don’t just click on it - ask the source directly if it's legitimate.

Emails go to junk email if:

- The sender wasn’t given permission to send the email
- Sender information is inaccurate
- There's no physical address
- Using spam trigger words
- Your subject is weak

Responsibility for Computer Data

The critical nature of data security and the responsibility of each employee to protect company data. We as employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality. Information should be saved routinely to one’s work folder on the server. Do not edit the source documents in their source location. Use the Save As function to save the file you are working on elsewhere. This allows others to use the document and ensure that confidential information will not be saved in the wrong location.

Passwords

Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. You do not want to keep your passwords written down on a sticky note and attached to your monitor.

Notification procedures

In the event, an employee's computer becomes infected by a virus or is operating outside its norm (e.g., Unexplained errors, running slowly when in normally runs well, changes in desktop configurations or browser configuration, Etc.) Employees should recognize a legitimate warning message, alert, or pop-up. In such cases, employees should immediately report the incident so their manager can be engaged to mitigate and investigate the threat.

Document management

Employees should never be in personal possession of company proprietary documents. This includes any member/employee paperwork or certification. If an error occurs, it is the employee’s responsibility to immediately report the incident so their manager can be engaged to mitigate and investigate.

Protecting Computer Resources

- Employees should lock their computers when stepping away or keep their laptops in a secure place to avoid being lost or stolen.
- Employees are responsible for accepting current virus protection software updates on company pcs. If you see the yellow shield with a red circle, right-click it and select Update Policy. To update your computer, search “Update” and you will see the options for Check for updates appear click open and if updates are available Click download. Let all updates complete before restarting. Do not install any updates that have the word preview.
- Unauthorized/Unlicensed software is not allowed to install on company computers. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt company data. If there are any questions about what software is authorized, please reach out to your manager.

Internet Use

Opening online links that are suspicious or from unknown sources is a No-No. Such links can release malicious software, infect computers, and steal company data. We must follow the safe browsing rules and limits on employee Internet usage in the workplace.

How to Spot Suspicious Activity

Spotting suspicious activities can help to enhance your awareness around cybersecurity teaching you to watch out for the following signs:

- The sudden appearance of new apps or programs on their devices
- Strange pop-ups during startup, normal operation, or before shutdown
- The device slows down suddenly with it worked well before
- New extensions or tabs in the browser
- Loss of control of the mouse or keyboard

Employees should report suspicious signs immediately. Even if it turns out to be a false alarm, it might still be beneficial to the employee by clearing up errors in their device that hamper productivity.