Cybersecurity and COVID-19

Corporate Cybersecurity

Your company's Information Technology Department is now more important than ever. With so many employees working remotely from home, your firm is most likely using more data, more bandwidth, and more unsecure Internet connections than ever before. Now is the time to reevaluate your security controls to ensure your company's information is still safe and employees are committed to protecting corporate assets.

Corporate Cybersecurity Tips

- Install a firewall and a company-wide anti-virus program. Keep virus definitions, engines, and software up to date to ensure your firm's security platform remains effective.

- Push out automatic updates to employee computers and other electronic devices. If possible, run updates at night to avoid disruption.

- Always encrypt and password protect Non-Public Information, Personally Identifiable Information, and other sensitive data. Examples include:
  - ◊ Customer name, date of birth, residential address, and social security number.
  - ◊ Bank, credit card, and credit report information.
  - ◊ Health records.
  - ◊ Proprietary or sensitive corporate information, including contracts, operating agreements, board meeting minutes, and other legal documents.

- Establish a Virtual Private Network (VPN). A VPN creates end-to-end encryption for devices that connect to the internet. VPNs help protect company internet connections from unauthorized intrusion.

- Prohibit employees from connecting certain external devices to their work computers via USB by disabling this feature. Examples of prohibited devices include:
  - ◊ Thumb drives, flash drives, or jump drives.
  - ◊ External hard drives.
  - ◊ Cell phones and tablets.

- Remind employees about the importance of good password management and to never leave their workstation unattended without first locking the computer. Tips include:
  - ◊ Regularly change passwords (e.g., every three or six months)
  - ◊ Do not reuse or recycle passwords.
  - ◊ Do not share passwords or "save" them to your computer browser for easier login.
  - ◊ Do not write down passwords and post them on or near your workstation.
  - ◊ Always lock computers before stepping away from your workstation.

MHI
Manufactured Housing Institute

- Regularly back up corporate data, and save it in more than one location. If your company is the victim of a security incident, the only way to reduce the risk of losing vital information is to make sure it is backed up in multiple, independent locations.
- Host WFH implementation events and information exchanges to provide additional guidance as your company transitions to a WFH environment. Continuously provide support to help employees with technical questions.
- Set up an information security training program and require all employees to complete training modules, including annual recertification testing.
    - ◊ Send out scorecards to leadership to promote awareness. Consider sending them every week or every other week.
    - ◊ To motivate employees, make information security a company-wide competition. Consider offering awards or prizes.
- Develop public-facing and employee-facing websites with guidance and answers to frequently asked questions. Make sure this information stays current.
- Identify non-compliant employees and, if a follow-up conversation is necessary, contact them privately.

Email and Emailing

Cybercriminals use deception to trick people into providing their personal information, and early evidence suggests criminals are using fear of COVID-19 to their advantage. While scams can be carried out via any communication platform, email is the preferred medium. The most common tactic is "social engineering," where criminals manipulate victims with threats (e.g., legal action or wage garnishment), tempt them with gifts or rewards, or deceive them by pretending to be someone else (e.g., a friend, client, co-worker, or supervisor). Be suspicious of any unsolicited message requesting your company's non-public information or employee personal or financial information.

Email Security Tips

- Never open an email from an untrusted source.
- Proofread every email before opening attachments or clicking on hyperlinks. Look for these common mistakes:
    - ◊ Spelling errors.
    - ◊ Poor grammar or word choice.
    - ◊ Punctuation errors.
- If an email from a trusted source looks suspicious, reach out to the person via a separate channel (e.g., telephone or text message) to confirm the email is legitimate.

- Use the "hover" method—hover your cursor over any hyperlinks or email links in the email—and if the "mouseover" text does not match the link text, do not click it.
- Report anything suspicious to your Information Technology Department.

MHI
Manufactured Housing Institute

Web Browsing

Data sent over HyperText Transfer Protocol (HTTP) is susceptible to interception, manipulation, and impersonation. This data can include browser identity, website content, search terms, and other information submitted by the user. Unencrypted HTTP connections are a privacy vulnerability, exposing potentially sensitive information about the company and its employees to anyone using unencrypted websites and services.

Web Browsing Security Tips

- Avoid using public Wi-Fi or other public access points. Even if your company provides a VPN, be careful when connecting to the Internet via a public access points.
- Never visit unknown websites or download software from untrusted sources. These sites often host malicious software (also known as "malware") that may compromise your computer.
  - ◊ Use the "hover" method—hover your cursor over any hyperlinks or email links—and if the "mouseover" text does not match the link text, do not click it.
  - ◊ If you need to download files or software, first check with your Information Technology Department.
- When entering private information into a website (such as during a purchase transaction), always check for the "S" in "HTTPS." The "S" stands for "Secure" in Secure HyperText Transfer Protocol. While not perfect, this security protocol provides additional protection.
- Less sophisticated websites may not be optimized for cell phones or tablets. Be careful when visiting websites not optimized for mobile platforms.
- When ending your session, always log out of any open websites, programs, applications, and databases before closing your web browser or other windows.

Helpful Resources

CISA CYBER+INFRASTRUCTURE

Cybersecurity Tips
National Cyber Awareness System

FFIEC

FFIEC Cybersecurity Assessment Tool

To assist with transitioning to a Work From Home environment, MHI has produced this packet of information that contains tips from the Cybersecurity and Infrastructure Security Agency (CISA); and the Federal Financial Institutions Examination Council (FFEIC). MHI encourages you to visit the "Helpful Resources" section of this packet, where you will find links to more detailed guidance and recommendations.

MHI
Manufactured Housing Institute