

Loss Prevention

CYBERSECURITY FOR REMOTE WORKERS

Last April, the FBI's Internet Crime Complaint Center (IC3) reported a large increase in cybercrime since the start of the COVID-19 pandemic. The bureau cited efforts by nation states to get information about COVID-19 research, and additional opportunities for hackers as a result of the fast shift to remote work. Employees working from home or in the field using personal equipment, accessing public Wi-Fi and relying on older security technology are at greater risk for cybercrime, online thefts and scams.

Every industry has different cyber liability exposures based on their operations. In construction, the decentralized nature of the industry requires the use of laptops, iPads and other mobile devices. If not properly secured, they are ripe for data theft and network intrusion. Construction firms store intellectual property and other confidential information that is valuable for criminals.

Small businesses face significant challenges during the pandemic – including just staying afloat. Hackers and other cybercriminals are adept at identifying weaknesses and vulnerabilities. Inadequate or outdated security software and relying on employee-owned equipment and Wi-Fi create opportunities for lawbreakers. Here are several basic suggestions to prevent cyber-attacks:

- 1. Conduct a Cyber Risk Assessment.** For small businesses, it's mostly about identifying your important devices and data, assessing vulnerability and creating a mitigation/control plan. There are many risk assessment tools on the Internet. IT consultants conduct risk assessments as part of their service.
- 2. Develop an Acceptable Use Policy (AUP).** An AUP is a way of communicating your rules concerning employee use of company-provided IT equipment. Employees must know what they can and cannot do with your equipment and how to secure equipment when it is in the field or at their home.
- 3. Train.** Employees may not know what to do when faced with a suspicious email, phone call or text. Phishing scams, spam, malware and business email compromise attacks can cause disruptions, create liability and cost money to

repair if they are not thwarted. Around the clock access to an IT professional (inhouse or vendor) is critical. Training should also include guidelines about using public Wi-Fi networks and advice about home networks.

4. Manage Passwords. Require strong passwords – upper and lower-case letters, numbers and at least one character (comma, percent sign, dash) – and have them changed periodically. Use strong PINs or passcodes on mobile devices.

5. Update Devices. Updates contain changes that fix glitches and enhance the security and performance of software and applications. Hackers and cyber criminals will search for outdated software to exploit.

6. Set-up a Virtual Private Network. A Virtual Private Network (VPN) allows you to set-up a secure connection to another network on the Internet, typically from a home network to a business network with a more secure connection.

A **business email compromise attack** occurs when a hacker gets into a business email system and impersonates someone in authority to defraud the company. A common scheme is when a hacker impersonates a senior manager and emails an employee asking them to transfer funds to a fraudulent account, or send sensitive information to the hacker's account.