Telework Security Practices for Delaware Businesses

BY WALTER DONALDSON CFE, CFCI, CFSSP

AN ORDER BY THE GOVERNOR to "shelter-in-place of residence" took effect on March 24th in Delaware. This closed all "non-essential" businesses in an effort to slow the spread of coronavirus. Under this new order, approximately one million residents, who are not employed by an exempted business, are now only permitted to leave their homes for groceries, to fill a prescription, or go to a doctor's appointment. Many of these individuals are now teleworking from home.

Not everyone is accustomed to working remotely and may not have considered the cyber security implications of doing so. Having the appropriate cyber security mindset could potentially save both an individual and their company from falling victim to a preventable security incident.

General Security Configurations while Teleworking

Ideally, an organization's IT manager has provided you with any specific rules associated with their business prior to teleworking. Absent those specific rules, there are universal security considerations individuals should establish in their home. To start, ensure that the home computer communications network is secure from any intrusion or eavesdropping. An individual can take the following steps to ensure a secure wireless network connection from home:

- Check the internet router to see if it is set up with "WPA2" or "WPA3" security.
- Make sure the router admin password is not the default password; or if so, change the password to something that only you will know.
- Ensure all devices connected to the network have current security updates installed.

Considerations When Using Personal vs. Business Devices

There is an increased security risk when using personal devices as opposed to using business devices with enhanced security features.

Passwords: If an individual is using their own computer or mobile device for teleworking, the employee should make sure they've enabled basic password authentication to access their device. Additionally, if two-factor authentication is available on any of the services or sites that are accessed on the computer, they should also be turned on.

Saving Information: Individuals often download company materials to their personal laptop, desktops, USB drives and cloud hosting services, like BOX or Dropbox. These methods and saving company information directly onto your personal hard drive should not be done without authorization.

Anti-virus Software: Short of installing your business's approved security solutions, like anti-virus software and network security settings, your personal computer is at an increased risk of compromise. An individual should ensure that they have an antivirus solution installed on their computer and that auto updates are turned on to ensure that their computers are up to date with the most recent security software patches.

Virtual Private Network: If an individual's business uses a virtual private network (VPN), they should ask if it can be installed on a personal device.

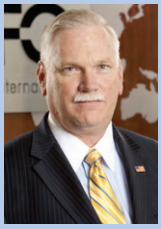
Downloading Software to a Computer: Business devices that have been issued to an employee should already have a standard image on the machine that includes all company approved software, security solutions and configurations. An employee should check with their IT manager prior to downloading any new software to the device. An IT manager should be able to remotely access into your machine to provide assistance, if needed.

Current Cyber Schemes

The FBI's Internet Crime Complaint Center ("iC3") has seen an increase in attacks during this coronavirus pandemic. For example, they have reported instances of fake CDC emails that deliver malware intended to steal information or to lock a person's computer, and then demand payment in order to "unlock" the computer. Phishing emails have also increased regarding charitable contributions; airline refunds; fake cures for the virus, vaccines and fake testing kits.

All of these scams can be avoided by some basic email and internet guidance to protect yourself from falling victim:

- Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email.
- Always verify the web address of legitimate websites, and manually type them into your browser.
- Check for misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in ".com" instead) ■



Walter Donaldson CFE, CFCI, CFSSP is a Managing Director of Freeh Group International Solutions, LLC (FGIS) headquartered in Greenville, Delaware. FGIS provides professional services in the areas of compliance, investigations & due diligence, safety & security and cybersecurity. For further information about how FGIS can assist your organization, please contact the office at +1 302-824-7533, or online at www.freehgroup.com.