From the desk of
Michael Aliperti
MS ISAC Chair

Securing Your Remote Office

October is Cybersecurity Awareness Month and with the increased cybersecurity risks of working from home, we should all be thinking about how to secure our home office.

After months of remote work, you have become a "work from home" pro. However, there may be some areas where you can shore up your home office cyber defenses. You may have realized that the security best practices you once followed are diminishing. Ask yourself - are you communicating with your colleagues and co-workers in a safe and secure way? Do you keep your passwords properly managed? Can you identify (and report) potential incidents or threats on your network? Answering these questions should make you realize that cybersecurity is more important than ever. For remote employees especially, there are many security risks – three in particular – that pose a threat:

Email scams

Many scammers send phishing emails with the intent to steal sensitive information from the recipient or the company. Especially in complicated times – like the novel coronavirus pandemic – phishers are hoping to take advantage of trusting victims. They'll often pretend they are someone within the company, like the CEO or a manager, to establish false trust. Remote workers are easy targets because they are not in the office and, therefore, hackers are hoping they won't check to see if the email is legitimate.

Unsecured Wi-Fi

During this time, many remote employees are using their private home network, which can increase the risk of leaked data. Third parties might be able to intercept and access sensitive emails, passwords and messages.

Personal computers

Many remote workers admit to using their personal devices rather than their designated work tech. According to Cisco, 46% of employees report transferring files between their work and personal computers. If employees obtain sensitive data and store it on their personal devices, that puts many organizations at risk.

Another source of vulnerability is that if you, as a remote employee, are using your personal computer and are not downloading the latest updates, you are more vulnerable to

cyberattacks.

What can you do?

While a list of everything you can do would be exhaustive, here are six suggestions that will go a long way towards securing your remote office. Not all of these can be deployed by everyone, but they are worth noting. We have ranked these (somewhat subjectively) in order of ease of implementation.

1 Use strong passwords.

Physical devices aren't your only concern. If a hacker tries to access any sensitive accounts, you want to make it as difficult as possible for them to log in. Make sure you are not only utilizing unique passwords for each account, but strong passwords as well. Using a password manager is a great precaution, as it ensures you are only using strong passwords; like those with special characters, numbers, upper and lowercase letters, etc.

2 Multi-factor authentication.

Multi-factor authentication (MFA) grants access to the device and all software after the employee provides more than one form of identification. Multi-factor authentication can prevent hackers from accessing your accounts, computer and mobile devices. The availability of MFA is becoming more and more widespread. If it is an option, we strongly recommend you take advantage of it.

3 Invest in antivirus software.

Your employer may provide a recommended application for a company-issued device, but if you use your personal laptop for work, you need to keep your system protected.

4 Follow company policies to the letter.

Your company likely has clear policies for accessing the company network outside the office. Those guidelines and rules should always be followed, but it's especially important when you're working remotely. Report any suspicious behavior to your IT department immediately and follow basic computer hygiene standards:

a. All systems properly patched and up to date. This simply means that the latest updates for your applications have been downloaded, as these are pivotal in securing known vulnerabilities, in which malicious actors could exploit.

b. Malware/Antivirus scans completed on a regular basis.

c. Do not open email attachments willy-nilly. Look at any received email with a cautious eye. It is still the #1 vector for bad actors to wreak havoc.

5 Don't allow family members to use your work devices.

Remember, the computer you do your work on is for employee use only – it's not the family computer. Treat your work-issued laptop, mobile device and sensitive data as if you were sitting in a physical office location. While we understand that this is not always feasible, you should continuously associate your actions with a security-first and data-aware mentality in mind. As an added benefit you will help your family and other users to become more cyber aware and cyber secure. If the option exists to use company-issued equipment, that will always be the first choice. A second choice is a dedicated machine that no one else uses; not for games, nor movies or checking out those tantalizing Facebook posts. Lastly, a shared computer, one that is following all the computer hygiene recommendations above and is being closely monitored.

6 Encrypt your messages.

Data encryption helps protect sensitive information by translating it into a code that only people within your company can access through a secret key or password. Even if scammers intercept your data, they won't be able to interpret it properly. This goes for any messages or information you send, receive, or store on your devices. If this is a feasible option at your organization, make sure to check with your IT department for what types of encryption they may offer or you can take advantage of the many free and paid applications that are available. Encryption requires a bit more technical savvy but is not beyond your capability!

Although October is Cybersecurity Awareness Month, please remember that we should all be cyber aware 365 days out of the year!