TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

April 2020

This monthly publication provided courtesy of Nina Tran, Cyber Security Manager, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Stay Cyber-Secured As You Work From Home

As the world's workforce moved to working from home literally overnight to slow the spread of the COVID-19 virus, here are some important reminders to keep you working securely:

Anti-Virus software and operating systems are updated:

First and foremost, make sure your devices have updated antivirus software installed and running. This includes all home devices and IoT devices. Make sure your AV is set to scan daily on a schedule. Equally important, make sure you restart your devices once a week to apply important OS updates. Check to make sure updates are set to allow important updates to run and install automatically.

Separate work devices from your personal life:

Dedicate your devices to be for work only. Do not allow family members to share your work devices. Do non-work related tasks on your personal devices. Lock your work computer if you step away even for a few minutes.

Make sure your home network is secure:

Set a complicated password for your home router. Use a password generator to created a complicated password that is at least 12 digits. Friendly passwords that are easily memorized can inadvertently shared with others.

Enable 2FA (Two Factor Authentication):

Regardless of how long and secured your password may be, it is still not as secured as 2FA or MFA (Multi Factor Authentication). Almost every application has the option to enable 2FA. The only cost is a minute or two of your time when you login to applications. Many companies are mandating at least 2FA on certain applications. If 2FA is still an option to adopt in your organization, set the example and show your colleagues and management that you care about protecting data.

Use VPN (Virtual Private Network):

To access shared data, your company's VPN is the best option. Your IT department can setup VPN software on your devices if you don't already have it. Once connected on VPN, you will have access to your company mapped drives as if you are at work. Remember to disconnect as you complete your day.

Secured File Transfer:

Request from your IT department for a Secured FTP software if you must send information to vendors or clients. SFTP software provide encryption that regular FTP software does not.

Stay Compliant:

Keep vigilante with compliance rules and regulations as you work from home. Fines are stiff and your company's reputation is at risk.

Beware of COVID-19 themed malicious sites:

An alarming number of hackers and bad actors are exploiting the COVID-19 pandemic for monetary gains. Think twice before you click on the link supposedly from the World Health Organization (WHO), COVID-19 map and news. As everyone scramble to make the changes necessary to work from home, they are forgetting key points that are the norms when they are at work. Many "news" links download malware that compromises your security. Once on your network, they will work laterally to gain access to your company data.

Never connect to open/public WiFi:

Connect to only known secured Wi-Fi. When in a bind, connect to your cell phone's hotspot. As tempting as free Wi-Fi can be, you cannot risk your company's data and reputation.