TechTips Newsletter

tech hero

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

February 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.

Six steps to improve your company's cybersecurity defenses

1. Know what you have

Identify all of your devices (including desktops, laptops, smartphones, TVs and printers) and applications (e.g., email, software, web browsers, websites) so you can take the steps to secure them.

This inventory will serve as a guide and checklist as you make your way through the rest of the toolboxes. Keep this list updated as you add or remove devices and applications. Keep this list updated as you add or remove devices and applications.

2. Update Your Defenses

Boost your digital immunity against threats such as viruses, spyware and more when you keep your systems updated. Allow auto updates to get the latest software updates to the software and applications that you use.

3. Beyond Simple Passwords

Lock your virtual doors and windows. Just like in the physical world, when you lock everything down, the bad guys may move on. Your accounts and data (such as email, personnel records or client databases) are valuable assets – to you and criminals.. Adopt password complexity and MFA to protect your data. Consider password management software that can secure you passwords. Many software have plug-ins to your browsers to allow quick access to passwords.

4. Prevent Phishing and Viruses through Awareness Trainings

Every year many small businesses fall victim to costly malware and phishing attacks, and it can be difficult to survive. These attacks can infect your systems resulting in revenue loss, expensive recovery costs, data loss, damage to reputation and more.

5. Defend Against Ransomware

Phishing is almost as old as the Internet itself and remains one of the most common types of cyberthreats. However, it ready shows an alarming tendency to adapt and evolve, and over 2020, we are likely to see it getting increasingly diverse and sophisticated. As users get more wary of suspicious emails, cybercriminals will more often pose as high-authority organizations, cleverly imitating their normal means of communication. Some people may find themselves targets of focused attacks of this kind by criminals getting access to the information about their contacts and posing as familiar individuals. According to AIG, phishing is likely to remain perhaps the biggest cybersecurity challenge and a major part of the cybercrime landscape, accounting for about a quarter of all claims.

6. Protect your email and reputation

Contrary to a popular image of a hacker as a somebody who looks for flaws in security systems and breaks through them using his or her IT skills, the majority of security breaches have always happened and still happen for other reasons. The weakest link in most security systems is not the software but the people. People neglecting company security policies and making stupid mistakes like using a single weak password for all authentications, both personal and business ones, are much more likely to cause a security breach than a failure to update the software on time. More than half of C-Suite executives (53 percent) and almost a third of small businesses (28 percent) who suffered a breach claim that it was caused by human error. It means that employee training still remains one of the first priorities of any employer looking to improve cybersecurity.