**PROTECTION AND SECURITY**

 Most businesses large and small rely on the internet to track their financials, order and maintain inventory, conduct marketing campaigns, connect with customers, engage in social media, and perform other critical operations. Yet, with startling frequency, we hear about massive computer breaches at even the top companies. Anyone who uses a computer connected to the Internet is susceptible to the threats that computer hackers and online predators pose. So it becomes necessary to be aware of the dangers involved. Here are some ways to prevent the malwares being injected into your devices.

**1.Create strong and unique passcode**

Password prevents unauthorized access to your devices and online accounts. People set unique passwords for their laptops and phones, but they forget to do the same for their routers. Hackers can easily gain access to the devices connected to these routers and use them to flood websites with much traffic. More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes. If you have too many passwords to remember, consider using a password manager like Dashlane, Sticky Password, LastPass or Password Boss.

**2.Use two-factor authentication**

Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Two-factor requires you to type in a numerical code in addition to your password when logging in. Hackers will need two sets of credentials instead of one, with the second code being sent directly to you. This could be an alternate email address, a phone call, or an SMS message to your smartphone. Even if the hacker has managed to steal your password, they won’t be able to get into your accounts unless they have access to whatever device you have your secondary credential sent to. Major online companies like Facebook, Google, Apple and Microsoft let you enable this.

**3.Use anti-virus protection**

Computer viruses, keyloggers and Trojans are everywhere. If you do not have security software, install an antivirus software and keep it up-to-date. It helps to identify the latest threats and allows a user to remove malicious software from his/her device. Viruses have various effects that may be easy to spot: They might slow your computer to a halt or delete key files. Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates. Run or schedule regular virus scans to keep your computer virus-free.

**4.Get anti-spyware software protection**

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove, and tends to serve up unwanted ads or search results to direct you to certain websites. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

**5.Use a firewall**

Firewall is a software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you of any intrusion attempts. The first thing to do with a new computer (or the computer you now use) is to make sure the firewall is enabled before you go online. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices.

**6.Sign up for account alerts**

Many email providers and social media websites allow users to sign up for an email or text alert when your account is accessed from a new device or unusual location. These email or text alerts can quickly notify you when an unauthorized person accesses your account and can help minimize the amount of time an unauthorized user has access to your information. If you receive such an alert, login to your account immediately and change the password.

**7.Shut down laptops and computers when not in use**

Switch off your machine overnight or during long stretches of time when you're not working. Always being on makes your computer a more visible and available target for hackers. Shutting down breaks the connection a hacker may have established with your network and disrupts any possible mischief. If your computer uses Wi-Fi or Bluetooth to connect to the Internet and other devices, you should turn these features off when you aren’t using them. This can prevent unknown persons from using your network or accessing your devices without your knowledge.

**8.Encrypt your hard drive**

Even if someone is able to steal your data or monitor your internet connection, encryption can prevent hackers from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker or FileVault, encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt your web traffic.

**9.Keep your software up-to-date**

Devices’ operating systems and Internet-connected software (like email programs, web browsers, and music players) should be updated regularly. Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. Smartphone manufacturers and app developers regularly release software updates that often include security improvements. Check often to ensure that your smartphone has the most up-to-date software.

**10.Review your network and device names**

Is your cell phone or home network named using your last name or other personally identifying information? This can make your device more vulnerable to attack, since it connects the device to you and makes it easier for hackers to guess your password. You should change the name of your devices and network so hackers cannot identify you so easily.

**11.Be cautious with “ Save my information for next time ”.**

Many websites store personal banking or credit card information to make it easier for you to buy a product or to pay a bill in the future. Although convenient, if your account is hacked, your payment information is more easily available to hackers. Ensure any website where you enter your financial information is secure (the website’s URL should start with “https://” - “s” is for “secure”), that your password is unique to that account, and that you log out once you are done.

**12.Use virtualization**

if you use sketchy websites frequently which are expected to be bombarded with spyware and viruses, the best way to avoid browser-derived intrusions is to clear unsafe sites. Virtualization allows you to run your browser in a virtual environment like Parallels or VMware Fusion.

**13.Beware of spam**

It is best to delete spam or dubious-looking emails without opening them. If you receive a questionable email from a friend or family member, it is best to contact that person and verify he or she sent it before opening the email or clicking on a link or attachment. Beware of email messages from unknown parties, and never click on links or open attachments that accompany them.

**14.Install only secured applications**

Some criminals make available applications (or “apps”) that look and function like legitimate apps, but actually install malware to your smartphone. Be sure to download apps only from trusted sources, and check the number of downloads and read reviews to makes sure you aren’t downloading a “look-alike” app.

**15..Review your login history**

If you feel like there’s some suspicious activity regarding your account, you can check to see how many current sessions you have opened with the application of choice. For example, your Google account lets you see your latest logins, what device they are on, and more. You can even see the geographical location of the login, so if there’s some weird activity going on, change your password and implement two-factor authentication immediately.