Dear Member

Over the next two weeks we will be covering staying safe online (part 1)

With hacks, scams, malware and more, the internet can feel like a dangerous place especially when you throw into the mix smartphones, tablets and WIFI enabled equipment such as doorbells and washing machines...!

As some terms may not be familiar, I have created a link directly to Wikipedia to explain these words in further detail. These words will look like this - HYPERLINK. Hover over the word and Use Ctrl and Click to take you directly to the web page.

Create Complex Passwords

Creating strong, unique passwords for all your critical accounts is the best way to keep your personal and financial information safe.

If you reuse your passwords, a hacker can take the leaked data from one attack and use it to login to your other accounts.

Password Managers are an excellent way to help you store and create strong passwords for all of your accounts.

Boost Your Network Security

Now that your logins are safer, make sure that your connections are secure. When at home or work, you probably use a password-protected router that encrypts your data. But, when you are on the road, you might be tempted to use free, public Wi-Fi. The problem with public Wi-Fi is that it is often unsecured. This means it is relatively easy for a hacker to access your device or information. That's

why you should consider investing in a Virtual Private Network (VPN). A VPN is a piece of software that creates a secure connection over the internet, so you can safely connect from anywhere.

Use a Firewall

Even if your network is secure, you should still use a firewall. This an electronic barrier that blocks unauthorised access to your computers and devices. Using a firewall ensures that all of the devices connected to your network are secured, including devices like smart thermostats, webcams, doorbells and even washing machines. This is important since many devices are not equipped with security measures, giving hackers a vulnerable point of entry to your entire network.

Keep Your Antivirus Program up to Date

Internet security software cannot protect against every threat, but it will detect and remove most malware. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Protect Your Mobile Devices

Our mobile devices can be just as vulnerable to online threats as our laptops. In fact, mobile devices face new risks, such as risky apps and dangerous links sent by text message. Be careful where you click, do not respond to messages from strangers, and only download apps from official app stores after reading other users reviews first. Make sure that your security software is enabled on your mobile, just like your computers and other devices.

Keep up to date

Keep all your software updated so you have the latest security patches. Turn on automatic updates so you do not have to think about it, and make sure that your security software is set to run regular scans.

Lookout for the latest scams

Online threats are evolving all the time, so make sure you know what to look out for. Currently, ransomware is on the rise. This is when a hacker threatens to lock you out of all your files unless you agree to pay a ransom. Stay on top of this and other threats by staying informed.

In Summary, we all love the internet and the vast array of services it provides, but always be cautious about what you do online, which sites you visit, and what you share. Use comprehensive security software, and make sure to back up your data on a regular basis in case something goes wrong. By taking preventative measures, you can save yourself from headaches later.

Next week – Staying Safe Online Part 2….

Nicholas Spike

Assistant Secretary