TECH CORNER

Dear Member

Staying safe online (part 2)

Following last weeks introduction to staying safe online, I have included further guidance below. Now that you have all the security features in place as per last weeks article, follow the below guidance to remain safe.

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.

Click Smart
Now that you have put smart tech measures into place, make sure that you do not invite danger with careless clicking. Many of today's online threats are based on phishing or social engineering as covered in previous tech corner articles. This is when you are tricked into revealing personal or sensitive information for fraudulent purposes. Spam emails, phony "free" offers, click bait, online quizzes and more all use these tactics to entice you to click on dangerous links or give up your personal information.

Share Selectively
There are a lot of opportunities to share our personal information online. Just be cautious about what you share, particularly when it comes to your identity. This can potentially be used to impersonate you or guess your passwords and logins.
Potential employers or customers do not need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You would not hand purely personal information out to strangers individually—do not hand it out to millions of people online.
The Internet does not have a delete key, any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you had not made or get rid of that embarrassing selfie you took at a party.

Practice Safe Browsing & Shopping
Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on.

Always make sure that the site’s address starts with “https”, instead of just “http”, and has a padlock icon in the URL field. This indicates that the website is secure and uses encryption to scramble your data so it cannot be intercepted by others. Also, be on the lookout for websites that have misspellings or bad grammar in their addresses. They could be copycats of legitimate websites.

Be Careful What You Download
A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app, anything from a popular game to something that checks traffic or the weather. Do not download apps that look suspicious or come from a site you don't trust.

Be Careful Who You Meet Online
People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to get familiar with unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

In the next Tech Corner article, we will be covering Two Factor Authentication (2FA)

Nicholas Spike
Assistant Secretary