October is National Cybersecurity Awareness Month

Social Media, Your Credit Score, and You

Let's face it, the internet has become the most important business and personal tool around. From streaming music and video, to socializing on social media channels, to using it for work — the internet has become indispensable to us. But just like any tool, we must understand how to use it properly so as to avoid injury.

The past year has seen an amazing upsurge in social media usage. With quarantine and social distancing being the watch words of the day, this is not surprising. Understand that second to email, social media is a major attack vector for fraudsters. There are a few basic steps you can take to ensure you do not become a social media cyber target.

Social Media Do's and Don'ts

- Be wary of what you post. Do not post personal information. It may help a fraudster steal your identity. Understand that nothing is truly deleted from the internet. Therefore, posts may come back and haunt you.
- Ensure that your computer operating system and software are up to date with the latest security patches and updates. This includes antivirus and antimalware software!
- Read the privacy policies of the social media channels you want to use. Preferably before you sign up. You want to be sure your personal information is safe.
- Links in social media feeds are just as dangerous as those in emails. Social media accounts are some of the most compromised accounts out there. You may be interested in a link your friend posted — was it really them or a fraudster?
- Be wary of whom you friend. Only connect with those individuals you know. A common fraudster tactic is to impersonate a co-worker or a business associate. They use this method to gain your confidence and then will focus their attentions on getting you to provide them with actionable information. Confirm all requests through communications channels to which you are familiar. Do not use contact information they provide.
- Observe proper password protocols — ensure that your password is long and complex. Use a passphrase to make it easier to remember. Ensure that all passwords are unique and never reused. Use a password manager as an aid in remembering passwords and enforcing complexity and uniqueness rules.
- Check the security setting of your social media site and invoke the power of multi-factor authentication (MFA). Setup your security questions, and when possible, enable secondary authentication such as cell phone or email confirmations. This secures your account from fraudsters who may have access to your user id and password.

Secure Your Credit Score

I think we would all agree that your credit score is important part of your financial life. For most people, your credit score is pulled infrequently. Why, then do we have it available 24/7, 365 days? This makes it easy for fraudsters who have the proper information to open lines of credit in your name! Why not lock or freeze it? The three major credit bureaus have provided means for you to do just that:

- Experian
- Equifax

- Trans Union

Business are familiar with this process so when you are in a credit pull situation, such as buying a car or house, ask the business when they plan on pulling your credit and which agencies they use. You can then unlock and relock your credit as needed. Locking your credit prevents fraudsters from opening lines of credit in your name. Ensure that your family members also lock their credit. Use this rule of thumb, if you can pull a free credit score on a family members social security number, you should lock the credit score.

The guidance, tips and best practices presented here are not secret. Share them with your family and friends. Cybersecurity is everyone's responsibility. Educate those in your household and you too can feel confident and safe when you and your family are online.

#BeCyberSmart this #CybersecurityAwarenessMonth