FOCUS FINANCIAL®

Enjoy these simple ways to protect yourself, your family and your business. We encourage you to share them with friends and family and post them on your social media. Safety is a great thing to share.

Passwords & Login Credentials

- Avoid reusing the same password for multiple applications. Use passwords that are 15 characters or more. Length directly correlates to difficulty of cracking the codes. Also, consider Pass Phrases that are inherently longer, and easier to remember.
- Use a Password Manager (via an app or online application) to store your passwords. Ideally, select one that randomly creates your passwords for you. The app will encrypt and store your passwords and allow you to login to accounts and systems directly from the Password Manager. Use a Pass Phrase to secure your Password Manager.
- Add multi-factor authentication to your logins. These are security settings that send a code to your phone or email requiring a secondary login.

Email

- When you receive email from unknown sources, avoid opening attachments or clicking links. Delete the item from inbox, then permanently delete it from your trash folder.
- Unsubscribing often requires you to click on a link or type in your email address. Instead of unsubscribing, mark unwanted emails as spam or junk mail and then permanently delete your spam or junk mail weekly or monthly.
- Avoid sending sensitive information via email. Rely on secure portals to upload information.

Cyber Hygiene

1. Avoid using public Wi-Fi networks in hotels, airports or coffee shops. If you have to use public Wi-Fi, purchase a VPN (Virtual Private Network) which masks your location and automatically encrypts communication.
2. Avoid USB drives. They can be infected with malicious software.
3. Avoid using unknown devices such as computers in hotel business centers.
4. Keep your software programs and virus protection systems current and patched. Patched refers to the update alerts that are generated by various software programs.
5. Be alert, trust your instincts. As a rule, do not click on links in email until you have identified it is a valid source. If you receive a phone call or email asking for your information, do not provide any information.