Fraud and Scam Series
#1- Protect yourself online

Dos and Don’ts to Protect Yourself Online

Do monitor your account. Use mobile apps and alerts to get notified and to stop unauthorized transaction right away. The faster you can identify and act, the easier it is to correct.

Don’t save your debit or credit card number on browsers and websites. These websites have vulnerabilities, and breaches are daily occurrences these days. It is best when shopping online to always use a credit or prepaid card and to enter the card number, expiration date, and CVC code each time. Also, always make sure the site is secured prior to entering your card or personal information. Ensure that the website’s URL starts with ‘https://’. Being careful to acknowledge the ‘s’ as that indicates the site or connection is secured or encrypted.

Do check your credit reports regularly. Sign up for sites like Credit Karma to monitor your report for fraud and errors on a regular basis. At the very least be sure to check all three reports annually and for free at annualcreditreport.com.

Don’t share those *copy and paste questionnaires* on social media. These help scammers identify answers to your security questions like mother’s maiden name, make of your first car, or where you were married.

Do sign up for debit card controls on the mobile app. Having the ability to turn on and off your card in case you misplace it, or it is stolen may help alleviate numerous unauthorized transactions.

Don’t open emails or click links from people or businesses you don’t know. These can be scams or put viruses on your computer which can track and steal your personal information.

Do use two-factor authentication and change your passwords regularly. Use password generators to make sure you get strong options that cannot be hacked easily.

Don’t use public or unprotected wi-fi. You don’t know who else is connected and what information they are able to take from you. Always use a secured wi-fi or your private network.

Do sign up for eStatements to limit sensitive information being sent through the mail. Save other sensitive documents to secured clouds such as our Virtual Strong Box (available on your online banking)

Don’t send sensitive documents or information through an unsecured email. Always encrypt the message or attachment or use a trusted file sharing website or platform.

Do keep computers and phones up to date with the latest software. Updates include patches which are known vulnerabilities to keep fraudsters at bay.

Don’t forget to log out and clear your cookies and cache. If it is a shared computer be sure to never choose the ‘remember me’ option. It is also good habit to clear browsing history, cache and cookies every so often.