Tips for protecting yourself online

There are a variety of scams and types of cybercrime that exist, such as; Identity Theft, Health and Medical Scams and Phishing Scams among others. There are several ways that you can help protect yourself from scammers and cybercrime. For more information on the types of scams and prevention, visit our list of resources.

- Keep your devices and software up-to date with the latest security upgrades.
- Use Antivirus programs.
- Use strong passwords that contain upper-case and lower-case letters, special characters and that are not easily guessed or identifiable.
- Never share your passwords.
- Never provide the answer to a security question in a text or email.
- Use 2 step verification if available.
- Ensure you are using a Secure Network Connection.
- Avoid using public Wifi connections and telehealth services.
- Never click on a link in an email from an unknown source or that you were not expecting.
- Hover over links to verify the source, confirm that is accurate.
- Look for red flags; email is not addressed to you directly, uses a generic greeting (ex. Dear Customer), spelling errors throughout the email, asking you to click on a link to confirm information, receiving offers that are “to good to be true”.
- Do not log into an account by clicking on a link. Visit the secure website login page or mobile app.
- Set up Auto-Deposit for receiving funds. Encourage your recipients to set up Auto-Deposit as well.
- Set up Security alerts.
- Limit the amount of personal and identifiable information your share online.
- If something seems suspicious do not proceed! It is better to err on the side of caution.