SECURE YOUR DEVICES

Viruses are harmful and give criminals access to your computer or mobile device.
Install anti-virus software and regularly update its virus definitions.

Outdated software have weaknesses that can be misused. It is important to keep your computer updated with the latest software.

Old browsers might not be equipped to protect your devices from the latest security threats. Update your browsers to make it harder for viruses to infect them.

Your devices are most vulnerable when they are not password protected. Set strong passwords and security PINs for your PCs, tablets, and mobile phones.

Wireless networks have weak security settings to help users connect to them easily.
Review and enhance your wireless network security settings.

SECURE YOUR INFORMATION

Phishing scams use false emails and websites to get login information. If you receive an email that includes a link to a website, ensure that the website is legitimate before visiting the site.

Never respond to unsolicited calls or emails from people you don't know asking for your personal (including banking) information.

Hackers can easily crack a weak password. Create smart and strong passwords by incorporating capital letters, numbers, and special characters.

Your social network profile can be a security as well as privacy risk. Restrict your profile to friends and family, and be careful about sharing personal information over social networks.

Email accounts can be compromised to reveal sensitive information. Ensure your email accounts are protected by strong passwords and changes regularly.

Always ensure your online banking, social networking and email account passwords are different and unique.

Criminals can also use paper documents to steal personal information. Make sure that yours are secure or switch to e-Statements.