

Use VPN

A VPN protects its user by encrypting their data and masking their IP address leaving their browsing history and location untraceable.

Utilise social media and social networking sites' privacy settings

The privacy settings control what people (including hackers and scammers) can see. The more information that you share, the greater the risk of being the target of scams, hacking or impersonation.

Select 'Report' if you observe something improper.

Report problematic content using the reporting tools provided by the website or social media platform, and ask a trusted person for guidance.

Use strong password

Create a password with a combination of letters, and numbers and use it on safe sites only.

Always double check for the safety of website

The internet is a resource, but it's not always benign. Understanding the potential risks of visiting unsafe websites crucial for protecting your sensitive information online.

Basic Digital Safety

Use caution when downloading apps on your computer or smartphone

Apps might contain malware that could infect your device. Only download apps from trusted official app stores (e.g. Google Play, Apple App Store). Third-party app stores can have a lot of fake apps that contain malicious code. You should try and avoid downloading APK files for mobile Android devices as these are not always easy to update to help keep the application secure.

Does your location, camera, phone number, files, microphone, etc. need to be accessible to your apps?

If you don't, you might be granting your apps access to information that you don't want to share or that they don't require.

Use Device Security Features

This security device may include the following.
Antivirus for smart meters and devices
Host-based intrusion detection and prevention for smart meters and devices
Firewalls for meters and devices
Encryption for low power device
Physical tamper prevention

