STAYING SAFE ON THE INTERNET

SAFE URL

URL stands for Uniform Resource Locator, a unique address for that particular website. Check if it starts with https. The ‘s’ stands for secure. Use Google Safe Browsing and Site Shot to check if the URL is safe.

TRUSTED NETWORKS

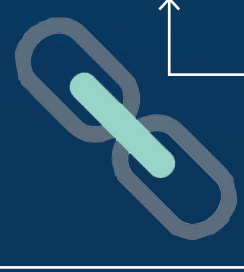
This means a set of interconnected devices that only authorised users can access. Data sent through such networks is usually secured.

ONLINE ADS

Apart from enticing you to buy totally unneccesary items, online ads can also be scams to part you from your money. Other dangers include hacking into your system, stealing your passwords and other sensitive information.

SUSPICIOUS LINKS

A suspicious link looks like a legitimate one but actually isn’t. For example, instead of paypal.com, it might say paypa1.com. Clicking on it can send out information about your system, take you to a fake website, or download malware onto your system.



STRONG PASSWORD

Keep important information safe from hackers and cybercriminals with a combination of uppercase and lowercase letters, numbers and symbols. You should remember it but others should not guess. Don’t choose names or initials or birthdays of family members.

SECURE PAYMENTS

Payment information such as bank details and credit card number are encrypted and you might be asked to authenticate the payment more than once to prevent unauthorised withdrawal or spending of your money.

TRUSTED APPS

Usually apps downloaded from playstores have some vetting, so there is a degree of trust. Don’t install apps that ask for too many permissions. Read up about the app and don’t download one that has too many negative reviews. Keep your phone system updated.