



BASIC

Digital Safety



WHAT IS DIGITAL SAFETY?

Protecting personal data, devices, and online activities from potential dangers like hacking, phishing, scams, and cyberbullying is known as digital safety. It ensures that any technology should be used responsibly and safely, protecting people from online fraud, identity theft, and exploitation.

WHAT MEASURES CAN WE TAKE?

Securing Passwords



- For different accounts use a different password to prevent hacking from multiple accounts if it were to happen.
- Make sure the password contains different letters, numbers and significant characters (for example: !, @ or %).

Being cautious with links and emails



- If you get sent a random suspicious link from a unknown sender, never click on it.
- Always make sure you verify with yourself any emails you receive to avoid any scams or phishing attempts.

MAKE SURE YOU..

Protect your devices



- Avoid using public, free wifi for sensitive transactions and uses of your device, use a VPN instead.
- Make sure you update your anti-virus protector programs so they can run smoothly and be able to track any virus.

Monitor your digital footprint

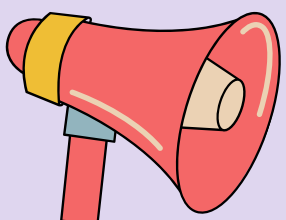
- Delete any old/unused accounts you no longer use to prevent any unwanted access.
- Frequently search your name on the internet to see what information about you comes up.

WHY DOES DIGITAL SAFETY MATTER?

Given how easily digital tools and platforms are welcomed into many aspects of our lives in today's digital world, online security must be given top priority. Ignoring digital safety can result in privacy violations, financial losses, and compromises of sensitive and personal data.



BEING PREPARED FOR A CYBER ATTACK



Having a cyberattack strategy in place is essential for minimising damage, protecting private data, and promoting quick recovery. It helps people and organisations deal with problems in an efficient manner, reduce downtime, and avoid financial and reputational losses.

EMERGENCY PLAN FOR A CYBER ATTACK

- Identify the threat, make sure you understand what the attacker has accessed without your authorisation.
- Freeze any cards/accounts you owe if you have suspected unauthorised access.
- Make sure you change passwords immediately to the affected accounts if you still have access to them.
- Report online to your bank or to the authorities that you are a victim of a cyber attack so they are able to help and assist you on what further steps to take.

