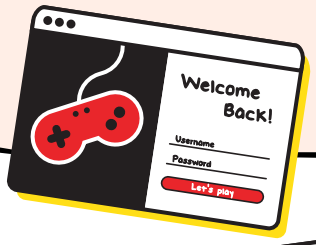
TIPS TO KEEP YOUR CHILD SAFE ONLINE

HOW CAN I SUPPORT MY CHILD TO NAVIGATE THE INTERNET SAFELY

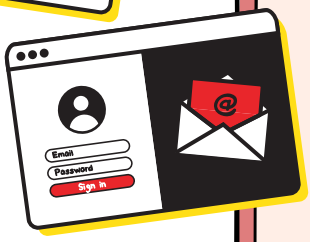
Technology has helped our children learn and develop in the digital space. It is important we support our children in navigating the Internet safely.

WHAT ARE SOME COMMON ONLINE DANGERS?



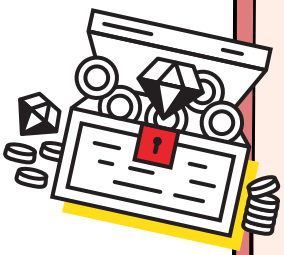
1. OVERSHARING OF PERSONAL INFORMATION ONLINE

- Everything done or posted on the Internet leaves a digital footprint that is permanent. It is impossible to delete information completely once it is posted online.
- Cyber criminals can gather personal information about your child *e.g. through your social media posts, uploaded photos etc to cause them harm, or impersonate them to harm others.*



2. CLICKING ON SUSPICIOUS/UNSOLICITED LINKS

- Similar to actual fishing, cyber criminals lure unsuspecting people with a bait. They disguise themselves as a trustworthy individual or reputable organisation to trick you into providing personal information or giving them access to your devices and accounts. They may even impersonate you to scam others.



3. DOWNLOADING FROM UNOFFICIAL/UNKNOWN SOURCES

- Children are easily tempted by game hacks or promises of free stuff, which could come in the form of messages or advertisements.
- These often contain malware that could compromise their devices.

4. SETTING WEAK PASSWORDS FOR ONLINE ACCOUNTS

- Children often use short simple passwords, and reuse them across their different accounts.
- These can be easily guessed by cyber criminals, who will be able to gain access to multiple accounts owned by your child.

WHAT CAN I DO TO KEEP MY CHILD SAFE ONLINE?

1. HAVE REGULAR CONVERSATIONS AND HELP THEM UNDERSTAND ONLINE RISKS

- Communicate and set ground rules and boundaries for online use with children
  - Encouraging your child to engage in online multi-player games only under parental supervision or with people they are familiar with.
  - Reminding your child not to accept friend requests from strangers.

2. TEACH YOUR CHILDREN TO GUARD THEIR PERSONAL INFORMATION

- Remind your child not to accept friend requests from online strangers.
- Enable privacy settings on social networks.
  - Do not share personal information or pictures of themselves.
  - Disable geotagging on devices.

3. SHOW YOUR CHILDREN HOW TO SECURE THEIR ACCOUNTS

- Create strong passwords of at least 12 characters using a mix of uppercase, lowercase, numbers and symbols. They can try using a passphrase based on a memory unique to them *e.g learnttoRIDEabike@5*
- Do not reuse passwords and use different passwords for each of their accounts
- Enable two-factor authentication (2FA), where applicable

4. TEACH YOUR CHILDREN TO SPOT 6 SIGNS OF PHISHING

- Mismatched or misleading information
- Use of urgent or threatening language
- Promises of attractive rewards
- Requests for confidential information
- Unexpected emails / messages
- Suspicious attachments

5. HELP YOUR CHILDREN PROTECT THEIR DEVICES

- Update software promptly
- Use anti-virus software