



FACT SHEET: Online Safety

1. Protect your personal information


- Don't overshare. Avoid posting your full name, address, phone number, or workplace
- Think before you share. Anything online can be copied or shared
- Check your privacy settings on social media accounts
- Log out of accounts (especially on public or shared computers)
- Avoid accessing sensitive accounts like banking on unsecured public networks



2. Use strong passwords

- Use a different password for each account
- Create strong passwords: at least 8 characters, a mix of letters, numbers, and symbols
- Use a password manager to help you remember
- Enable two-factor authentication

3. Be careful what you click

- Don't click on suspicious links in emails, messages, or pop-ups - even if they look official
- Check if a website starts with https:// (the "s" means it's secure), and look for the padlock 
- If something feels "off" or too good to be true, it probably is
- If you get a strange message from a friend, double-check by calling or texting them directly

4. Avoid viruses and scams

- Install antivirus software and keep it up to date
- Be cautious of:
 - Emails saying you've won a prize
 - Messages asking for your bank details or passwords
 - Calls or texts pretending to be from your bank, Amazon, etc.
- Always install updates on your phone, tablet, or computer



5. Shop safely online

- Only shop on trusted websites
- Use secure payment methods like credit cards or PayPal
- Avoid deals that seem "too good to be true"



If something doesn't seem right online, talk to a trusted friend, family member, or local support organisation.

