Safer Together

A Spotlight on Cyber Security for Queensland Residents

Cyber scams are one of the most common online threats used by cybercriminals to compromise your personal information. This checklist is designed as a practical tool to review your cyber security and identify potential security risks.

When Creating Passwords:

- I ensure each password is unique and unpredictable for each of my online accounts;
- I use a combination of 15 or more upper and lowercase letters, numbers, and symbols;
- I never include my personal information, such as my name, date of birth, or age;
- I ensure my passwords are updated and changed regularly;
- I enable Two-Factor Authentication.

When Using Social Media:

- I understand and can adjust my social media privacy and security settings;
- I limit the personal information which I share to others online;
- I avoid sharing pictures and videos which might identify children;
- I enable Two-Factor Authentication on each of my accounts;
- I avoid clicking on unknown links.

Queensland Police
Queensland Government

Safer Together

When Receiving Emails:

- I avoid sharing any sensitive information such as passwords;
- I never send money or provide bank account details to anyone via email;
- I avoid clicking on links and opening attachments unless I know and trust the sender;
- I always look for spelling mistakes, blurred company logos and inconsistencies in email addresses, domain names and contact details as this may indicate a scam.

When Receiving Text Messages:

- I never share any personal information via text;
- I block and delete unknown or suspicious text messages;
- I avoid clicking on any unsolicited links or attachments;
- I always look for spelling mistakes and inconsistencies in contact details as this may indicate a scam.

Support Services Available:

The Australian Government offers a range of resources and support services to assist you in the event that you have been the victim of a cybercrime.

- Learn more about cyber scams or report a scam at scamwatch.gov.au.
- Review free online learning materials at beconnected.esafety.gov.au.
- Access up-to-date cyber information and news at esafety.gov.au.
- If you have been the victim of a cybercrime, report it to cyber.gov.au.
- If you believe your bank account has been hacked, contact your financial institution without delay.
- In the event your identification, such as your driver licence or online accounts, may have been stolen or hacked, contact IDCARE for specialised support at idcare.org or by calling 1800 595 160.

Scan the QR code using the camera on your mobile to learn more about how you can protect yourself online now.

To learn more about how we can stay safer together, visit **police.qld.gov.au/SaferTogether**

For crime and safety updates, subscribe to your local myPolice News or follow your local myPolice on Facebook at **police.qld.gov.au/stay-connected**

Queensland Government