

Keep safe when using social media websites (i.e. Facebook or Twitter).

Golden rules

- Use unique, strong passwords for different social networking sites
- Don't share your password and make sure you change it on a regular basis
- Using someone else's computer? Use a one-time password
- Log out of social networking sites once you are finished
- Don't accept friend requests from strangers - only befriend people you know
- Be careful about giving out your private details
- Share your personal information only with people and companies that need it
- Only download Apps (applications) from websites you trust
- Don't click on links that appear out of nowhere (i.e. pop ups, advertisements)
- Keep your anti-virus software, browser and other applications up-to-date
- Don't paste script (code) into your web browser's address bar
- Use browser add-ons such as Web of Trust and Firefox's NoScript to keep your account from being hijacked



Scammers often attempt to replicate popular web services and trick you into giving out your personal information via fake websites.

You should only need to log into your social network once each session. If it looks like the network is asking you to log in a second time, ignore this and re-enter the website address into your web browser to confirm that you are logged in.

Scammers can hack your friends' accounts and send links from their accounts. Beware of enticing links or "goofy" posts from anyone. If it looks like something your friend wouldn't post, don't click on it.

Report scams

Email: scam@antispam.govt.nz

TXT: Forward the message to our free shortcode 7726 (SPAM)

Phone: (04) 495 9314

Fax: (04) 495 9314