IT'S HOW WE CONNECT

TOP TIPS
PROTECT YOUR PERSONAL INFORMATION

Whether it's banking, shopping or socialising, everything we do online involves information about us that's important, personal or private. Here are some simple steps to manage your digital life so that your information remains yours.

1. USE A STRONG AND UNIQUE PASSWORD/PASSPHRASE EVERY TIME; AND CHANGE IT REGULARLY

Creating a strong, unique password for every online account is key to improving your online safety. A strong password is long (more than 8 characters) and contains a random mixture of letters, numbers, symbols and capitals. Your password should be different for every site.

Typing out three or four words, what's known as a passphrase, can often feel more natural than a complex combination of letters, numbers and symbols. Add a few capitals and punctuation and you have a strong and easy to remember passphrase. Use it where a site or app permits a longer number of characters.

You could also try a reputable 'password manager', a software tool that can help you create, remember and manage passwords.

2. BE SUSPICIOUS

Trust your instincts.
Be suspicious of anything asking for your response.
If something you encounter is unsolicited, too good to be true, coercive, or targets your personal or financial information, take the time to cross-check it. Verify the information by independently checking with an organisation's website or over the phone.
You can also quickly research scams and hoaxes online. Check the Australian Government's SCAMwatch radar for known scams, scamwatch.gov.au.

3. ENABLE TWO-STEP (ALSO CALLED TWO FACTOR) AUTHENTICATION

A website requiring a password and a second criterion (two steps) to logon significantly increases the security of your account. Enable it wherever it is offered. Two-step (or two-factor) logon means that a different, second step is required to log on or transact. In addition to your username and password, the second step will often involve something such as a secure token or a code sent by SMS (text message) to your mobile.

4. CONSIDER YOUR PRIVACY

Be cautious about the information you reveal online. Don't reveal too much, especially on social media. Restrict who can access your posts in the settings. Check the site's terms and conditions to see if it is secure and will protect your data. Consider using an alias or fake details where your real identity is not required or important. For example, you don't need to use your mother's actual maiden name or your real date of birth.

5. AVOID UNSECURE PUBLIC WI-FI NETWORKS FOR TRANSACTIONS

Unencrypted (typically free) Wi-Fi that you might find in public spaces and cafes is ok for surfing the web, but you don't know who else has access to that network. It is not hard to intercept information over unsecure Wi-Fi so it's best to use a trusted, encrypted network (such as your home broadband network) for shopping, banking, sending personal information or other confidential activities.

6. SECURE YOUR ROUTER

A router is a device that connects your home network to the internet. The most important settings you need to change are both the wireless and the router passwords. Change them from the default to something not easily guessable and something only known to you. For safer home wireless, use the strongest encryption wireless protocol (such as WPA2) that is compatible with your network.

WHAT IS PERSONAL INFORMATION?

Personal information is information that identifies you.

Here are some examples of things you shouldn't share publicly:

- full name
- address
- phone numbers
- usernames and passwords
- date of birth
- email address
- bank details
- usernames if they link to any of the above
- any fact used as a backup question for forgotten passwords (ie: mother's maiden name)