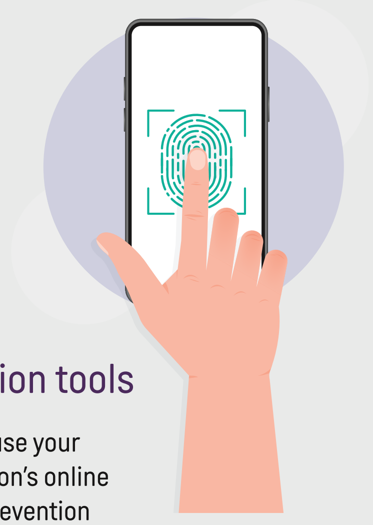
How can consumers reduce fraud risk?

30 YEARS | Australian Payments Network



Authentication tools

Register for and use your financial institution's online payment fraud prevention solutions whenever prompted.

Biometrics are increasingly used for transaction authorisation, both in-store and via remote channels.

In-app payments can improve convenience and security via biometric support (e.g. thumbprint or facial recognition).

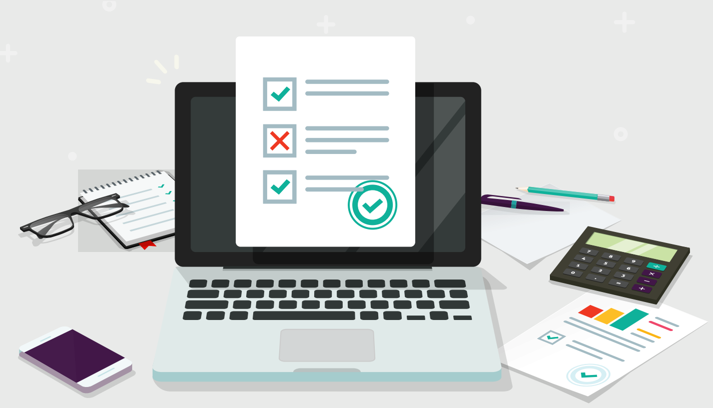
Know who you are dealing with

Take a few minutes to ensure that you are dealing with a legitimate merchant online; do some checks before making a payment on a website for the first time.

Only provide card details on secure and trusted websites – look for a locked padlock icon in the toolbar and 'https' in the website's address.

Be suspicious of offers that look too good to be true – they probably are.

More information on Online Shopping Scams is available at ScamWatch.gov.au.



Be alert to phishing attacks

Be cautious when clicking on hyperlinks and email attachments or texts sent by an unknown contact.

As a general rule, do not provide your personal details to anyone you do not know or trust who makes contact with you, especially if it includes a proposition that involves payment.

Take time to install systems on your devices to protect against viruses and malicious software.

More information is available at ScamWatch.gov.au.

Protect against theft

Report any lost or stolen cards to your financial institution straight away. Similarly, tell your financial institution immediately if/when you change address.

To protect against mail theft, you should:

- Install a lockable mailbox and clear it daily
- During extended periods of absence, have mail held at the post office or collected by a friend
- Contact your financial institution if your new card has not arrived as expected.

Protect against skimming

The vast majority of payment terminals, ATMs and cards in Australia support chip transactions, which give strong protection against skimming fraud.

Always keep your card in sight when making a payment, and do not hand your card to anyone else when making contactless payments. If you spot anything suspicious at an ATM or unattended terminal, do not use the machine and report it to your financial institution.

Contactless payments using a mobile device can provide added protection through biometric authentication and tokenised card credentials.

Protect your PIN & personal details

Consumers should keep their PIN secret, and always cover the PIN pad when entering PINs at point-of-sale terminals and ATMs.

Financial institutions will never ask their customers to divulge their card PIN over the phone, online or in an app.

Keep personal documents secure at home and shred any bills or statements before throwing them away.

Contact: Toby Evans – Head of Economic Crime, AusPayNet | ecf@auspaynet.com.au

www.auspaynet.com.au