Keep your money safe

Your guide to ATM, EFTPOS and online security

Electronic and online banking provides the freedom to manage your money 24/7. It's safe, convenient and inexpensive. However criminals also use electronic banking to defraud people of their money. The main risks occur through scams known as 'skimming' and 'phishing'. This flyer looks at how these scams work and outlines some simple steps you can take to keep your money safe.

Guard your PIN, it's the key to your account

Your Personal Identification Number (PIN) is the key to your account. Never divulge it to anyone. Neither the staff of the Commonwealth Bank, nor any other reputable organisation, or any individual will ever ask you to reveal your PIN in person, by phone or via email.

Protect yourself against skimming

'Skimming' is a means of capturing the data stored on the magnetic stripe of your debit or credit card. A skimming attack occurs when an illegal magnetic stripe reader is placed over the card insert slot of an ATM or EFTPOS machine. Your PIN is then captured by a false keypad or via a tiny camera mounted on the ATM, EFTPOS terminal, or simply by someone standing near you.

Criminals need both your PIN and your card details to access your account. While it's impossible to know when a skimming attack is occurring, some basic precautions can help protect your money.

1. Avoid ATMs that appear to have been tampered with

Watch out for tell-tale signs of ATM tampering. These may include unusual marks, scratches or adhesive tape around the card entry slot or keypad. Play it safe – if an ATM doesn't look right, speak with Commonwealth Bank staff and use an alternative ATM.

2. Shield the keypad when you enter your PIN

Cover your hand when using an ATM or EFTPOS terminal to prevent your PIN being detected.

3. Change your PIN regularly

By changing your PIN regularly, you can reduce the risk of unauthorised transactions resulting from card skimming.

4. Check your account balance and transactions regularly

The only way to know if your account has been skimmed is by reviewing your bank balance and credit card statements for unfamiliar entries. Make a habit of checking your account balance regularly. You can do this easily at any time via **netbank.com.au**

Keep your money safe

TIP – You can decrease your daily ATM withdrawal limit within NetBank as a way of reducing risk. Then increase the limit for those times you may need extra cash.

'Phishing' – don't take the bait

Phishing is a scam where criminals, who might masquerade as individuals, organisations or companies, contact you by email, SMS or over the phone, asking for personal or financial details. Phishing emails can look very authentic, even featuring the logo of the Commonwealth Bank or another organisation. However the tell-tale sign is that they contain a link – clicking on this link will take you to another website which asks for details of your accounts including your PIN.

If you receive a phishing email do not click on any hyperlinks and forward it to **hoax@cba.com.au** immediately. If you receive a phone call asking for your PIN, hang up straight away.

TIP – NetBank offers a very secure environment. You can trust the links within NetBank to other pages within the Commonwealth Bank website.

We've got you covered

Our 100% Security Guarantee means we'll cover any loss should someone make an unauthorised transaction on your account using NetBank – provided you haven't given out your client number or password and you immediately notify us of the loss, theft or misuse of your password and of any suspicious activity on your account.

We're here to help

Please contact us at any time if you have concerns about the security of your money. If you discover unexplained entries on your statements, or you are concerned you may have become a victim of phishing, immediately contact your nearest branch or call us on **13 2221**.

For more security information please visit **commbank.com.au/security**

By working together, we can keep electronic banking safe.