**How to protect your bank cards from fraud**

The risk of a fraudster accessing your bank account through the card you use at the ATM or a shop terminal is very real. In fact, [card fraud](http://www.apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2014.pdf) accounts for more than $624billion a year, or 48c in every $1,000 Australians spend on their bank cards[1](javascript:;).

But there are a few simple steps anyone can take to minimise the risk of people accessing our accounts via our cards. Here they are.

**1. Check the machine**

One of the most common ways a scammer will try to get access to your bank account is at the ATM. This is usually done by installing a ‘skimmer’ over the card reader, which captures the data on your card when you place it into the machine. The scammers then use that data to create a dummy card, which can also be used to access your account.

Skimmers can be extremely difficult to detect. Most are specifically built to blend in with ATMs so you often need to be actively looking for them to notice something is wrong. And, because you’ll still receive access to your funds even if your card passes through a skimmer, there are few advance warning signs that your account will be compromised.  
  
So before you place your card into the card reader, always check an ATM for:

* any signs of tampering, including scratches and marks
* anything that looks out of place, for instance different coloured plastic around the card slot
* anything that moves when it’s pushed (ATMs are built well and don’t usually have loose parts).

If you notice anything suspicious, report it to the financial institution that owns the ATM and use another machine.

**2. Cover your PIN**

Capturing your card data is one thing. But to be most effective at stealing your money, the scammers want your PIN too.

For this reason, most skimmers are also accompanied by a camera, which is designed to capture you entering your PIN on the ATM’s keypad. Again, these cameras can be difficult to detect, given that many are no larger than a pinhead.

To make sure your PIN isn’t secretly recorded, use your free hand to cover the hand you’re using to enter your PIN. This alone should be enough to render most cameras ineffective.

**3. Keep sight of your card**

Not all card-related scams happen at the ATM. Another common place for scammers to steal your card information is at a restaurant or shop. This could involve a waiter taking your card away from your table when you pay the bill but running it through a skimmer while they’re at it. Alternatively, a store attendant may skim your details while it’s behind their desk.

**4. Ask questions**

Some scammers will try to defraud you right in front of your nose.

For instance, a taxi driver may take your card from you at the end of your journey, swipe it and then tell you their EFTPOS terminal isn’t working. In fact, they may have just run it through a skimmer and not the terminal at all.

So trust your instincts. If something looks suspicious, ask questions. Could you see the EFTPOS terminal? If the transaction failed can they provide you with a receipt? If you’re in doubt why not tell the driver you’d like to call the bank to make sure the payment hasn’t gone through? And make a note of the driver’s registration and licence details just to be safe.

**5. Know who you’re speaking to**

You don’t have to have to physically hand your card to another person to have it compromised. After all, we’re often asked to give our card details out over the phone.

In most cases that’s fine. But sometimes a scammer will pose as a legitimate organisation in order to get your details from you. For instance, they may pretend to be a utilities or telecommunications company or another reputable business. So never hand your credit card details out to someone who has called you. Instead, call the organisation back – and use the number on their website to do so rather than one they give you, just to be safe.

The same goes for online transactions. If you’re in any doubt, never enter your account details, even if you’ve clicked on a link that purports to be from a reputable business. Instead, go direct to their website and login.

**6. Check your balance**

Banks are usually quite effective at detecting suspicious activity on their customers’ accounts. But they're not perfect. So check your account balance regularly. When you do, go through your transactions and make sure they match up to what you’ve spent. If you have a joint account make sure your partner does the same.

While this won’t prevent your card details from being stolen or your account from being compromised, it will help you minimise any damage. And, if you notice anything suspicious call your bank or financial institution immediately.

**7. Stay vigilant**

Finally, scammers often rely on targeting us when we’re distracted or when we least expect it. For that reason, many bank card breaches happen in crowded places (such as busy malls), when we’re enjoying ourselves (such as bars and restaurants) or when we’re out of our comfort zone (such as when we’re overseas). For that reason, you should always be especially cautious when you’re at your most vulnerable.

**And if you’re the victim of bank account fraud…**

If you notice fraudulent activity on your bank account, notify your financial institution immediately so that your card can be put on hold or cancelled. You can find [how to report a fraud or stolen card to Macquarie](http://www.macquarie.com/au/about/disclosures/security-and-fraud#?tab:disclosures-security-and-fraud-row=1) here. Alternatively, if you notice scammers at work, always contact the police.