

Video transcript – Episode 3: ATM security

WARREN PERUMAL

EXECUTIVE MANAGER – ONLINE BANKING SECURITY

You may have noticed some recent media coverage about theft of your personal details that can happen when you use your debit or credit card in ATMs or EFTPoS machines. This illegal activity is known as card skimming.

The Commonwealth Bank has a wide range of security measures in place to help prevent card skimming. We also we have a guarantee in place to protect our customers in the unlikely event they are affected by card skimming. In the next few minutes I'll explain a few basic, common sense steps you can take to help protect against skimming.

Card Skimming occurs when criminals attach illegal devices to ATM or EFTPoS machines. These illegal devices are designed to copy, or "skim" the details of your credit or debit card and capture your PIN. With this information a fake card is created and used along with your PIN to access your accounts and steal money.

At an ATM, skimming is achieved by attaching a card-reading device over the regular card entry slot. And a hidden camera or fake keypad overlay is the used to capture your PIN.

EFTPoS skimming is almost impossible to detect because the skimming and PIN capture usually happens inside a tampered machine with nothing suspicious visible on the outside. It's not until the bank – or sometimes customers, notice unexplained transactions or money being withdrawn from accounts that the skimming activity is discovered.

So how can you tell if skimming might be occurring at an ATM or EFTPoS machine you use – and what should you do about it? Skimming is not easy to detect – but there are some tell tale signs you should make yourself aware of. Does the ATM look normal? Apart from usual wear and tear are there any unusual markings or changes in its appearance - things like cuts or cracks, glue residue, exposed wires or the remnants of double sided tape.

Does the card entry slot look normal – or does it appear to have an extra device attached to it? Can you see the green reader light flashing? Same for the keypad. Does it look normal? Or does there appear to be an extra layer over the pad?

A hidden camera is the most common way criminals use to learn your PIN. Are there any new or unusual items mounted on or close to the ATM like this light diffuser that contains a hidden camera filming PINs being entered?

It may not be easy to spot skimming devices on ATMs – but there are general precautions you should always take when using an ATM to help protect against skimming.

If you use a particular ATM regularly, familiarise yourself with its features and appearance. This will help you notice when anything appears unusual with the ATM. Also cover your hand when entering your PIN. This is just a normal precaution that helps keep your PIN secret from any prying eyes or hidden cameras.

As well as a copy of your credit or debit card a criminal involved in skimming also needs your PIN. So apart from shielding your PIN when entering it into an ATM, you should also choose a PIN that's not obvious or easily discovered. Don't write your PIN on your card or ever keep it with your card. Also, don't use the same PIN for any of your other cards.

Never provide your PIN in response to phone or email requests and change your PIN regularly at any ATM or Commonwealth Bank branch.

If you believe an ATM appears suspicious or has been tampered with – don't use it. Report it to the nearest bank or the police.

Many of the precautions that apply to ATMs also apply to EFTPoS machines - like covering your hand when entering your PIN – and keep your credit or debit card in sight during a transaction. Be suspicious if a shop assistant wants to swipe your card out of sight – or in a second machine. If you have doubts, you should refuse, pay by cash or leave the store. Back at home, you should regularly check your statement for any unauthorised transactions. NetBank is a convenient way to do this, online, anytime.

You should immediately change your PIN as soon as you suspect skimming or any suspicious activity has occurred on your account – and immediately report the activity to the bank.

Skimming is a serious crime and we are investing in the latest technology to keep our ATMs and EFTPoS machines free of skimming devices. So while you should be aware of skimming and know what to look out for, it's important to understand that only a very small proportion of ATM users have been affected by skimming.

Commonwealth Bank serves 10 million customers throughout Australia – and the number of our customers who have been affected by skimming is a fraction of one percent.

And we guarantee to refund the value of fraudulent transactions within five business days if the loss was due to skimming. ATMs and EFTPoS machines have become a way of life because they offer tremendous convenience and access to your funds 24 hours a day.

It's very unlikely that you'll ever be affected by card skimming – but knowing about the simple precautions I've covered in this video, combined with our guarantee, you can continue to use all Commonwealth Bank ATMs and EFTPoS machines without worry.

(LOGO: Commonwealth Bank)

(SUPER: DETERMINED TO BE DIFFERENT)

(SUPER : To find out more, visit
commbank.com.au/security)