'Electronic pickpocketing' looms as next threat in credit card fraud, police, security experts say

Reported By Nic MacBean
Dated 30 May 2014

Photo: Cybercrime detective Brian Hay says identity thieves may exploit tap-and-go credit card technology to wirelessly pick people's pockets. (ABC News: Giulio Saggin)
Related Story: Tap-and-go cards boost crime stats: Victoria Police
Related Story: Romanian man faces Sydney court over ATM skimming charges
Map: Australia

Identity theft doubled from 2012 to 2013 and police are concerned about "electronic pickpocketing" as organised criminals get smarter and take advantage of weaknesses in Australians' defences.

A study by financial security firm Veda shows credit application fraud is at its highest level since 2009 in Australia, and the company says the main reason is the growing technical skill and innovation of organised criminals.

Queensland fraud and cybercrime detective Brian Hay shares that view, and has warned the ABC that identity thieves may exploit contactless credit card technology in order to wirelessly pick people's pockets.

He says all it takes is a little technical know-how and a $130 trip to an electronics store to give a potential criminal the tools to steal card details in this way.

The warnings about the rising tide of credit-card theft come after Victorian police said on Wednesday that contactless credit cards were one of the main drivers behind the rise in crime rates in the state last year.

Victoria Police Chief Commissioner Ken Lay said there were 11,600 more credit card deceptions in the 12 months to March 2014 compared with the previous year, and the issue was "chewing up an enormous amount of police resources".

This is what you had to say about electronic pickpocketing and the hacking of tap-and-go cards.

Contactless credit cards such as Mastercard's and Visa's Paypass, payWave and Tap&Go let people make purchases of less than $100 without needing a signature or PIN, and police say it is easy for thieves to take advantage of this.

Police around Australia have given many examples of this type of theft, such as an elderly Tasmanian man whose card was used repeatedly for five days in 2012 before he realised it had been stolen.

Detective Superintendent Brian Hay says the $100 limit means these types of theft are largely opportunistic, and he is more concerned about the potential for "electronic pickpocketing".

CONTACTLESS CARDS VULNERABLE TO HACKING

The cards use radio-frequency identification (RFID) technology, which is vulnerable to hacking.

Mr Hay says while the majority of the credit-card information is encrypted, the card number and expiry date is vulnerable.

HOW ELECTRONIC PICKPOCKETS OPERATE

Detective Inspector Brian Hay, from Queensland Police's fraud and cybercrime squad, describes what he would do if he was an "electronic pickpocket".

"So I know it's you because you're my target. I'll stand close to you in the train and that will allow me to clone your card from your pocket.

"I visit your LinkedIn profile and identify where your work history is and who you've been working with and how long you've been there for.

"If you've got a Facebook profile I'll take the details off that. I'll probably find out where you live because you uploaded a photograph from your iPhone of last weekend's barbeque and you didn't disengage the geotag setting so I know exactly where you live.

"I'll put a profile together, take out an online loan application for $20,000 or $30,000 as well as take out a couple of new credit cards in your name.

"So rather than extract a couple of hundred or a thousand dollars from your card, I'll take out $30,000 of debt in your name."
"As the card's chip gets closer to an electronic pulse, it will emit data," he said.

"Some of that data when it transacts with your credit card is in an encrypted format, but the number of the card and the expiry date is not encrypted so essentially it could be cloned.

"What that means is it gives potential for card cloning and identity takeover if you know your target."

He says the technology is cheap and readily available in stores like Dick Smith, and he estimates that $127 and technical skill would be enough to buy components and build an RFID hacking device.

"If I had one of those in my pocket, satchel or briefcase, and you were standing next to me on a train and your wallet was in your back pocket and I moved near enough to activate the signal on the RFID, well then I've got your details," he said.

He is keen to stress that electronic pickpocketing is a potential threat rather than an existing problem, but it is a real concern for police.

"It's not a technique that we're seeing criminals adopt at this point in time, but it's a vulnerability in the system," he said.

Research by credit-security experts Veda suggests it is precisely these vulnerabilities in the system that criminals are exploiting.

The company analysed frauds on Australian banks and credit providers, finding an overall rise of 27 per cent and a 103 per cent spike in identity theft.

The increase in credit application fraud can be partly explained by growth in credit markets," said Imelda Newton, general manager of fraud and identity solutions.

"However the real driver has been a change in the way individuals and criminal gangs are using new technologies to exploit and defraud credit providers."

RISK OF IDENTITY FRAUD INCREASING, FORENSIC SPECIALIST SAYS

Forensic specialist Brett Warfield says fraudsters are increasingly stealing identities rather than creating bogus identities because credit providers have gotten better at spotting fakes.

"The shift from identity fabrication to identity takeover confirms that fraudsters are adapting to improvements in identity verification and checking practices," he said.

He says people's identities are getting easier to steal because online traders and merchants are increasingly storing customers' details in databases.

The Veda research draws on an extensive database of confirmed frauds, but Mr Hay says such information is lacking because so much fraud goes unreported to police.

"If you talk to someone who has had their card data compromised, the typical response is that they call the bank, the bank repays the money and issues a new card, but the person doesn't go to the police," he said.

"Does the bank or the card-issuing authority go to the police? No.

"So we've got a constant daily avalanche of these illegal card transactions taking place ... and we don't know from a law-enforcement perspective what the true situation is."

He says he expects this to be the case with electronic pickpocketing because people will not realise their details have been stolen until a fraud occurs, and they might not even realise it then.

"You've got to look for the $1 or $2 transactions which means your card has been compromised," he said.

"That means your details have been traded in the black markets globally and they've done a little tester to see if your card's still active."

He says there is no way to "turn off" the RFID chip in cards, but he has heard of people wrapping their cards or lining their wallets with aluminium to block the signal.

Ms Newton says banks and credit providers can do their bit by introducing more effective identity-checking procedures, especially "out of wallet" checks like secret questions.

"The best protection ... is for credit providers to work together and and adopt a multi-layered approach to detecting fraudulent activity," she said.

Submitted by Todd Tinker, Manningham Council