



smh.com.au
 The Sydney Morning Herald
 Print this article | Close this window

The great credit card swindle

Conrad Walters and Nick Galvin
 October 7, 2008

Australians lost more than half a billion dollars in credit card fraud last year, and security experts warn that banks are not doing enough to protect customers online and are playing down the problem for fear of harming their reputations.

Last year 383,300 people lost an average of \$1600 to credit card fraud, says the Bureau of Statistics, which acknowledges the true figure is much higher.

This is because the bureau's survey into personal fraud - the first of its kind - recorded only an individual's most recent loss, but one-third of victims admitted they had been bilked two or more times.

Further losses were suffered by 124,000 victims of identity theft and 57,800 people defrauded by "phishing" - online scams that collect personal details.

An investigation has found hackers, computer security experts and law enforcement authorities agree that online crimes involving credit cards and other transactions are easy to commit, hard to track and that criminals quickly circumvent new security measures.

In spite of this, bank customers are given little information about the severity of the problem.

Between 2006 and 2007 the dollar value of fraudulent credit card transactions grew by 30 per cent and the volume of illegal transactions climbed by 35 per cent, says the Australian Payments Clearing Association, which collects statistics from the nation's financial institutions.

While its figures show progress against activities such as cheque fraud, credit cards are the biggest and fastest-growing area of fraud, especially within online use.

Finance and computer experts say the growth is the result of banks inadequately protecting consumers.

"To encourage customers to get into online banking, the banks and online merchants downplayed the risks of fraud," said Andrew Wallis, an analyst at the independent research company Gartner.

"It's a classic thing. How do you get people moving into something? Well, you don't tell them it's dangerous. You don't mention the negative side. You'll extol the virtues and the benefits."

The benefits are clear - fewer tellers for banks and greater convenience for customers - but the dangers are complex.

"Realistically, the vast majority of people are never going to become computer security experts," Mr Wallis said. "It's the banks' responsibility to do everything they can to protect the customer."

Advertisement

Who are
 your
 ancestors?

ancestry.com.au

Steve Lewis, of the security software vendor VeCommerce, said: "I talk to some of the chief security risk officers in the banks. You don't hear much about it in the media but, once you're in there having a quiet chat, you learn there is a lot going on, a lot that is not talked about."

Katrina Ryan, a student from the northern beaches, learned a lot more about online fraud than she wanted to after receiving a phone call from her bank one evening. "The guy said they had detected irregular spending habits on the card - things I wouldn't usually spend money on - and they thought it was fraudulent and they had cancelled the card," Ms Ryan said.

Included in the \$2000 binge was \$900 worth of liquor. But when the thieves decided they fancied a \$2500 television, their luck - and available credit - ran out and the Commonwealth Bank stepped in.

Ms Ryan then had to go to the branch and begin the arduous task of sorting her legitimate purchases from the crooks' spending.

It was nearly two months before her money was returned to her and she was able to begin using her new card.

"They were good at detecting it but investigating it and getting the money back into my account took forever," she said.

No is sure how the thieves obtained Ms Ryan's card details, but she suspects it may have happened while shopping online.

The bureau's fraud survey of 14,300 people, released in June, found 3.2 per cent of people over the age of 15 had lost a total of \$615.4 million through credit card and bank card fraud in the previous year.

This is more than five times higher than the payment clearing association's self-reported figure of \$111 million from banks and card issuers.

The chief executive of the association, Chris Hamilton, said he stood by the lower figure while conceding he could not account for the discrepancy.

"It's as reliable as any full, self-reported statistical collection can be," he said. "[Banks] might be disinclined to provide information sometimes. But when asked a direct question, it's been my experience that they tell you the truth."

Mr Hamilton said banks reimbursed customers for most losses, although he recognised card fraud caused tremendous inconvenience for individuals.

Several banking executives said getting the right level of security for online banking meant balancing competing needs.

"You could lock it down completely, and then no one could use the system," said John Geurts, head of security at the Commonwealth Bank.

"It's like the perfect hospital. You wouldn't have any patients. [At] the perfect secure bank, you wouldn't offer these services. But that's not what the consumer wants. That's not what we want."

He said a "healthy tension" existed between customers, banks, regulators and shareholders, and that any investment to increase security needed to justify itself financially.

Mr Geurts said the bank's internet fraud losses were "negligible" and that customers were reimbursed in most cases where fraud was alleged - although he declined to quantify that.

But while some level of fraud may be an unavoidable cost of doing business for banks, there is alarming evidence that some stolen cash is funnelled into the coffers of organised criminals and, potentially, terrorists.

Many of the hackers who steal information are small players who on-sell it to more sinister elements who then launder the proceeds.

Mr Wallis explained the process from the perspective of a typical hacker who has acquired credit card details. "I'm a hacker," he said. "I don't know anything about money laundering. Well, who's good at money laundering? Let's see ... drug merchants, arms merchants, all the things that are classics in organised crime."

No one denies banks have instituted measures to inhibit credit card and online frauds. Credit cards with magnetic stripes are being replaced by cards with an encrypted computer chip and a PIN. And many financial institutions issue customers with "tokens" that generate a random, changing number to ensure their online banking transactions are protected beyond simply entering a user name and password.

But Cambridge University researchers announced in June they could compromise chip-and-PIN cards, and scammers can infect computers with "trojan" software that captures the fleeting numbers displayed on tokens.

Late last year, Commonwealth Bank customers were targeted by a particularly virulent trojan. Discovered by F-Secure, an anti-virus vendor, the trap planted "malware" - malicious software - on unprotected computers.

From the customer's perspective, everything was done correctly, said Fei Wing Chia, security response manager for F-Secure.

Customers went to the correct site, logged in properly and saw the familiar padlock that indicated the site was secure. But then the trojan jumped into action. If the customer was transferring funds overseas, it inserted an extra box on the webpage and captured a special password reserved for such transactions.

A customer might legitimately transfer \$100. "The trojan then inserts an additional transaction to a money mule's account," Mr Chia said. The "mule" would then transport the money to a safe place and split the proceeds with the hacker.

Australia was the sixth most targeted site in the world for trojan attacks, he said.

This story was found at: <http://www.smh.com.au/articles/2008/10/06/1223145272367.html>