HACKING With scams and security breaches rife and arrangements protecting bank customers from net fraudsters coming under review, many computer users are ill equipped to protect themselves.

World Wild Web

By **MARC MONCRIEF**

THE X-men lie stacked in the corner, powerless before Matthew Hackling. In Hollywood, Mystique, Iceman and Nightcrawler are the names of super-powered mutants from the *X-Men* franchise of movies and comic books. To Hackling and his peers in the anti-hacker squad of business consultant firm Deloitte, in Melbourne, these are the names of guinea pig PCs that lack the security updates so many of us also lack. The computers that wear them, white letters on peeling black labels, are easy pickings.

Here, in a white room furnished with standard corporate cubicle wood-grain desks, Deloitte tests the online defence systems for some of Australia's biggest corporations. Companies send in their websites and Hackling and his team chop them to bits.

I am only the second person from outside Deloitte allowed inside Hackling's electronically sealed, three-by-five-metre inner sanctum. The first was a client who demanded the same demonstration I was about to receive.

Hackling invites me to log on to Iceman, a computer that, like most home computers, has nothing to protect it from a hacker attack. It has no anti-virus software, no security updates for its operating system, nothing to stop an intruder from tapping into its internet connection.

I invent a password to log on and type a sentence I leave stranded in a big white text box on the screen's desktop. I lock the system down.

Within seconds, using a computer across the room and software freely available over the internet, Hackling has stolen my password, broken my encryption and gained access to the computer. He takes a picture of my lonely sentence ("Hey, how you going?") and flaunts it to his colleagues.

If it had been my home computer, he could have stolen my schedule, my contacts, my bank information, my photographs, whatever sits in cyber storage. The violation complete, he promises the computer's log will carry no trace of the crime. The whole thing was done under my name.

The wall above Hackling's terminal boasts a modestly framed diploma in security studies. One imagines nightclub queues or prisons, and wonders how Hackling ended up in the BHP Billiton building. But Hackling's expertise is being used to fight a war in the air around us — a war with virtual spies, virtual assaults and very real casualties.

The Australian Bankers Association estimates its members lose about $25 million a year to online fraud as customers innocently buy gifts, contact friends or manage their finances over the internet. However, estimates vary widely because it is almost impossible to know what percentage of online fraudsters are caught. It's not like an old-school bank robbery, where the man with the gun is clearly indicating a theft is taking place. KPMG partner Gary Gill says $25 million a year sounds "pretty low".

So-called "phishing" scams — the ubiquitous emails fraudulently asking people to update their banking or credit card information — capture the unwitting and the unprotected. And as computer users become more familiar with such scams, fraudsters have become more cunning.

Mark Voss, director of information security at accounting firm Pricewaterhouse-Coopers, describes software that can embed itself in a computer, waiting for a user to log on to a certain website — a bank, for example. The program will automatically reroute the user to a false-front website that mimics the site he or she expects. The user enters username and password and unwittingly allows an international criminal syndicate access to his or her accounts.

Voss says web browsers are built with a defensive mechanism against this kind of attack. Websites are certified according to their domain names and when the two don't match, the browser should warn the user. Unfortunately, he says, tests show that 100 per cent of users ignore the message.

It's not just the casual home user who ignores basic security measures, either.

Hackling once strolled through Deloitte's own 14th-storey office in the BHP building and found more than 40 unprotected wireless networks ripe for the picking. Families use the same trendy wireless networks to access the internet from around the house, or while taking tea in the garden.

Using a modest antenna, one could access these networks from kilometres away, Hackling says. Free, unlimited internet access could allow criminals to send spam emails around the globe or even attempt to break into other, more secure networks. If the attack is traced, the unsuspecting family or business whose line is exploited could fall under suspicion.

Hackling describes teams of hackers driving around in vans full of signal scanners, searching neighbourhoods for accessible networks. He says it is more common than anyone outside the industry would imagine. Businesses and households lagging behind on the security updates issued every month by Microsoft and other software companies are easily compromised.

Customers using the internet to do their banking are at present protected from the fray by an arrangement under which banks reimburse customers for money lost to internet fraudsters. Soon, that arrangement could change.

Last month, the Australian Securities and Investments Commission announced a review of the code of conduct applying to electronic money transfers — banking done via EFTPOS, ATM, telephone and the internet.

It is under this code that banks voluntarily repay customers for money lost online, but *The Age* has received anecdotal reports of abuse levelled at customers who have sought to recoup lost money, indicating sometimes the service is provided with less than a smile.

ASIC stresses that the review of the "EFT code" has just begun, but it confirms that it will consider whether customers should bear some of the responsibility when hackers break into their personal computers. ASIC's executive director of consumer protection, Greg Tanzer, says it might be appropriate for some customers, such as those who have been defrauded a number of times but have failed to put any protective measures in place, to carry some of the liability for lost money.

Australia Consumer Association finance spokesman Nick Coates says banks and other financial companies had made good money as customers moved online. He warns they will probably try to make even more by shifting the costs of that move onto users.

"Consumers, having struggled with using the internet and moving online, and being concerned about using that new technology, could face a situation where they don't have the skills to understand what they need to do to fulfil their duties under the EFT code," Coates says.

Security specialist Matthew Hackling is fighting a war against virtual assaults. PICTURE: ANDREW DE LA RUE

ASIC is now accepting submissions for its review, which will ask whether households are equipped to battle a global enemy who seems always one step ahead of the security industry. This week, hackers attacked at least three of the internet's 13 "root" servers — the computers that maintain the internet's domain name system. The systems were able to handle the attack, but the methods used revealed a higher level of hacker sophistication than ever before seen. The pimply-faced teen with a modem and a mischievous tic has given way to sophisticated criminals motived by profit rather than adrenaline.

Several months ago *The Age* was contacted by a computer programmer who said he had developed software that would end the banks' security problems. He claimed to have contact with Russian organised crime syndicates dedicated to identity theft, which he said were responsible for phishing and spyware attacks around the world, including Australia. He claimed a familiarity with criminal systems that would allow him to undermine their attacks. He had access to a network of web-based hacker communities where tricks were shared. Screen shots of the online account pages of apparently innocent bank customers were displayed like trophies.

When we next attempted to contacted him, he was in jail. It seems the man with the solution was also the problem.

High in one of Collins Street's most prestigious corporate towers, green Japanese characters spill down a wall. It is a screen saver based on the opening sequence of the *Matrix* movies projected from the laptop of KPMG security specialist Ian Green. They vanish when Green tickles the mouse of "Coopers". In KPMG's geek fiefdom, the computers are named after beer.

The website of a fictitious shipping company (Hacme) appears in the projection. Green (who has since moved to National Australia Bank) logs on to the site and shows how simple it is for a hacker to steal the user identity of a system administrator if a company has not put enough thought into its web architecture. This kind of attack lays bare the company's entire database.

KPMG partner Rob Greenberg says the IT industry is resigned to following failure with short-lived success. No matter how comprehensively tests are carried out, the possibility of a new hack being developed is ever-present. Developers often do not know what the vulnerabilities of their software may be until they put it out into the world and allow the hackers their pleasure.

"They have endless resources and teams working 24 hours a day," Greenberg says.

He says web services — applications, such as calculators, that are available online — will be the next key battleground for hackers.

Third-party sites send user queries to web-service applications, often without the interaction being noticed by the user. Hackers may be able to exploit the communication to compromise any referring site. It could mean access to thousands of users through just one well-placed hack.

How can you protect yourself? Greenberg shrugs.

"Keep your anti-virus up to date," he says. "Get a personal firewall. Make sure your wireless is encrypted." And pray, I hear.

As I leave the KPMG building, thinking of my innocent laptop sitting defenceless at home, I marvel aloud at the danger. From behind one of the cubicles, the voice of an eavesdropper whispers: "You ain't seen nothin'."

Marc Moncrief is an *Age* business reporter.

LINKS

- www.staysafeonline.info
- geobay.com/d61192