

Unmasking the thief within

IDENTITY THEFT IS MAKING INTERNET CRIMINALS FILTHY RICH TO THE TUNE OF \$3.56BN. **IS THERE A WAY TO STOP THEM?**

BY SARAH STOKELY

In the recent movie *Firewall*, Harrison Ford's character Jack Stanfield discovers he's been a victim of identity theft after a debt-collection agent shows up at his office demanding payment for online gambling debts Stanfield never incurred. Yet the phenomenon of online identity theft, in which fraudsters obtain and use the victim's credit card or other personal details, is not confined to Hollywood. The practice of phishing, or tricking people into disclosing personal data online, is estimated by analyst firm Gartner to have netted criminals about \$3.58bn worldwide in 2006.

One common form of phishing is for the perpetrator to set up a spoof website that looks very much like a genuine banking website. Thousands of spam emails that have a link to the sham site are then sent out, requesting that consumers log in to confirm their personal details. If consumers are tricked into thinking the request is genuine, they've just handed over ID details such as their bank account or credit card details to an online fraudster.

Identity theft is not only an online crime. For example, it's possible to access personal or company data from a lost or stolen laptop, or a discarded credit card slip. But the ability to reach hundreds of thousands of potential

victims via email is a very cheap and fast way to perpetrate this style of crime.

While other online criminal activities, such as hacking, rely on the perpetrator gaining access

to a company's computer network, phishing is much simpler because it relies on tricking people into voluntarily giving up their information.

Phishing attacks on the rise

The bad news is that the number of phishing attempts being made appears to be on the rise, as are the amounts being lost to scammers. Internet security software company Symantec's global *Internet Security Threat Report* found that in the first half of 2006, there were more than 150,000 unique phishing attempts globally. In June 2006, the Australian Securities and Investments Commission (ASIC) revealed that complaints about phishing accounted for more than one in five of all consumer scam complaints it received during the 2005-06 financial year.

ASIC says the number of phishing complaints has increased by 25 per cent over the past two financial years. Financial institutions, governments and online retailers have all taken measures in recent years to clamp down on online crime, and bolster consumer confidence in online trading.

Although many spam and phishing





originate from the US, Australia has its own phishing attackers. In June 2006, the Bleeding Edge blog (www.bleedingedge.com.au) run by INTHEBLACK's Inspector Gadget and *Age* columnist Charles Wright reported receiving a phishing attempt posing as a letter from Westpac Bank. The email suggested the recipient click on a link to view the bank's updated internet banking terms and conditions. Clicking the link led to a website >



● **By using images instead of text, messages are able to avoid detection by unsophisticated anti-spam filters that rely purely on the analysis of textual spam content** ●

> that seemed to duplicate the Westpac sign-in screen perfectly.

As online threats are exposed, phishing perpetrators are changing their clandestine tactics. "Cyber-criminals are starting to shift away from attacking online banks directly," says Gartner analyst Avivah Litan. "They are leveraging

less-conventional brands or using hard-to-detect social engineering methods to reap financial gains." Internet software security firm Sophos produces an annual *Security Threat Report*. The most recent edition found that more than 75 per cent of all phishing emails detected in 2006 were targeting users of PayPal or eBay.

In recent times, phishing attempts have begun to be disguised as news bulletin emails claiming to be about current events, such as the death of US celebrity Anna Nicole Smith. IDC Australia senior security analyst Patrik Bihammar says attacks focused on individuals are on the increase. "Spear-phishing is a highly targeted phishing attack," he explains. "Whereas traditional phishing scams are designed to steal information from individuals, spear-phishing attempts to gain access to a company's entire computer system."

Targeted attacks occur because scammers are trying to move up the food chain, either by gaining access to large amounts of corporate data through spear-phishing, or by focusing attacks on more lucrative targets, such as holders of "gold" credit cards that have larger credit limits. According to Gartner's survey, the average loss per victim grew from \$328 to \$1588 per victim in 2006. "Thieves seem to be targeting higher-income earners who are also more likely to transact on the internet," says Gartner's Litan.

Phishing attackers also evolve, changing their methods to get around common security practices. According to Rob Forsyth, the Asia Pacific managing director of Sophos, we can expect to see an increase in spam messages that contain JPG or GIF images and links to infected websites. "By using images instead of text, messages are able to avoid detection by unsophisticated anti-spam filters that rely purely on the analysis of textual spam content," Forsyth explains. In one example, a scam claimed to be directing users to



a site where they could download free educational toys from the popular children's show *Sesame Street*

Protect your clients

Fraudsters may try to steal personal details directly from individuals but it's much more effective for them to fraudulently access the details of thousands of consumers via vulnerable business databases. In one infamous case in 2005, ChoicePoint, a US provider of identification verification services for business and government, mistakenly granted access to its data records to an illegitimate business.

The gaff exposed 145,000 customer accounts to potential abuse. The company reported \$14.6m in charges relating to the incident – not to mention the \$19.2m fine ChoicePoint incurred from the US Federal Trade Commission.

This is an extreme example, but all organisations keeping records of their customers' private data need to ensure the data is secure. "To effectively prevent fraud and unauthorised data access, enterprises must secure both the front and back doors into their accounts," Gartner's Litan warns. "They must move beyond authentication that relies on passwords, especially for sensitive or high-risk transactions, and monitor back-end account activity, such as suspicious inter-account transfers or insider theft of sensitive information."

"This can help ensure that no matter how an impostor gets into an account – for example, through insider activity, the phone, a store or automated teller machine (ATM) – the illegal activity can be stopped in its tracks."

Responding to the threat

For a small business, the challenge is twofold. Accounting and business advisory firms that hold valuable client data on site must keep it secure. They also need to protect their own data. In addition, clients will often look to their accountant or financial adviser for guidance on internet and data security. "One of the best remedies is user education and awareness," explains IDC's Bihammar, adding that internet security relies on a combination of technology and human behaviour. "Users need to be sceptical, and not click and believe everything they see." It sounds obvious, but it's a point well worth making to clients.

Bihammar also points out there are other ways, apart from online scams, in which data can be >



● **One of the best remedies is user education and awareness. Users need to be sceptical, and not click and believe everything they see** ●

Patrik Bihammar IDC Australia
senior security analyst



> stolen. Data can also leave your business by walking straight out the front door. "Laptop and mobile device theft and loss is a big problem," he says. "End-point or mobile encryption is a way of limiting the damage of loss of sensitive data."

In addition to the obvious steps of warning staff about dodgy sites and the like, security measures need to be built in to your computer network to reduce the threat of internet security breaches.

As online attacks evolve to counter common security measures such as anti-spam filters, its necessary to keep up to date with security-prevention measures. Regular updates

to your computer operating system and security software is a must, and you may also wish to consider other forms of security software.

Software companies have also begun to build anti-phishing tools into their browsers. Both Mozilla's Firefox browser and Microsoft's Internet Explorer 7 (IE7) try to flag known phishing attack

sites to consumers. But analysts say many attacks could still slip through. "Many of the browser upgrades are still incomplete and immature in terms of protections afforded," Litan says. "For at least two more years phishing attacks will continue to increase, since it's still a lucrative business for the perpetrators.

"The anti-phishing measures some enterprises



have put in place to protect their brand and their consumers are not working,” she adds. “Phishers are moving from site to site to launch their attacks more quickly than ever. The average life of phishing sites has gone from one week a couple years ago to about one hour in 2006. Within a year or so, phishing sites may be user-specific – that is, a single site will be set up to launch a phishing attack against a single user. It’s no wonder the detection services can’t keep up with these rapid criminal movements.”

Security products

Even small businesses that use a single computer need adequate internet security to avoid the risk of online threats. Choose carefully and you may be able to find inexpensive software that meets your needs. Some free open-source software such as AVG (anti-virus) or Check Point’s ZoneAlarm (firewall) have good-quality free software, with the possibility of upgrading to a more full-featured, paid version if desired. You may also want to consider intrusion detection and anti-spyware software for further protection.

Traditionally, security software products such as anti-virus or anti-spam performed a single action. But recently there’s a trend towards security companies offering all-in-one products and security services. Microsoft Windows Live OneCare is a subscription service that includes anti-virus, anti-spyware, anti-phishing, and two-way firewall. It costs \$99.95 per year to cover up to three computers. Internet security software company Symantec has a similar service called Norton 360.

Another provider of managed security services is Message Labs. It manages email security by filtering emails before they reach the client company, using predictive intelligence technology, signature management and client-configurable, approved and blocked sender lists.

One advantage of managed services is the predictable cost and scalability of the service. The downside, of course, is that it is an ongoing cost rather than a one-off investment in a software package. Internet security can also be built into your computer hardware, rather than simply using security software. One company that performs this service is Fortinet. Its FortiGate-60 product (RRP \$1030) can handle the security needs of an office of up to 50 staff. It includes a four-port 10/100 ethernet switch, as well as firewall, anti-virus, anti-spam, VPN, intrusion prevention, and anti-phishing features.



If there are concerns about employees compromising a company through inappropriate email or internet behaviour, it may be prudent to institute an internet usage policy. It may also be wise to consider software such as web and email filtering product SurfControl, which blocks inappropriate internet usage.

Yet no amount of expensive software can protect a company from online fraud if careless internet usage puts data at risk. By ensuring that you and your employees remain aware of the risks and trends in online fraud, you're less likely to become a victim of this insidious type of crime. ■

