# GOING PHISHING

THE SCARIEST THING ABOUT CYBERCRIME IS THAT YOU MAY NOT EVEN KNOW YOUR BUSINESS IS A VICTIM. SCAMS TO GAIN ACCESS TO YOUR COMPUTER SYSTEMS HAVE BECOME HARDER TO DETECT, WITH CORPORATE COMPETITORS AS WELL AS THIEVES OUT TO STEAL YOUR DATA. BY **JACKIE CAMERON**

Paul Orffer doesn't come across as someone who is out to hoodwink you – or anyone else for that matter. Clean-cut, with movie-star good looks and a polite demeanour, it would never occur to you that he has attempted to dupe you into compromising your company's computer network. You will only find out after you have fallen into one of his traps, when your boss calls you in to explain why you have ignored policies aimed at safeguarding corporate secrets and client data.

Johannesburg-based Orffer is among the growing ranks of highly trained risk specialists whose job it is to identify where big organisations have weaknesses that could allow intruders to access their IT systems. Senior manager of risk advisory, RA security, privacy and resiliency at big accounting firm Deloitte, Orffer is paid to think and act like a criminal. He uses a range of tactics to figure out who will succumb to devious ploys, effectively opening the company's doors to people with sinister intentions.

For example, Orffer has left USB drives on desks to see who will take them home (even though they don't belong to them) or plug them into their office computers. As soon as files on the drives are opened, secret messages are sent back to Orffer (he may make it more tempting by using file names such as 'My Pictures'). Other times, he distributes emails encouraging people to click on the kinds of links they have specifically been asked to stay away from at work.

'Fake South African Revenue Service tax return documents work well, as do fake banking notices,' says Orffer of the types of electronic lures that are most effective. It takes very little to activate a program that will send files in search of your company's most sensitive data – from boardroom minutes to top clients' financial details – and transmit it beyond computer firewalls, he cautions.

## VIRUS CHECK

According to global anti-virus software provider Kaspersky Lab, roughly one out of every 10 South African companies has experienced an attempt by outsiders to infiltrate its computers in the past year. At least half of all the IT decision-makers surveyed by Kaspersky admitted they do not believe enough is being done to secure systems. And, when it comes to cyber-crime, sinister strangers can be less of a worry than the culprits sitting right next to you. A recent survey of South African companies by Kaspersky Lab indicates attempts to breach security from inside organisations are almost as frequent as those coming from outside.

Riaan Badenhorst, head of Kaspersky Lab's operations for sub-Saharan Africa says hackers have accessed the network infrastructures of approximately 13% of local companies. But only about a third of hacking breaches are a result of faceless intruders exploiting vulnerabilities in the company's software.

'Targeted attacks are complex and typically they involve a long period of preparation during which malicious users try to find the weak points in a corporation's IT infrastructure and locate the tools necessary to launch the attack.' These weak points are often people, he says.

An expert in international software security, Alex Balan of BullGuard agrees technology alone does not offer enough protection: 'You always need more than just software, to be on the safe side. Software is automated, so it can help prevent many problems – but not all.'

*It takes very little to activate a program that will send files in search of your company's most sensitive data – from boardroom minutes to top clients' financial details*

## *SLICK TRICKS*

IT specialists have a term for the practice of manipulating insiders in order to facilitate infiltration of confidential systems: 'social engineering'. Approaches are often made through email, but con artists also contact individuals in other ways, such as over the telephone. They may sound as if they are from an organisation the company deals with and divulge confidential information in order to gain trust and get someone to, in return, share vital information such as a password.

Balan gives an example: 'You might get a call from someone who tells you there has been an unusual payment from your account that they would like to verify and that, before they can go further, they need to make sure you are the correct account holder by checking details such as your mother's maiden name and so on – which they already know. You might be directed to a website next so that you can type in your password.'

A common tactic used to fool people into turning off essential company anti-virus and hacking protection is hidden in enticing-looking games. 'The instructions will ask for you to disable the anti-virus software so the game will work properly,' says Balan.

The trend is increasingly for those with ill-intent to customise their phishing attempts, says Orffer. He is referring to the type of fraud that involves sending out seemingly legitimate correspondence in order to gain access to passwords and other information. Criminals will look at your social media sites and even phone family and friends, gathering information in preparation to sting the company you work for.

## *INSIDE JOBS*

Worrying, too, is that people are being either planted or coerced into knowingly working with outsiders who are up to no good. David Loxton, co-head of the Johannesburg forensics team at law firm ENS Africa, has been kept busy piecing together details of international crime syndicates that have infiltrated a large South African company by posing as contract workers.

It took several years for those at the helm of the company, which is listed on the Johannesburg Stock Exchange, to realise criminals were stealing information linked to its clients and operations. 'They copied products and even accessed board packs and business plans,' says Loxton.

> *People are being either planted or coerced into knowingly working with outsiders who are up to no good*

ILLUSTRATION: GALLO/GETTYIMAGES

## QUICK ANTI-CYBERCRIME TIPS

- Be careful who works for you. Those contract workers may seem cheap and efficient, but they may not be employed only by you, warns David Loxton of ENS Africa.
- Lock down the data. In this era of bring-your-own-device (BYOD) and cloud storage, organisations are no longer in control of their own IT perimeters, says Charles Foley, CEO of Watchful Software. Data-centric security, which mixes classification technology, encryption technology and rights-management technology, can help mitigate this risk, he says.
- Deter shoulder-surfing. Customers and colleagues can take sneak peeks at passwords and smartphone cameras can be used to make permanent records of screens, points out Peter van der Sluijs, an analyst at Secure (European Association for Visual Data Security). 'Intelligent siting of workstations' is one way to stop this, although you can also buy privacy filters for screens in order to restrict the field of view, he says.

The investigation has become an international matter, requiring liaising with senior officers of the Federal Bureau of Investigation in the US. The syndicate's organisers are believed to be based in Russia. So far, two foreign nationals, both of whom were hired by the company on temporary contracts, have been arrested, says Loxton. The company involved has not divulged further information about this serious breach of its system because it fears the damage to its reputation may lower its share price and cause its clients to worry that their personal information too has also been exposed. Loxton says it is more common than not for companies to keep secret the fact that they have been victims of cybercrime.

Ed Wallace, head of incident response and advanced threats at international information security company MWR InfoSecurity, agrees that such security failures are usually kept under wraps. 'Everyone always denies it,' says Wallace, whose company has a growing team based in Johannesburg.

He also says it is strongly suspected that major culprits are state-sponsored. This is because the targeted companies are often competing with state-owned corporations (particularly Russian or Chinese ones) for big international contracts. And, they are losing data linked to mergers and acquisitions, corporate pricing and other information of potential commercial interest. Financial services, oil, gas, mining, energy-construction and telecommunications-related companies are especially vulnerable, says Wallace.

What has become glaringly obvious is that corporate IT employees are not equipped to handle the unique threats posed by cybercriminals on their own. As Wallace says, 'It's difficult to maintain your expertise unless you are seeing it in company after company. This is a specialist subject.' Orffer concurs, adding, 'This is not just an IT problem – this is a risk that businesses need to be aware of.' ■