



Australia & New Zealand

Social engineering: Deceiving people, not machines

The weakest part of any business computer system is almost always the human being using it – something cyber criminals know only too well.

Social engineering is extremely pervasive and frequently effective

Security experts easily convinced workers to reveal their passwords in exchange for a free pen.

Over half the computer users questioned in a recent AVG survey had received phishing emails.

Cyber criminals are often portrayed as technical geniuses plying their trade through the use of deviously complex computer code. While there is some truth to this, gaining access to a computer can be as simple as fooling someone into revealing a password. This tactic of exploiting the "human aspect" of computer use is known as "social engineering" and is widely recognised as one of the most effective techniques used by cyber criminals.

"Human beings are often the weakest link in the security chain," warns the US government advice site Stay Safe Online. "Criminals and con artists know this and exploit it. Learn how to spot the tricks they use."

Its Easy to be Fooled

Things to look out for include such simple tactics as phoning a random extension and tricking whoever answers into revealing their network password by asking seemingly-innocuous questions. "If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organisation and rely on the information from the first source to add to his or her credibility," warns US government security agency US-CERT.

A fraudster used this technique to make calls to the Barclays Bank in the UK, eventually convincing a call centre worker to issue a credit card in the chairmans name. Armed with the credit card and personal details about the chairman, the conman then went to a Barclays branch and withdrew 10,000 of the banking executives money. Ouch!

An example of how easily people can be tricked by social engineering was revealed by the organisers of the InfoSecurity Europe conference. Experts convinced 90 percent of workers stopped at Waterloo Station in London to reveal their passwords in exchange for a free pen. Some more suspicious workers refused at first, but eventually revealed enough information for the experts to accurately guess their password. Kevin Mitnick, one of the most notorious hackers of all time, has admitted that social engineering was a fundamental part of his approach. "When the average person conjures up the picture of a computer hacker, what usually comes to mind is the uncomplimentary image of a lonely, introverted nerd whose best friend is his computer and who has difficulty carrying on a conversation, except by instant messaging," Mitnick explains in his book *The Art of Deception*. "The social engineer, who often has hacker skills, also has people skills at the opposite end of the spectrum well-developed abilities to use and manipulate people that allow him to talk his way into getting information in ways you would never have believed possible." Beware the Phishers

But social engineering doesn't have to be done in person or over the phone. One of the most popular social engineering techniques is phishing, which is when cyber criminals bombard computer users with emails purporting to be from banks or other trusted entities where valuable information is protected by passwords.

Recipients are encouraged to respond to the mail by clicking a seemingly-legitimate link and entering their login credentials. "An attacker may send email that appears to come from a reputable credit card company or financial institution and that requests account information, often suggesting that there is a problem," explains advice on the US-CERT web site. "When users respond with the requested information, attackers can use it to gain access to the accounts." Recent research conducted by AVG revealed that around 55 percent of the 250 users surveyed had received phishing emails. The survey particularly looked at how increased use of social networking sites such as Facebook, Twitter and MySpace were contributing to the growth of phishing and other security threats.

Other interesting results included:

21% accept contact from members they dont recognise

52% let friends access social networks on their machine

64% click on links offered by community members

26% share files within social networks

20% have experienced identity theft

47% have been victims of malware infections

The emergence of social networking sites has led to a blending of programming-type hacking techniques with social engineering, a threat acknowledged by AVG back in 2007.

"The anti-virus industry has been in a transition period for the past two to three years as malware has morphed from simple viruses to complex malicious web site hacks that combine exploits and social engineering to scam unsuspecting users of their data," said Lloyd Borrett, Marketing Manager, AVG (AU/NZ). Education is Key

When it comes to protecting against social engineering attacks, technologies such as those provided by AVGs Internet Security software have an important part to play, but experts agree that educating staff is fundamental.

"An educated workforce is the main line of defence against online threats in business," is the advice from the UK government-backed Get Safe Online campaign.

US-CERT is more specific in its guidance: "Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organisation, try to verify his or her identity directly with the company."

The best strategy for businesses is to instil in their staff the notion that handing over any information to someone whose motives are suspect or unknown is not a good idea. This "paranoid" attitude should be brought home to new hires from day one; new employees are the most susceptible to social engineering techniques, according to Kevin Mitnick. "New employees are a ripe target for attackers. They don't know many of the people yet, they don't know the procedures or the dos and don'ts of the company. And, in the name of making a good first impression, they're eager to show how cooperative and quick to respond they can be," he warns.

Of course, it always makes sense to back up education with protection, so businesses should also ensure they have up-to-date security software in place. AVGs Anti-Virus and Internet Security products include AVG LinkScanner, a technology that can quickly and accurately determine whether or not a web page is hosting a phishing attack.

Criminals will always be able to find the chinks in any company's computer security armour but, by paying attention to the people as well as the computers, businesses can make it much harder for the cyber criminals to break through.

Online references:

Stay Safe Online US National Cyber Security Alliance: <http://www.staysafeonline.org/>

US-CERT United States Computer Emergency Readiness Team: <http://www.us-cert.gov/>

Barclays chairman loses 10,000 in identity scam: <http://business.timesonline.co.uk/tol/business/law/article3164914.ece>

Office workers give away passwords for a cheap pen: http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

The Art of Deception by Kevin Mitnick: http://en.wikipedia.org/wiki/The_Art_of_Deception

Get Safe Online - UK: <http://www.getsafeonline.org/>

About AVG (AU/NZ) Pty Ltd www.avg.com.au

Based in Melbourne, AVG (AU/NZ) Pty Ltd distributes the AVG range of Anti-Virus and Internet Security products in Australia, New Zealand and the South Pacific. AVG software solutions provide complete real-time protection against the malware, viruses, spam, spyware, adware, worms, Trojans, phishing and exploits used by cyber-criminals, hackers, scammers and identity thieves. AVG protects everything important and personal inside computers documents, account details and passwords, music, photos and more all while allowing users to work, bank, shop and play games online in safety. AVG provides outstanding technical solutions and exceptional value for consumers, small to medium business and enterprise clients. AVG delivers always-on, always up-to-date protection across desktop, and notebook PCs, plus file and e-mail servers in the home and at work in SMBs, corporations, government agencies and educational institutions.

AVG products actively protect over 110 million users worldwide, including more than 4.6 million users in Australia and New Zealand.

AVG (AU/NZ) has more than 2700 resellers across Australia, New Zealand and the South Pacific.

For more detailed information please contact:

Lloyd Borrett AVG (AU/NZ) 03 9581 0807

Shuna Boyd BoydPR 02 9418 8100

Media resources, including logos, box shots, screen shots etc., are available online at: <http://www.avg.com.au/media/>