Small Business Security Guides

Social engineering: Hacking people, not machines

AVG | AT WORK

Social engineering:
Hacking people, not machines

The weakest part of any computer system is almost always the human being using it - something hackers 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 http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/
- Over half the computer users questioned in a recent AVG survey had received phishing emails

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

It's 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 organization and rely on the information from the first source to add to his or her credibility," warns US government security agency US-CERT.

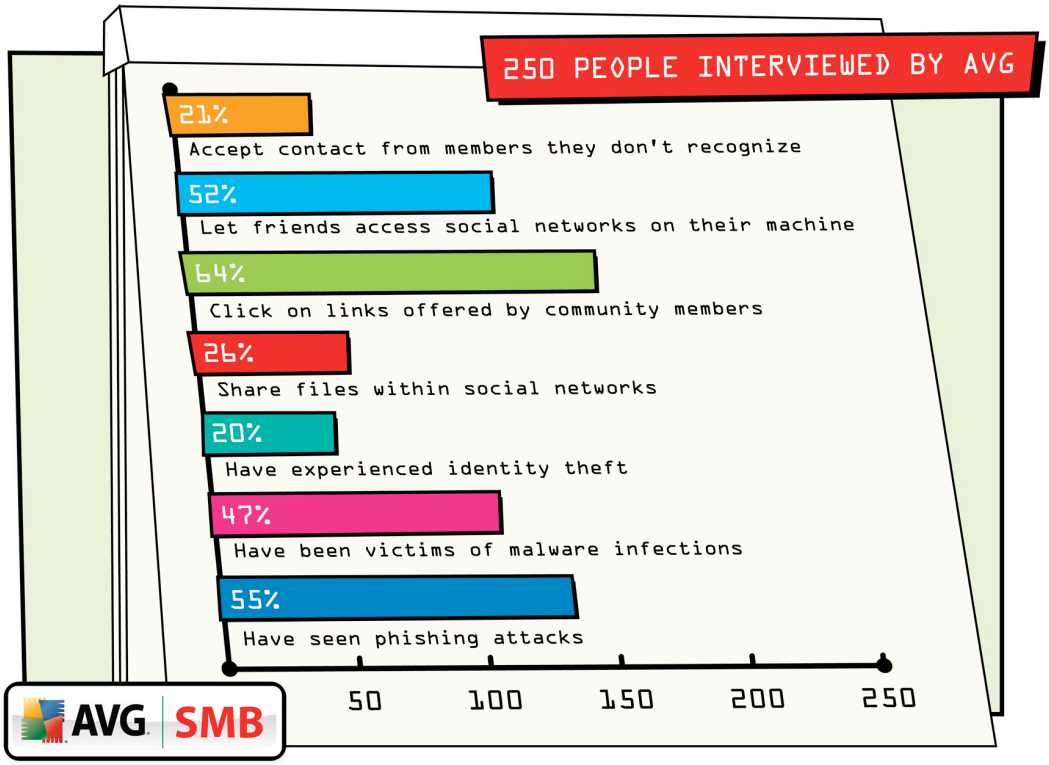
An example of how easily people can be tricked by social engineering was revealed recently by the organisers of the InfoSecurity Europe conference. Experts convinced 90 percent of workers stopped at Waterloo Station in London to reveal their passwords in exchange for a free pen. Some more suspicious workers refused at first but eventually revealed enough information for the experts to accurately guess 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 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 website. "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. "

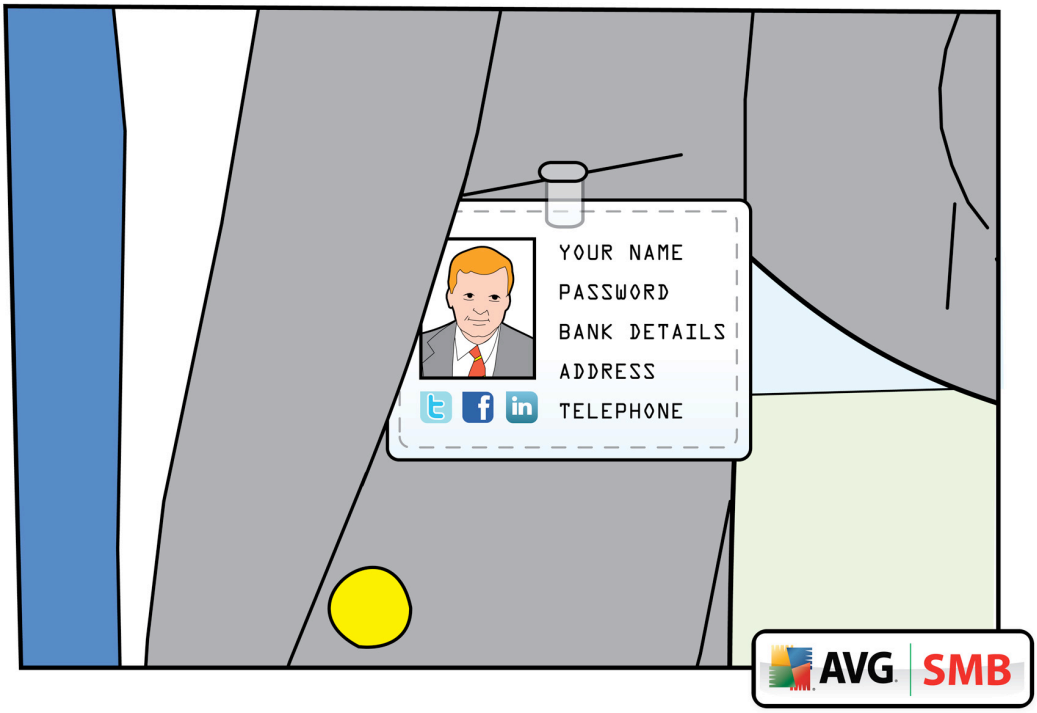


The emergence of social networking sites has led to a blending of programming-type hacking techniques with social engineering, a threat acknowledged by AVG back in 2007. “The anti-virus industry has been in a transition period the past two to three years as malware has morphed from simple viruses to complex malicious website hacks that combine exploits and social engineering to scam unsuspecting users of their data,” said AVG Technologies’ Global Security Strategist Larry Bridwell.

Education is key

When it comes to protecting against social engineering attacks, technology such as AVG’s has 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 GetSafeOnline 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 organization, try to verify his or her identity directly with the company."

The best strategy for businesses is to instill 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. AVG 9.0 includes 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 hackers to break through.

AVG SMB group at:
http://bit.ly/avglinkedin

Become an AVG Fan at:
facebook.com/avgfree

Read our blogs at:
blogs.avg.com

Follow us at:
twitter.com/
officialAVGnews

Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/
officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

AVG | AT WORK