

Social engineering takes many forms: physical access to buildings, phishing, telephone calls and so on. As Dorothy Denning, author of Information Warfare and Security said, "Any medium that provides one-to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar."

I may call the organisation's help desk pretending to be an employee who has forgotten their password. Help desk staff will frequently assist this helpless, non-technical caller to log on remotely and reset their password for them, without ever verifying their identity. Our testing shows that this is a common problem at most organisations in all business sectors.

Another technique involves visiting the premises in person. As a bogus employee or visitor, it is simple to look for information lying on desks, overhear conversations or even just use a vacant desk & PC. In one case, I was able to gain access through the building's back door, walk around every floor without challenge, read personnel information and customer contracts in unlocked cabinets, steal the contents of post trays and obtain a staff list containing names, job titles, e-mail addresses and phone numbers.

Alternatively, I can be an office cleaner. I wander around the IT department, looking under each desk for stray sandwich wrappers and plastic cups. Whilst I'm under the desk, it is a matter of seconds for me to attach a hardware keylogger between keyboard and system unit. These small keyloggers are effectively invisible on the back of the computer, and record every keystroke the IT folk make. They will capture usernames and passwords, as well as every e-mail and browser entry until I return to remove the keylogger in the same way. Of course there are plenty of similar opportunities throughout the organisation - the CEO's secretary's PC for instance, or the Finance Director's. Most organisations are vulnerable to this type of attack and will never know that it has taken place. The truth is that virtually no one conducts proper staff vetting, and they certainly don't check the cleaner's credentials!

Removing and studying the contents of bins marked "For Shredding" or "For Recycling" proves very interesting too, as a source for passwords, network diagrams and personnel information. Shoulder surfing - looking over someone's shoulder to see door entry codes, their password, information on their screen or what they are writing - is also extremely rewarding. Sometimes the simplest techniques are the most successful and often do not involve any technology at all.

Mail attachments, web links and "discarded" USB sticks remain very popular amongst social engineers, enticing users to click to gain access to something appealing or illicit whilst silently installing Trojan software on their computer. Once installed, this software can capture every keystroke and mouse click, and even take screen shots, then quietly mail everything to the attacker.

In one recent project, we crafted an e-mail with a link to a web page purporting to be a survey on information security hosted by our customer. We used graphics and links from the genuine corporate web site on our own server to ensure the pages looked realistic. Using simple web forms, we harvested user names and passwords, as well as valuable information about the organisation's security procedures and mailed the results to our own e-mail server.

When members of staff are travelling, unattended laptops can also be infected without any obvious evidence of intrusion, or data may be stolen and later used to compromise the office network.

Inside the mind of a social engineer - 23/07/2010

Peter Wood is CEO at First Base Technologies, an ethical hacking firm based in the UK, and a member of the ISACA conference committee. Peter founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as social engineering, network penetration testing and skills transfer. Peter is also a world-renowned speaker and security evangelist.

Peter Wood
peterw@firstbase.co.uk
www.firstbase.co.uk
www.white-hats.co.uk
www.peterwood.com