



Factsheet 19 – Social engineering – what is it and how it can be used for fraudulent purposes

The purpose of this factsheet is to explain what social engineering is and how it can affect online users.

Social engineering refers to tricking or scamming people for fraudulent purposes.

Social engineering techniques are used by cyber criminals in order to trick people into performing actions which have an adverse impact for them. The potential adverse impacts vary but include any of the following:

1. Harms the security of their computers, for example by fooling people to click on web links or email attachments that install malware on their computer;
 - The installation of the malware is, in turn, generally harmful to the interests of the computer users as it is often used to steal a range of personal information, passwords and other useful information for financial fraud.
2. Seeks to gain access to their online accounts by tricking users into disclosing their usernames and passwords, usually by pretending to be a trusted party.
 - These accounts could be for personal use such as online bank accounts, email accounts, ISP access accounts, e-health records accounts, or social networking accounts, eBay or PayPal accounts; or they could be for business use such as online bank accounts, tax file agent accounts, staff accounts which include personal bank account information, domain name registrar accounts, web-hosting accounts, etc.
3. Seeks to steal money from people by fooling them into providing personal identifying information or financial information such as credit card details, bank account details or tax file numbers for the purposes of financial fraud.
4. Fooling people into sending money directly to the criminal under false pretences.

The aim of such trickery is to get a potential victim to do something which benefits the criminal at the victim's expense. Social engineering doesn't have to involve computers or online communications but it often does.



Examples of social engineering

Nigerian or 419 scams

In these cases, the criminals tend to contact potential victims by spam email, but they might just as easily do so via a telephone call, a fax or a letter. The aim of a 419 scam is to get the victim to send money to the criminal under some false pretext. There is no limitation to the potential number of fraudulent stories a criminal may devise. The victim may, for example, think they are sending money to a charity, or to a prospective romantic interest who needs money for travel to visit the victim, or think they are investing in a lucrative business deal overseas, or they may think they are helping out a friend who appears to be in trouble, such as was the case in a scam used to trick the friends of an Australian business woman, which we wrote about in the [May SSO Newsletter](#).

The government's Scam Watch (www.scamwatch.gov.au) web site provides more detailed information about [Nigerian or 419 scams](#).

Phishing scams

Phishing scams are similar, except the criminal pretends to be a well known organisation or institution. For Australians, the phishing emails and web sites pretend to be from organisations you know, such as your bank, your ISP, the Australian Tax Office, Centrelink or other large organisations (such as a university).

Sometimes other well-known "online" brands may be the target of phishing as well such as social networking sites such as Twitter, MySpace, and e-commerce sites such as eBay and PayPal, or web based email accounts such as Hotmail, Yahoo and Gmail. **Where ever it is possible for an online criminal to obtain other people's usernames and passwords, it also provides an opportunity for phishing.**

Cyber criminals using phishing techniques usually send out an email that impersonates a legitimate organisation with a web link to a web site which also impersonates the same organisation. Sometimes the phishing emails may request the information requested via email, rather than to submit the details to a web site; or use an SMS rather than an email as the initial hook.

Combining social engineering with malware

Criminals often use social engineering to trick you into installing malware on your computer without your knowledge. Criminals may trick you into installing the malware by getting you to click on a web link in an email or watching a video online,



or claiming your computer is infected with malware and offer free software to install to fix the problem. Any topic which might arouse your curiosity or personal interest could be used to entice you to take an action which could result in malware being installed on your computer.

Once the malware is installed, criminals have the potential to gain control of your computer and all personal information on it, which the user can access online, over the Internet, via their computer. Once the computer is compromised with this malware, the criminal is able to harvest the information from the computer or use the computer as a resource with the Internet connection to conduct other criminal activities, with a high degree of impunity.

What you can do

The key is to be critical of everything you read online. Do not automatically believe and trust the claims made, including from within email which was sent, or appears to be sent, by people you know. Question whether the sender is really who they claim to be. Question whether the web link or email attachment is really what the sender claims it is – or whether perhaps it is just a ruse to steal your information or attack your computer for criminal purposes?

Further reading

Read the factsheet, [Protecting yourself against phishing attacks](#) and [Understanding digital certificates and how they can help build trust online](#), for tips to help you better detect and avoid becoming a victim of a phishing attack.

Report prepared August 2009