

Crime prevention advice for Social Engineering



The phrase 'social engineering' is quite a new term in the world of cybercrime but it is something that has been around for decades. It involves playing on the good will of individuals in a process of manipulation and deceit.

What is Social Engineering?

Social engineering is the process of deceiving someone to gain access to personal information or private systems. Criminals will use social engineering because it is often easier and quicker to play on someone's trust than spend endless hours attempting to hack computer systems, or they may use it to entice someone to click on a link containing a virus they have sent.

Forms of Social Engineering

Social engineering revolves around impersonation. This could be as a member of staff, potential supplier or simply enquiring as a member of the public.

Phishing - These are electronic communications, normally emails, which seek to obtain personal information.

Pretexting - This is where a fake scenario is provided in an attempt to gain trust.

Quid Pro Quo - The criminal will offer a service in return for information, e.g. IT support.

Baiting - This is done by leaving a memory stick or removable device around and waiting for curiosity to take over and for it to be plugged into a computer where it can infect all the computers on the network.

What can you do?

- Ensure all staff are aware of who to give information to and what can be shared via the likes of social media.
- Be wary of people who do not normally associate with the business incase they have damaging intentions.
- Secure all devices connected to the business with firewalls, anti-virus and spam filters to limit the chances and effects of being a victim.
- Do not respond to suspicious contacts

If you feel you may have been a victim, it is important to not be embarrassed about the situation and to act quickly. In your business, it would be important to inform the relevant parties and also change all passwords incase the criminal has also managed to access your systems.

