What is Social Engineering?

Social Engineering is the term used to describe a collection of cyber-fraud techniques increasingly employed to trick companies and individuals into handing over personal data, money and other assets. It manipulates, disrupts and deceives to gain illegal control over IT systems, personal computers, phones and tablets.

A social engineering campaign might identify one particularly valuable target, such as a large corporation, a multi-millionaire, celebrity and even you. This will gather as much specific information as possible about the target using data sources such as Companies House registrars, trade associations, sports and social clubs, schools, universities, social security numbers and social media.

Why should we worry?
The very targeted nature of social engineering means that the fraud it likely to be greater and more damaging. With so much data available online today, particularly personal data on social media, it is relatively easy to build a well targeted and convincing campaign to fool even the most vigilant person.

Some favourite Social Engineering Techniques

Pretexting
This one is becoming popular and usually applied when the target is already known. The intention of the cyber-criminal is to steal more information, possibly by posing as a known provider, to lure them into volunteering more personal information.

Delivery or Diversion Theft
This is found in delivery, postal and courier sectors where cyber-criminals target a delivery company to trick them into making the delivery somewhere else.

Phishing
One of the best known cyber-crime techniques where criminals seek to steal IT and computer user names, passwords, credit card details, usually via a phishing email appearing to come from a known and trusted provider, work colleague or personal friend. Bitcoin promotions, utility companies, HMRC and suppliers that each seem genuine and harmless enough are increasingly hi-jacked by hackers and fraudsters.

Spear Phishing
This is where a phishing campaign is a lot more specific and targeting a specific organisation or individual. A Spear Phishing campaign may take weeks or months of background research by the fraudsters to gather enough information to make their scam convincing enough to work.

Water-Holing
This technique takes advantage of Websites people regularly visit and trust. The attacker will again research the selected group of Web users to discover the sites they most regularly visit and seem to trust and then look for the vulnerabilities on those sites to plant exploit and other nasty code. It is then a matter of time before one or more of the target users becomes infected with malicious code or actually hacked.

Continued over →

Quid Pro Quo
You give me something and I will give you something. Typically, this will again be an email offering you a free shopping voucher, or BITCOIN sign-up screen and similar offers to encourage the user to click to accept or enter, where upon you download exploit code and your PC is infected. This is now happening on mobile phones.

Honeytrap
This is usually aimed at men where attractive women are promoted via an online dating site or similar to trick them into clicking a malicious Web link.

Rogue Virus Scans
Fake or Rogue anti-virus, anti-spam and anti-spyware have become frequent arrivals in email in-boxes in recent times, designed to trick us into downloading or running a fake scan which again infects our PCs with malware or hack exploit code.

Conclusion.
All these scams should be preventable if we all pay more attention to the way we use our office IT. Management need to set the rules of engagement and staff need to abide by them. Cyber security awareness training, whether online or in the classroom will help ensure your organisation's cyber security policies and office IT best practice guidance are understood and adhered to.

See the Action Fraud and YouTube Video
…a funny example of a Facebook scam
https://www.youtube.com/watch?v=yrjT8m0hcKU&t=4s