Social engineering

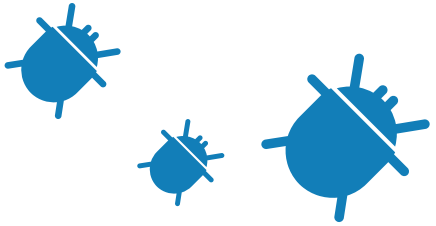
The threat of cyber fraud can seem difficult to combat, as the software used by fraudsters can be extremely complex. However, it is important to remember that most cyber fraud attacks depend heavily on human interactions – fraudsters have long identified that the easiest way to breach an organisation's defences is to target its people, not its systems.

Social engineering is the method by which fraudsters aim to trick people into breaking normal security procedures. Fraudsters are usually looking for the victim to give up sensitive information, such as bank login details, or for them to enable malicious software to be installed onto their device. They may also trick the victim into carrying out a fraudulent payment themselves.

Fraudsters in social engineering cases often have thorough knowledge of the company to enable them to build trust with the victim. They may be aware of regular payments that are due, or of the structure of teams within your company, enabling them to impersonate internal employees.

The most common forms of social engineering for business customers are:

- Invoice fraud
- CEO Impersonation Fraud
- Phishing
- Vishing
- Smishing.



[2] Mcafee, 2016. [3] gov.uk, 2016.