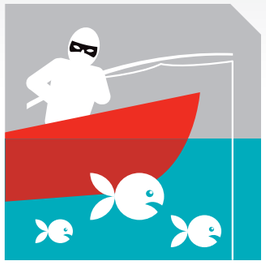
What is social engineering?

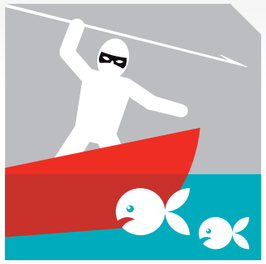
In cyber and information security, 'social engineering' is the use of deception to manipulate individuals into divulging confidential information or taking an action that may not be in their best interest.

Common techniques that you and your colleagues should be aware of:



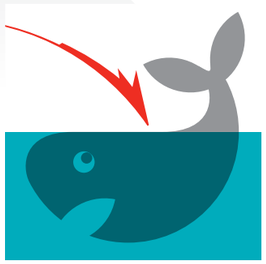
Phishing

The most prolific form of social engineering. The fraudulent attempt to steal personal or sensitive information by masquerading as a well-known or trusted contact. Email phishing is becoming increasingly sophisticated and attackers use techniques to make the email appear legitimate or to lure the victim into acting quickly. Attackers disguise the email address so that it appears to be from a well-known organization, such as a bank, utility company or government.



Spear phishing

Attackers limit the target audience and increase the precision of their messages. An attack may target individuals within a particular business sector, company, or department. A spear phishing email may even target one individual of value to the attacker. An attacker will research their target(s) in order to maximise their chances of success. They will find out information about the organization, and combine this with knowledge obtained from their victim's social media profiles and other publicly available information.



Whaling attack

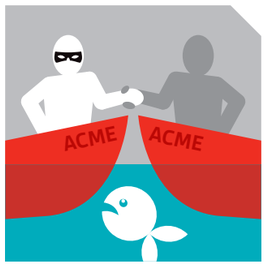
A sophisticated phishing attack used to steal confidential information, personal data, access credentials and specifically information of high value from an economic and commercial perspective. Whaling indicates that the target is a big fish to capture, and targets can be executives of private businesses or government agencies. A whaling email is designed to masquerade as 'critical' business email and sent from a legitimate authority, designed for upper management and reports some kind of fake highly confidential information.

Voice phishing (aka vishing)

Over the phone social engineering to obtain access to personal and financial information. The scammer may pretend they need certain information from the target to confirm their identity. This technique is typically used to steal credit card numbers or other information to be used in identity theft. Scammers may impersonate co-workers, bank officials, or an individual who the victim perceives as trusted or having authority.

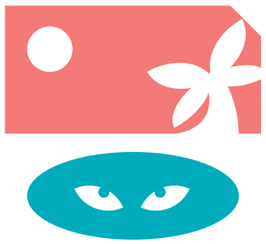
Smishing

SMS phishing, or smishing is the practice of sending text messages purporting to be from reputable companies, that encourage the victim to pay money out, share valuable information or click on suspicious links. A popular technique on personal devices.



Business Email Compromise (BEC)

Business email compromise (BEC), or email account compromise (EAC) exploits the fact that many of us rely on email to conduct business. A BEC scam will identify and research a target organization, send spear phishing emails or calls to a victim in that organization and convince them that they are conducting legitimate business transactions. This scam can be one of the most financially damaging attacks.

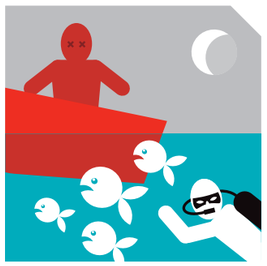


Watering hole attacks

The use of trusted websites to infect victim's computers. A watering hole attack works by compromising a trusted third-party website to deliver malicious code against the intended victim's computer. The attacker will research their victim and identify trusted websites that they are likely to access such as a supplier's website, an industry journal, or some other website of interest to the victim.

Quid pro quo

The offer of a service or benefit in exchange for information or access. Similar to baiting but instead of a promise of a thing, a quid pro quo attack promises a service or action-based benefit. Commonly, hackers impersonate an IT helpdesk or specialist for a large company. The attacker spam calls a number of direct employee numbers and when a victim is on the phone, the attacker offers assistance or software upgrades to their work machine. This often includes the attacker asking the victim to temporarily disable security features on their machine.

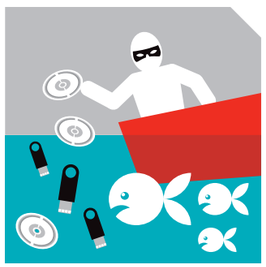


Diversion theft (aka 'round the corner')

A confidence trick exercised by professional thieves, normally against a transport or courier company. The scammer persuades the victim that a consignment should be received elsewhere – hence 'round the corner', the goods can then be easily stolen by the thieves. Diversion theft can also occur on the internet when attackers steal some confidential information by persuading a legitimate person to deliver or send that information to someone else who is associated with them.

Scareware

Involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.



Baiting (or physical baiting)

A wide scale attack through the use of online adverts and websites or physically seeding an area with throw away lures such as memory sticks. These usually have visual hooks or offers that are too good to be true or with an urgent warning. Curiosity will have the victim find out what the memory stick contains, or a website may allow a user to stream videos, before a pop-up 'detects a problem', which clicking a link will solve. In both cases users are tricked into giving away personal information, or their machine may automatically download malware.

Tailgating

The attacker's focus is to get physical access to a site or building with restricted or controlled access. The simplest way of doing this is by walking in behind a member of staff who has legitimate access, following common courtesy the staff member will usually hold the door open, or the attacker may even ask the employee to hold it open for them.

Your best defence techniques

Think before you click

If it sounds too good to be true, it usually is

Remember scammers will convey urgency in emails or through conversation to get you to act

Know your next move

Report suspicious activity to your IT department

If you click a link or download something malicious, notify your IT department immediately as it will have protocols in place to resolve or remove the issue

Security awareness and training

Provide regular training and reminders for your staff

Run phishing simulation campaigns for your employees

Need help keeping your organization secure?

Find out more

EMEA
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us