SBS INSIGHT HUB

SHARD Business Services

INTRODUCTION TO FRAUD ACTION - OVERVIEW

What is Social Engineering?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Spear phishing

Spear phishing is targeted at individuals, often starts with a face-to-face or social media encounter where the attacker builds up a level of trust, then follows up with an email.
It is reported that spear phishing attacks have a much higher success rate than standard phishing

Vishing/voice phishing

A form of targeted social engineering attack that uses the phone. Types of vishing attack include recorded messages telling recipients their bank accounts have been compromised. Victims are then prompted to enter their details via their phone's keypad, thereby giving access to their accounts.

Pretexting

Pretexting is when the attacker creates a convincing pretext for contacting you, often with a sense of urgency, to fool you into revealing confidential information. A common example is where the scammer pretends to be a caller from your IT department, who needs your login details to resolve an IT issue.

Baiting

A common feature of social engineering is the bait used to entice the victim to open an attachment or click on a link, for example, you're a winner, or important information – new travel guidance or even there is a problem with your account and that you must very some security information.
When the message appears to be from someone you know, or think you know, you are more likely to trust the message an act upon it.

Phishing Attacks

Phishing, like social engineering generally, is used because it is easier to exploit a human being's natural information to trust than it is to hack directly. Types of people who undertake these attacks are:

Criminal

Criminals, including hackers, who use phishing to obtain confidential information and use it for unlawful purposes

Hacktivists

Hacktivists may seek to embarrass an organisation or to make a political/ideological point

Insider

Insiders use their inside knowledge to gain access to information that its off limits.

Network Risks

- Hackers may sell on your personal or organisations personal and confidential information
- Criminals might see an opportunity to steal money or data from you or your organisation
- Blackmailers might offer to keep your personal and confidential data quiet, for a price

Malicious Code

Malicious code refers to any software programming code designed to cause damage or security breaches which could compromise your computer and network security and data

'An organisation has one month to respond to any complaints of inaccurate data, unless there are reasons to extend by up to another two months, in which case a reasonable explanation will be required.'

'The right to erasure is often known as the right to be forgotten. Under Article 17, data subjects can request that information be erased and ask that any further processing in specific situations be prevented.'

shardbusinessservices.co.uk
07714651415
office@shardbusinessservices.co.uk
shardbusinessservices
shardbusiness
@shardbusiness