Social Engineering – Fundamentals

This Loss Prevention Standard provides guidance on detecting and mitigating cybersecurity risks from manipulation and deception tactics aimed at exploiting human trust.

Version: 1.6
Date: 5th March 2026

Social Engineering – Fundamentals

Introduction

The concept of Social Engineering is nothing new. Threat actors continue to employ a variety of tactics to achieve their aims which include gaining unauthorised access to a network, obtaining sensitive information, stealing monies or stock, or installing malicious software on endpoints.

Whilst these end goals are to infiltrate, the methods which threat actors utilise are always evolving. Organisations, regardless of size, must familiarise themselves with the changing cybersecurity landscape and be able to adapt quickly to new threats as they emerge.

What does Social Engineering look like?

Social Engineering, as defined by the National Cyber Security Centre (NCSC), is where threat actors use "psychological manipulation to trick users into making security mistakes or giving away sensitive information."[1]

Mass Phishing Campaigns

Some Social Engineering attacks may be more generic in nature and target a wide audience. An example of this could be a wide-reaching phishing email campaign with no specific target. Said email may instruct the target to urgently reset their password, with links in the email leading to a decoy password reset page. If the target did enter any credentials on this page, it may be captured by the threat actor who in turn could use this to log into the target's legitimate account.

Phishing emails are not just limited to obtaining login credentials. An email could also advertise claiming a prize (baiting), with the link directing to a website which downloads malware. Another example of phishing could be where an individual receives a suspicious text message (smishing) about an undelivered parcel which they didn't order.

Targeted Social Engineering

Social Engineering campaigns may also be narrower in scope. Threat actors may look to target specific sectors, organisations or even individuals. In order to target more successfully, threat actors may use more complex techniques than simply sending a malicious link within a single email.

[1] https://www.ncsc.gov.uk/static-assets/documents/ECW21-HO-Cyber-Security-Social-Engineering-slides.pdf

Pretexting is where a threat actor attempts to establish a relationship with the target in preparation to launch an attack. By doing this, the target could be more likely to trust the threat actor should they eventually launch the actual attack.

Spear phishing is the term used when referring to phishing attempts targeted at specific individuals, such as those who work in an organisation's finance or IT functions.

The term whaling refers to targeting a person of high significance within an organisation, such as senior executives and board members.

Threat actors may also carry out vishing attacks, aiming to trick a target through a phone call. For example, a call to an IT helpdesk to trick staff into resetting user credentials to gain unauthorised access to an organisation's systems.

This targeting of an individual and the psychological manipulation that follows often leaves the target devastated to have unknowingly been party to the illegal activity.

Business Email Compromise

Business Email Compromise (BEC) is a targeted form of Social Engineering where a threat actor gains access to, or convincingly spoofs, a legitimate email account. This is often a senior executive, finance user or trusted supplier.

Using this account, the threat actor sends seemingly genuine messages instructing staff to change bank details, pay an urgent invoice or share sensitive information. Because the request appears to come from a trusted internal source, recipients may feel pressured to act quickly and bypass normal verification checks, leading to significant financial loss or data exposure.

Impersonation and Artificial Intelligence

The widespread adoption and availability of Artificial Intelligence (AI) tools have enabled threat actors to craft more convincing and complex social engineering attacks.

Traditional phishing attacks are often associated with malicious emails and links. The use of generative AI tools has allowed threat actors to create 'deepfake' videos claiming to be a specific person to convince a target that it is the real person. The same applies with AI creating voice messages which mimic the person's voice. As generative AI tools continue to advance, it is becoming increasingly challenging to establish whether recordings and images are authentic.

Beyond mimicking the likeness of people, AI can be used to generate bogus documentation in support of an attack. For example, government-issued documentation such as driving licences and passports, as well as fake invoices.

Homoglyphs

A homoglyph is a character that looks like another, even though it is not the same. Threat actors often use characters from different alphabets, such as swapping Cyrillic for Latin characters, so domain names and links look legitimate despite being not. Threat actors may also use a combination of letters to replace another, such as using 'rn' in place of 'm'.

Whilst this may seem an obvious difference when reading this document, consider how this could be mistaken when working at speed through emails, being under pressure or generally not being alert. Another example could be as simple as replacing the letter 'O' with the number '0' or using different fonts and spacing settings to alter the appearance of characters.

Homoglyphs can be used in domain names registered by a threat actor and used in phishing links for a more convincing attack. When not looking closely 'microsoft.com' (real) and 'rnicrosoft.com' (fake) could be confused.

In-Person

Whilst the term Social Engineering is perhaps most often linked to technologically facilitated attacks, it is important to remember that such attacks can occur in person. If an organisation has its own premises and physical infrastructure, physical security controls should be considered. Could somebody tailgate behind somebody into a building? Or is it possible for a threat actor to be able to gain access through a convincing story, such as them conducting an inspection, delivering a package or completing maintenance?

Social Engineering Statistics

- The Crime Survey by the Office of National Statistics (ONS) for England & Wales (ONS) recorded "**4.1** million fraud incidents, a 8% increase in the year ending September 2025" [Crime in England and Wales - Office for National Statistics].

- The NCA reports fraud accounts for "**41%** of all crime in England & Wales in the year ending Sept 2024" [nationalcr...ncy.gov.uk].

- UK Finance's 2025 Annual Fraud Report notes a rise in unauthorised fraud, driven significantly by social engineering tactics, with criminals using social engineering to obtain one-time passcodes enabling fraudulent transactions [ukfinance.org.uk].

- A summary of UK Finance reiterates "criminals are using social engineering to trick people into divulging one-time passcodes." [https://www.independent.co.uk/money/fraud-text-scam-claims-help-b2758979.html].

- FBI data reported in multiple sources shows "BEC/EAC scams resulted in over **$2.4** billion in losses in 2021, making BEC the most financially damaging cybercrime" [tanium.com], [fbi.gov].

- Social engineering breaches specifically add further cost and take longer to detect/contain [blog.knowbe4.com].

- In the UK, **374,000** fraud cases were reported to the National Fraud Database in 2023, with **£1.8bn** in losses prevented [cifas.org.uk].

What is the Objective of Social Engineering Attacks?

We have seen that Social Engineering encompasses a variety of techniques to facilitate an attack through bypassing technical controls and defences, but what is the end goal?

- **Credential Theft**. Threat actors try to make you type your password on a fake page. If they do, they can log in as you. Other accounts may be targeted with the same credentials, so a threat actor may be able to access more accounts if the username and password are the same.
- **Business Email Compromise**. The objective of social engineering in Business Email Compromise is to exploit human trust and authority to manipulate employees into performing unauthorised actions, such as transferring funds or disclosing sensitive information, by impersonating legitimate business contacts through convincing email communication or email spoofing.
- **Financial Gain**. By impersonating suppliers or managers, a threat actor may be able to convince executives or those involved in an organisation's financial affairs to transfer funds to an account controlled by the threat actor. Attachments within a phishing email could contain malware which if executed could launch a ransomware attack, with threat actors requesting payment to release the victim's data.
- **Data Exfiltration**. Social Engineering may be used to impersonate suppliers or other staff within an organisation. A threat actor may request for sensitive information to be shared. Malware could also be installed through phishing which enables threat actors to exfiltrate data through more technical means.

Mitigation Steps

There are several steps which can be implemented to mitigate the risk of social engineering attacks:

- **Multi-factor Authentication**. Mandating the use of multi-factor authentication (MFA) can provide a level or protection in the event of a user's login credentials being compromised. Even if the threat actor is in possession of the credentials, they will likely still need another factor of authentication to access the user's account. MFA should be enabled on all accounts where available, with factors such as hardware tokens (e.g. YubiKeys) and Time-Based One-Time Passwords (TOTP) being preferred over SMS text messages due to SMS being at risk of SIM Swapping attacks.
- **Use Different Passwords.** Users should be encouraged to avoid re-using the same password across multiple accounts. Should a threat actor obtain the user's password for a specific account, they will not be able to use the same password to log into a different account. Using unique passwords for each account therefore provides a level of compartmentation should credentials be compromised.
- **Password Managers**. The use of a reputable password manager can also support an organisation's effort to counter Social Engineering. These tools provide a way for users to securely store passwords, making it easier to use a unique password for each account. Some password managers also provide an auto-fill function, which automatically fills in login details such as a username and password into a site's login field. This functionality provides some protection against Social Engineering, as in order to function, the password manager must store the site's address. Should a user find their way to a phishing page which uses a different domain to that of the legitimate site, the password manager will not enter the login details as it does not match the site address stored within it.

- **Employee Training and Awareness.** It is advised that organisations provide regular employee training to increase the awareness of the workforce in spotting Social Engineering attacks. Organisations may wish to consider conducting phishing simulation exercises to monitor who is clicking on simulated emails and to provide further training and support to those who do. It is encouraged that IT managers share information concerning any increased attack activity involving the organisation itself or the business sector to enable employees to keep up to date as the threat landscape evolves.
- **Sign-off Process.** To counter the risk of payments being diverted to a threat actor in a Social Engineering attack, organisations should implement a sign-off process prior to sending payments. For example, requiring that a senior manager approve payments over a certain amount and provide a ‘second pair of eyes’. The Aviva Loss Prevention Standard Payee Verification Policy provides useful guidance in this regard.
- **Verification of Change Requests.** To ensure that requests are legitimate, a call back to a nominated representative of the organisation (taken from source contract details not the email request) should be undertaken prior to making any changes to bank accounts. The Aviva Loss Prevention Standard Payee Verification Policy provides useful guidance in this regard.
- **Strengthen Email and Communication Security**. Deploy anti-phishing & advanced email filtering as phishing remains the most common of all social engineering vectors. Organisations could implement external sender tagging, helping staff instantly identify impersonation attempts. Organisations should ensure their Domain Name System (DNS) records are correctly configured with DMARC, DKIM and SPF to mitigate against unauthorised senders being able to successfully spoof and send emails from their domain name. This is critical because Business Email Compromise (BEC) relies heavily on email impersonation**.**
- **Report Fraud.** Fraud can be reported to the City of London Police (national policing lead for economic crime who work in partnership with other law enforcement agencies. UK's Home for Reporting Cyber Crime & Fraud - Report Fraud

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

- Cyber Security Awareness Training - **Phishing Tackle**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Cyber Security Centre: https://www.ncsc.gov.uk/
- Report Fraud: https://www.reportfraud.police.uk/
- National Crime Agency: https://www.nationalcrimeagency.gov.uk/

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks**
- **Cyber Security: Respond and Recover**
- **Cyber Security: The Internet of Things**
- **Ransomware - Cyber Loss Prevention Standard**
- **Cyber Essentials - Accreditation**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

5th March 2026

Version 1.6

ARMSGI1212024

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.