BE SAVVY ABOUT THE SOCIAL ENGINEER:

your guide to what social engineering is and how to protect yourself

CPNI
Centre for the Protection of National Infrastructure

DISCLAIMER

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

WHAT IS SOCIAL ENGINEERING?

Social engineering is the process of obtaining information from others under false pretences – in essence, manipulation. It is based upon the building of an inappropiate trust relationship with individuals, and can be used against those within an organisation. For example, it could be an attempt to gain entry to a site, or an attempt to access an organisation's IT systems using a bogus pretext.

A social engineer might choose to manipulate an instant rapport they've built with that employee, or build a longer-term relationship with them. They will establish a level of trust so that the staff member feels comfortable to disclose information or grant the social engineer access without a second thought.

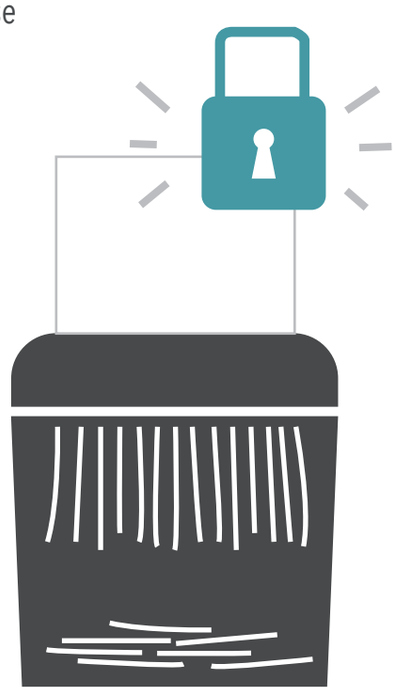
The important point about social engineering is that your organisation might well have sophisticated firewalls, good password protection and robust entry procedures, **but without a good understanding of how you may be exploited by a social engineer your workforce remain vulnerable to the threat.**

This guide will help you to understand the kinds of threats that you may face from social engineering,what these threats might look like and what you can do to help protect yourself and your organisation.

WHERE MIGHT THE THREAT COME FROM?

Those engaged in social engineering might include:

- **Protest groups –** looking for information or practices that validate their cause
- **Criminals –** seeking to steal information or materials
- **Commercial competitors –** seeking information on products or contracts
- **Terrorist cells –** after information they can use to target someone or something
- **Foreign Intelligence Services –** interested in obtaining information from UK sources to advance their own military, technological, political and economic programmes



WHO MIGHT BE VULNERABLE?

All employees are vulnerable to social engineering, but there are certain groups of staff that may be more vulnerable than others. For example:

- **Production workers**
- **Administrative staff**
- **Sales and marketing professionals**
- **Junior/inexperienced staff**

WHY?
Because they regularly deal with a wealth of organisational information that would not necessarily be thought of as 'sensitive'. However, the value of this information can often be underestimated.

- **Receptionists**
- **Personal assistants**
- **Customer service representatives**
- **Security officers**

WHY?
Because they are under instruction to assist outsiders and to ensure they portray a customer-focused and cooperative company image. They are encouraged to be helpful when someone requests information and that is a trait that can be exploited.

A social engineer might try to target individuals who:

- Feel they do not receive proper recognition for their work
- Gossip and discuss things of no direct concern
- Have a desire to show off their expertise to peers
- Are indiscreet about their work, or share sensitive information

HOW MIGHT SOMEONE BE TARGETED?

An important point to remember is that the social engineer is unlikely to ask a direct question – e.g. 'What's the access code?' Rather, they'll ask small, seemingly innocuous questions, picking up little bits of information (e.g. 'Are the access codes changed often?' 'Which team is responsible for the access codes?'), cues and signals from staff who maybe don't realise the value of that information.

Key to combatting social engineering is to recognise when it's happening. Sometimes that's quite easy to spot; other times, not so much.

THIS MIGHT HAPPEN:

- **In person** – a social engineer may target specific employees at a networking event, showing an excessive interest and knowledge in their work
- **Through corporate communications** – employees are susceptible to being targeted by social engineers through their phones or IT devices, where they might be vulnerable to phishing emails, attachments containing malware or bogus phone calls
- **Social networks** – online activity is particularly vulnerable and employees must be mindful of being targeted by social engineers on social media sites, both professional networking or personal sites

The social engineer may also manipulate an employee's desire to be helpful, or exploit that non-savvy use of the internet (for instance, the employee might be the type that regularly opens email attachments without checking where they're from).

The social engineer might use information provided by individuals known to the employee on social media, or readily available organisational information (like on the website, in the 'About Us' section) to give the illusion that they have insider knowledge and are therefore trustworthy.

Outlined below are a few examples of scenarios to illustrate how a social engineer might target someone. Remember, with social engineering you often don't know it's happening. However, if you are mindful of the threat, and stick to your organisation's security policies and procedures, you'll put yourself in the best position to avoid being exploited.

SOCIAL ENGINEERING TO GAIN ACCESS THROUGH A SECURE ENTRY POINT

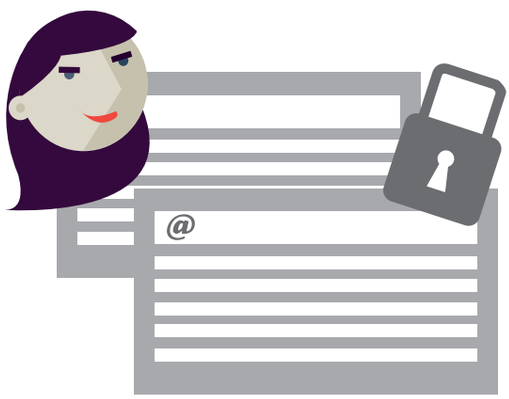
A person claiming to be a delivery driver approaches the security guard at the entry point. They tell the security guard that they 'have an important delivery', have 'lost the paperwork' and will 'get in trouble with the boss' if they don't make the drop. As it's a plausible story and they do seem to know the name of the organisation's Facilities Manager the security guard lets them in, even though it goes against the organisation's procedures.

SOCIAL ENGINEERING FOR IT SYSTEMS ACCESS

A person claiming to be from 'IT support' approaches the receptionist at the front desk. They say they've just been drafted in to 'update a few things in the system back-end'. They're not on the visitors list but seem to know the IT Manager's name, location of the server room and ask whether the receptionist can give them access. Despite the organisation having the most sophisticated firewalls and password protection system, a very feasible story like this can be enough to grant someone with malicious intent access to the organisation's IT systems.

SOCIAL ENGINEERING TO OBTAIN SENSITIVE MATERIAL

A commercial competitor develops a friendly relationship with an employee that has access to sensitive materials. They learn beforehand about the organisation and the way its employees typically behave. They regularly pay for meals and drinks with the employee, cementing an even friendlier relationship by buying them thoughtful gifts for their or their family's birthdays or special occasions. The competitor cultivates this association on increasing levels of trust, gaining access to incrementally more sensitive information.



WHAT TYPES OF ATTACK ARE THERE?

Social engineering attacks can be either dispersed or direct:

- **Dispersed attacks** – also known as 'mosaic attacks', these involve one or more people gathering small bits of information from various staff members over a period of time. Seemingly innocuous, innocent conversations reveal pieces of information that might not seem significant on their own, but can be valuable when piecing a bigger picture together.

- **Directed attacks** – generally these are directed towards a specific individual with access to valuable information. These attacks involve building a sustained relationship with the person: maybe they meet the social engineer at a conference, the social engineer spends some time befriending that employee before asking for access to non-sensitive documents that are easy to obtain. Gradually, the social engineer asks for small favours, in return for reward, and will incrementally ask for more valuable information, perhaps using subtle coercion tactics.

Bear in mind also that these types of attacks aren't mutually exclusive; for example, a social engineer might use a dispersed attack in order to gain access to the employee on whom they wish to use a directed attack.

WHAT MIGHT A SOCIAL ENGINEER ASK ABOUT?

The social engineer is typically well prepared. They learn about the organisation and the way its employees typically behave beforehand. They may pose as a trustworthy newcomer – say a new starter, a delivery driver, an external engineer that doesn't know the ropes yet, or maybe just a particularly friendly stranger – creating a plausible context to legitimately ask for help.

THE SOCIAL ENGINEER MIGHT ASK YOU TO:

- Provide information on colleagues, the systems you work on, your projects or your organisation's equipment

- Influence or bypass certain organisational policies

- Grant access to certain systems or materials

WHAT SORT OF DAMAGE CAN BE DONE?

IF SOCIAL ENGINEERING IS SUCCESSFUL, IT COULD:

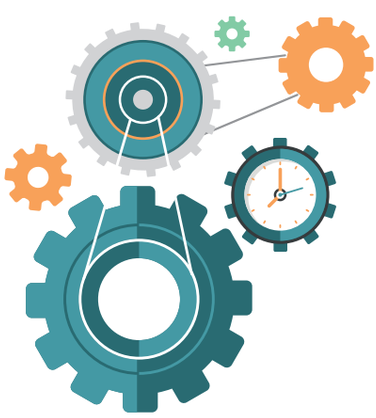
- Compromise your safety
- Compromise the safety of your colleagues
- Compromise the safety of the public
- Compromise the safety of your workplace
- Jeopardise a negotiating position
- Give a competitor a commercial edge
- Damage reputations – either an individual's or a whole organisation's

HOW DO WE PROTECT OURSELVES?

Your biggest weapon is simple common sense and actually knowing how much 'too much information' is.

The purpose of this pack is to help you recognise the common signals and threats, and give simple, practical advice to deal with them.

It's important for employees to remember that social engineers go after the individual, not the organisation – the company might be organisationally very secure, but it's the vulnerability of one human element that is usually exploited.



Follow these four steps to help you minimise the risk of being exploited by a social engineer:

1. **Understand the threat –** by familiarising yourself with the social engineering approaches and threats described in this pack, you'll be able to better prepare and protect yourself.

2. **Do an online search of yourself –** and see first hand what your digital footprint looks like. Is there information online about you that would draw a social engineer's attention to you and make you look like an attractive target? Do you need this information to be online?

3. **Keep relationships professional –** because it's better to be safe than sorry. Social engineering is most effective when your guard is down, so always think carefully about with whom you're speaking and what you're talking about. For example, always verify if they're a collaborating organisation, supplier or customer, and don't be afraid to double check with others.

4. **Communicate securely –** and ensure you stick to your organisation's policies regarding communications and sharing sensitive, work-related information. Try also to minimise the link between work and home on social media.

For more information or guidance on protecting against the social engineering threat, please visit your organisation's intranet or speak to your organisation's security team.

To test your knowledge and understanding of the threats based on the information in this guide, we have a short quiz that you can complete. Turn over to the next page and see how many of the five questions you can get right.

BE SAVVY ABOUT THE SOCIAL ENGINEER: THE SOCIAL ENGINEERING QUIZ

Social engineering can happen at any time, even outside of work, and sometimes it's hard to know what to look out for. You've heard all about the situations and scenarios in which social engineering can occur. Now it's time to test that knowledge!

QUESTIONS

1. What does the term 'social engineering' mean?

a) It's when a criminal tries to break into the office building when no one's around.
b) It's when someone tries to obtain information from others under false pretences.
c) It's when a competitor starts a social media campaign that obviously copies yours.
d) It's when someone from outside delivers a package to the wrong department.

2. Which of these employees is vulnerable to social engineering?

a) CEO
b) IT assistant
c) Receptionist
d) HR professional
e) All of the above

3. Which of these could be a social engineer?

a) The unexpected visitor at reception asking for access to your building.
b) The email from someone you're not familiar with asking you to click on a link.
c) The telephone call from someone who says they work in your office (who you've not come across before) asking for personal details about a colleague.
d) The friendly stranger in a café who moves the conversation onto questions about a sensitive project at your workplace.
e) All of the above.

4. Why would a person use social engineering tactics?

a) To gain classified commercial intelligence on your product pipeline.
b) To find out security information that will help them to launch a physical attack on your office that would harm employees.
c) To gain information that would further the agenda of a foreign government.
d) To test the effectiveness of your computer system firewalls so they can launch a cyber-attack.
e) All of the above.

5. In social engineering terms, what does a dispersed attack involve?

a) The sustained 'grooming' of one key employee using flattery, gifts and rewards to extract classified information.
b) Use of coercion tactics, such as the presumption of urgency, to get an employee to let a social engineer pass a point of entry.
c) Coercing several employees to reveal small, seemingly innocuous pieces of information that build a picture of the organisation of significantly higher value.
d) A physical attack on the company building from multiple angles.

ANSWERS

1. Answer = b)

The term 'social engineering' refers to when someone tries to obtain information from others under false pretences – in essence, manipulation. It is based upon the building of an inappropriate trust relationship with an employee that can be used against those in the organisation.

2. Answer = e)

All of the above – anyone can be vulnerable to social engineering, although customer-facing roles, such as receptionists, can be particularly attractive as targets.

3. Answer = e)

All of the above – any one of these scenarios could be an example of social engineering, resulting in you unknowingly being manipulated into sharing information or giving access to an individual who has no legitimate reason. Be aware of the threat and take sensible precautions to help minimise you and your organisation's vulnerabilities.

4. Answer = e)
All of the above – social engineering tactics can be used for a variety of reasons by those wishing to cause harm to your organisation, your community and/or the wider public.

5. Answer = c)

A dispersed attack is coercing several employees to reveal small, seemingly innocuous pieces of information that build a picture of the organisation of significantly higher value.

BE SAVVY ABOUT THE SOCIAL ENGINEER:

YOUR GUIDE TO WHAT SOCIAL ENGINEERING IS AND HOW TO PROTECT YOURSELF

CPNI
Centre for the Protection of National Infrastructure