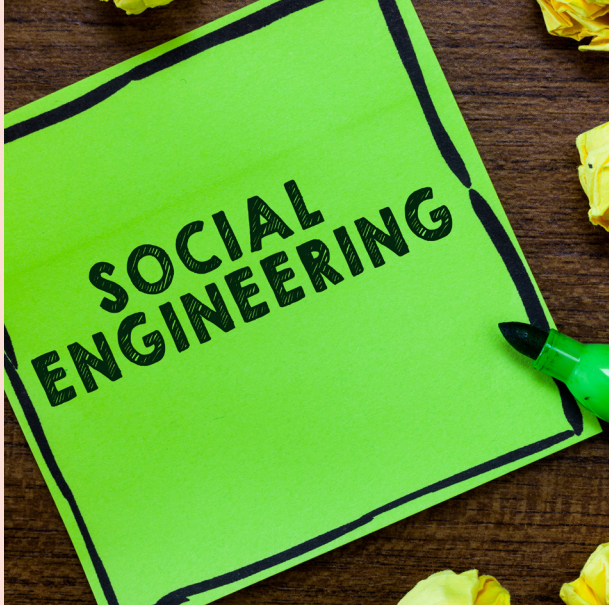
Tip sheet

SOCIAL ENGINEERING ATTACKS

Often used as reconnaissance, social engineering is also a means of espionage used to obtain crucial information by exploiting human error, trust, gullibility or ignorance. Regardless of whether conducted for profit or used to access systems or information considered relevant, social engineering may only be the first step in enabling a fraudster to launch targeted and personalised cyber attacks.



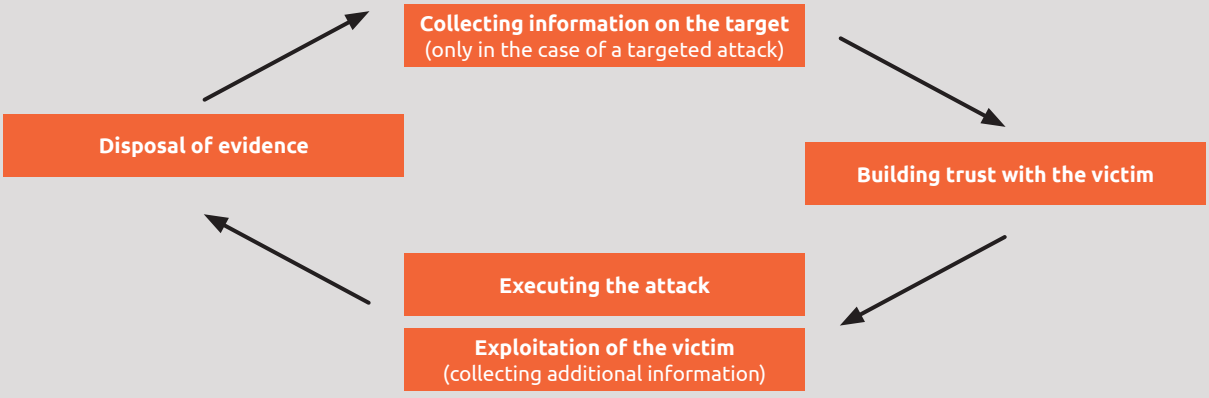
The art of manipulation, lying and deceit

Social engineering has existed since time immemorial. Arsène Lupin, the master spy, for example, used psychological tricks and deception (misdirection) to steal valuable objects. More generally speaking, magicians tricked, and continue to trick, their audience with slick illusions to prove that magic really does exist.

Social engineering also involves a fraudster's skills of manipulation and lying to persuade the victim that they are genuine, thereby gaining the victim's trust. In addition to manipulating communication, it involves psychological effects such as body language and tone of voice.

Social engineering attacks exploit a weakness in human cognitive functions, particularly by using processes of influence, manipulation, enticement and pretence. In terms of IT, examples of these attacks are attempts at phishing, voice phishing or vishing, and even pretexting, to name but a few. They can prove to be just as accurate as conventional hacking, even though the fraudster conducting the attack may have less technical knowledge.

Life cycle of a social engineering attack



restena
réseau · sécurité · .lu

Main techniques for collecting information

Searching through rubbish

Bins and waste containers may contain some real treasures: architectural drawings, confidential documents which were not destroyed, post-its with important information scribbled on them.

Search for poorly protected access

Poorly protected buildings, and doors which have not been locked or closed properly provide easy access... just like holding the door open for someone you don't know when entering a building or area with restricted access, particularly by means of a badge reader.

Manipulating people

Media (social media, business directories, websites, etc.) provide a wealth of information about companies and their employees. Once in possession of this data, attackers will use it to make themselves seem credible to their victims or to extract even more specific information from their contacts.

Main attack scenarios

Thanks to the information collected, fraudsters are able to launch multiple attack scenarios, which are not just limited to using software tools.

Did you know?

84% of cyber attacks originate from social engineering*

(Voice) phishing (vishing)

By means of a written message or telephone call, attackers try to obtain a victim's private information (credit card, password, postal address, email address, etc.) by impersonating someone else.

CEO fraud

The attacker asks the victim to transfer a sum of money, by impersonating a member of the executive board or someone in a senior position within the organisation. This fraud uses various techniques: spear phishing, whaling, or deepfake.

Physical data theft

The attacker exfiltrates confidential data from an organisation and makes it public and/or accessible to unauthorised persons.

Installation of malicious sensor systems

Using software

The attacker convinces the victim to install a program, software or any other malicious sensor directly on their equipment (computer, smartphone, coffee machine, etc.), such as a keylogger, without the victim realising that this will be put to malicious use.

In person

The attacker goes to the site in person, using poorly protected points of access (open doors or disguise) to install keyloggers or other surveillance sensors in strategic places with restricted access (such as machines in a computing centre).

Social engineering targets the weakest link in the chain: the human being.

** Source: European Union Agency for Cybersecurity (ENISA), report : 'Cybersecurity for SMEs - Challenges and Recommendations', June 2021*

How do you avoid a social engineering attack?

In general, it is vital to be vigilant and adopt a critical approach as protection against social engineering. The best defence is prevention and for all employees to be made aware of the risk by IT teams, perhaps their internal Computer Security Incident Response Team (CSIRT), if there is one.

- **Keep all confidential information locked up and password-protected.** Do not allow access to this information, regardless of whether it concerns you or details of your organisation's or its partners' activities.
- **Do not pass on any confidential information without first being sure of the identity of the person asking for it,** independently of the communication channel used.
- **Do not let yourself be charmed by flattery or intimidated by threats:** if the words you hear seem excessive, be on your guard!
- **Keep up-to-date with the security protocols and procedures used in your organisation:** the more informed you are, the more you will know the boundaries not to cross to guarantee your own security as well as that of your colleagues and your organisation.

How should you react when faced with a social engineering attack?

If there is even the slightest doubt regarding the legitimacy of an email, a request for information or a person's actual existence, act immediately.

- **Validate the request for information through another information channel:** discuss it with your colleagues, talk about the content of the request with your superiors.
- **Ask the person concerned to contact you by another means:** so you can be sure of their identity and that they actually exist.
- **Ask additional questions to detect any possible anomalies during the conversation:** ask your contact for details about things they should know or continue the conversation with deliberately incorrect information to gauge their reaction.
- **Work in collaboration with your organisation's IT department or CSIRT team:** even if no specific action can be taken against the fraudster who contacted you, the IT department must at least be informed of this problem. The onus is then on the IT department to take the necessary measures in its technical infrastructure and, above all, to inform all employees and make them aware of the problem.
- **Ask for a visitor's badge or proof of identity from anyone you do not recognise in a restricted/ protected area:** physical safety is of the utmost importance; in the worst case scenario, do not hesitate to escort the person to the security point or inform security.

In social engineering, attackers work on the basis of "act before you think", very often by putting pressure on the victim or acting as if it is an emergency. The best means of protecting yourself is therefore always to "think before you act".

'Social engineering bypasses all technologies, including firewalls'
quote from Kevin Mitnick, author of several books on cybersecurity

Recommendation and responsibility

Permanently destroy all documents and IT equipment containing confidential information you no longer need.

Shred printed documents and degauss your hard drives using suitable tools.

Restrict access to all materials, equipment and buildings.

Restrict access with effective, up-to-date passwords, keep databases updated, encrypt IT equipment if necessary, etc.

Do not blindly trust requests from strangers.

Remain alert, question the merits of requests you receive, regardless of how you receive them.

Example: vulnerability of research and education

It is quite easy for an attacker to impersonate a student and ask questions about the course or even register for the student mailing list, which can then be used to obtain information about people in the group.

Once the information has been obtained, the attacker can try to block essential data for the institution, divert money from grant budgets intended for research and development projects, or even access exam questions to be used for the attacker's own ends, i.e. to sell to third parties.

Service offer

Thanks to its Computer Security Incident Response Team (Restena-CSIRT), the Restena Foundation assists the Luxembourg's research and education community encountering computer security incidents. It also conducts tailor-made phishing and awareness-raising campaigns on hot topics and jointly organises conferences such as CyberDay.lu and Data Privacy Day.

For more information on this service, please visit www.restena.lu/csirt

restena
réseau · sécurité · .lu