3.5 The human layer of cybersecurity – the art of social engineering

by Elisa Norvanto

When it comes to cyber security, any successful organisation must focus on people, processes and technology. Technology provides automated safeguards and processes to determine the series of actions to be taken to achieve a particular end. However, even organisations with strong security practices are vulnerable to human error.[1] *To ensure the strength of the human aspects in any information security plan, an organisation must first recognise and address the human aspect's biggest threat, namely social engineering.*

Cybersecurity has become a part of everyone's life, and it can affect anyone using and anything related to the Internet. As the digital era develops, cyber security evolves and software vulnerabilities diminish. However, people, as individuals, are more exposed today than ever before. Cyber security is vitally important to public and private organisations. Effective information security comprises multiple layers of defence which work together to protect information, access to networks and information systems. The premise is that if one layer fails, other layers will fail too. Technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programmes, and encryption are often the only areas that are considered in cyber security. However, effective penetration attacks are often social rather than technical and they account for the majority of cyber attacks. Indeed, **the most significant vulnerability in information security relates to human error**. If, as a result, an individual with malicious intent is able to bypass a system, that individual can bypass all of the other defensive layers designed to ensure information security.[2]

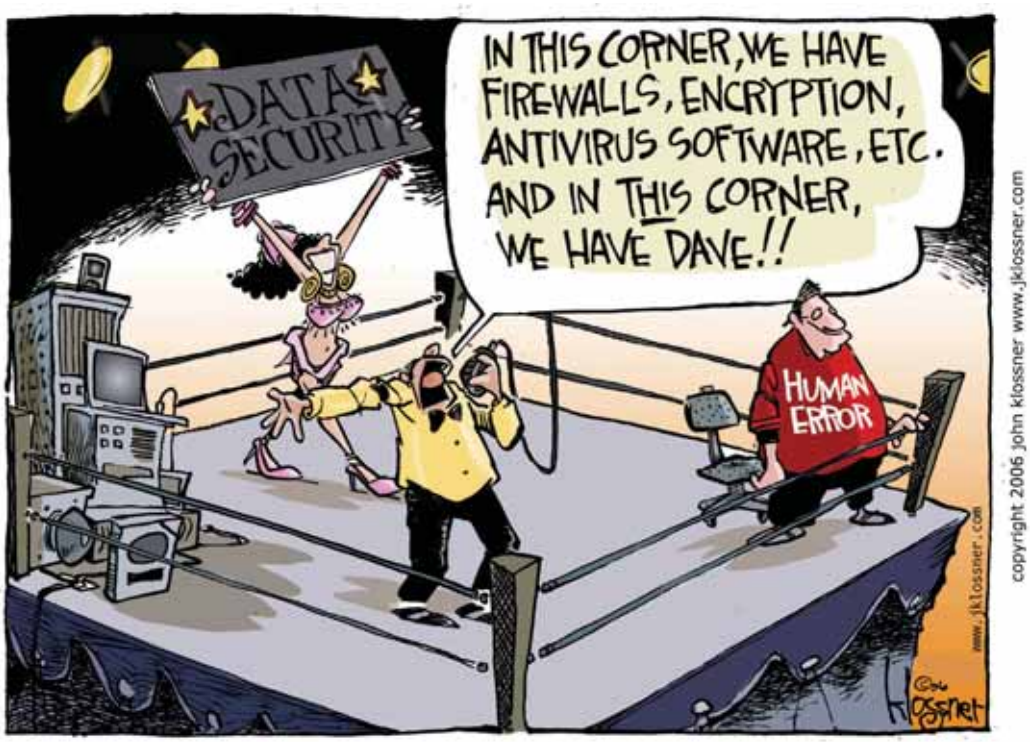
According to IBM's Cyber Security Intelligence index[3], 95% of all information security incidents involve human error. Many of these entail successful attacks by external

---

1 Fran Howarth, 'The Role of Human Error in Successful Security Attacks', *SecurityIntelligence.com*, 2.9.2014. Retrieved on: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

2 Ugo Emekauwa, 'The Human Layer of Information Security Defense', 19.10.2007. Retrieved from http://securitynewswire.com/block/index.html.

3 Fran Howarth, 'The Role of Human Error in Successful Security Attacks', *SecurityIntelligence.com*, 2.9.2014. Retrieved on: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/



attackers who exploit human vulnerabilities in order to trick insiders within organisations into unwittingly providing access to sensitive information. These mistakes can be costly since they involve privileged insiders, such as government employees, who often have access to the most sensitive information. The greatest impact of successful security attacks concerns disclosure of sensitive data, the introduction of malware, or the theft of intellectual property. While cyberattacks are generally considered to be technical, successful ransomware operations employ **social engineering tactics** to help identify, target and exploit vulnerabilities.

Social engineering

Cyber criminals use social engineering tactics in order to convince people to open email attachments infected with malware, persuade unsuspecting individuals to divulge sensitive information, or even scare people into installing and running malware.[4]

4 Andy Mc, 'Do your employees know they are being targeted?', *Security*, 18.11.2017. Retrieved on: https://www.insta.digital/do-your-employees-know-they-are-being-targetted/.

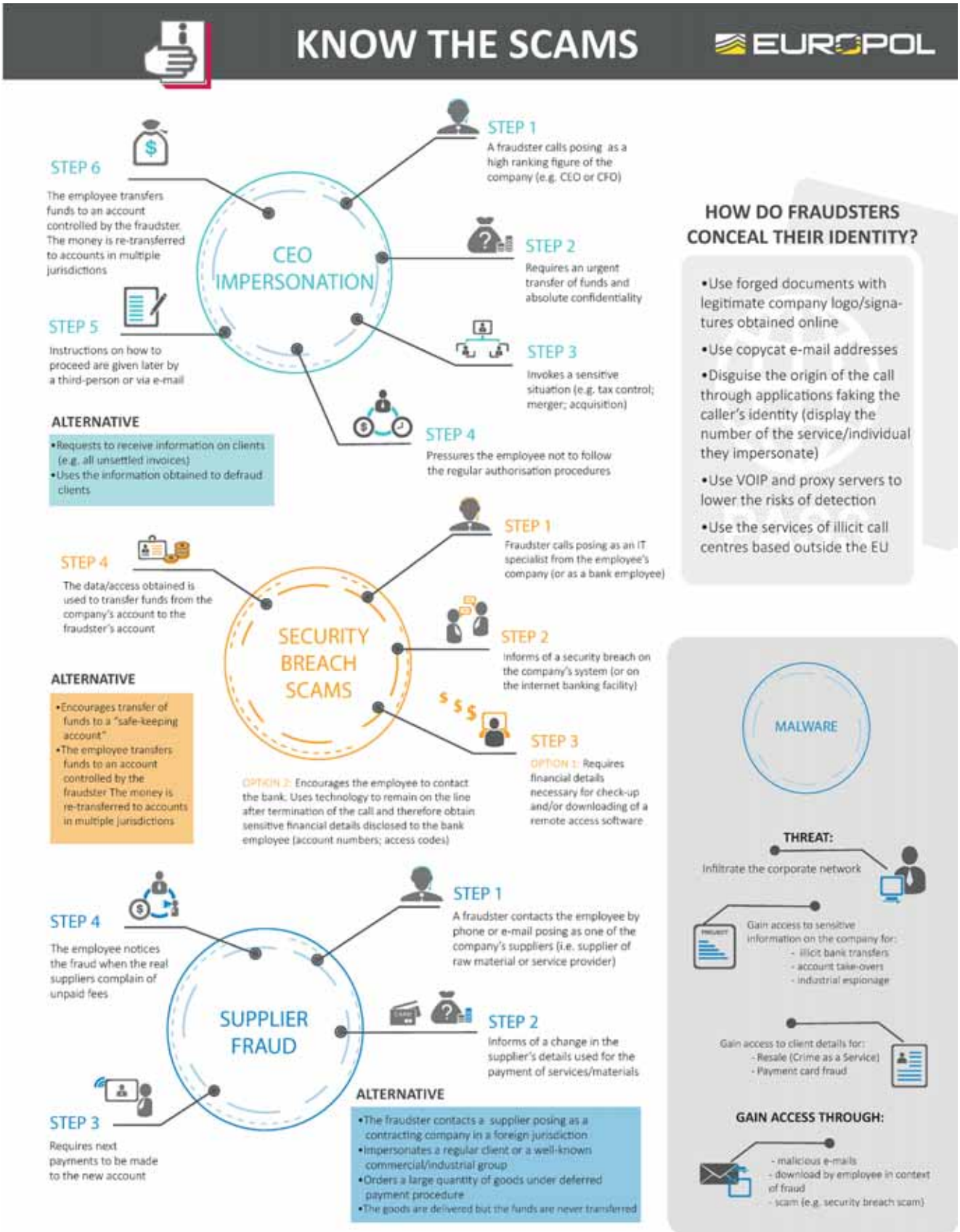
Social engineering is the art of exploiting human flaws to achieve a malicious objective.[5] They can be human-based and technology-based. 'Human-based' involves a person-to-person interaction to obtain the desired action. 'Technology-based' involves a digital interface that attempts to achieve the desired outcome, such as pop-up windows and email attachments.[6] In both cases, social engineering uses **human interaction to psychologically manipulate targets** through deception and persuasion in order to influence the target's actions. Cyber threat actors use social engineering techniques to deceive, persuade, and influence targets to disclose information. It often involves tricking people into breaking standard security practices or giving away information, most often over the telephone or via email, but also through direct observation and unauthorised physical access. When successful, many social engineering attacks enable attackers to gain authorised access to confidential information. Social engineering attacks differ from traditional hacking in the sense that social engineering attacks can be non-technical and do not necessarily involve the compromise or exploitation of software or systems.[7]

---

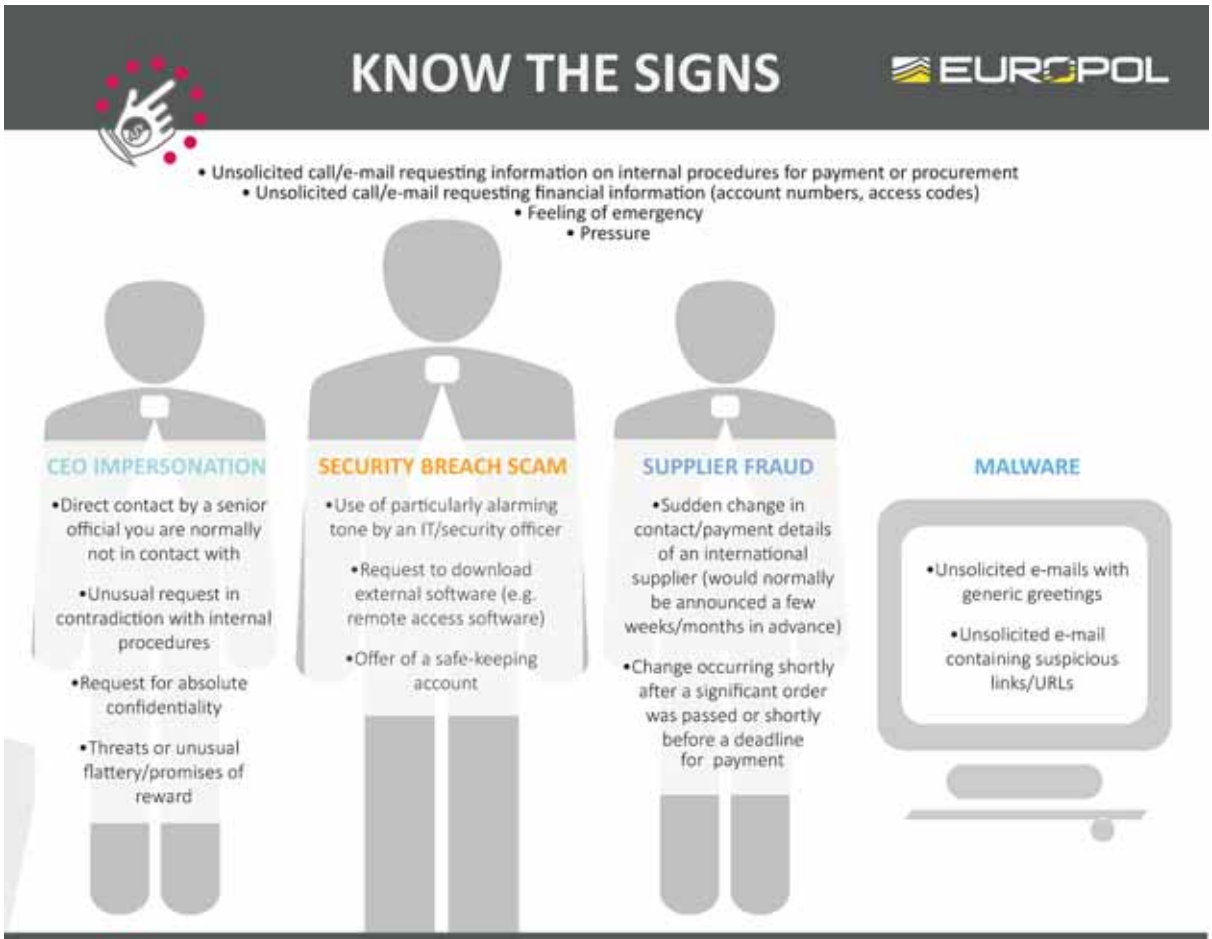
5 Mitnick, K. D. and Simon, W. L. 'The art of deception: Controlling the human element of security.' (Indianapolis, IN: Wiley, 2002).

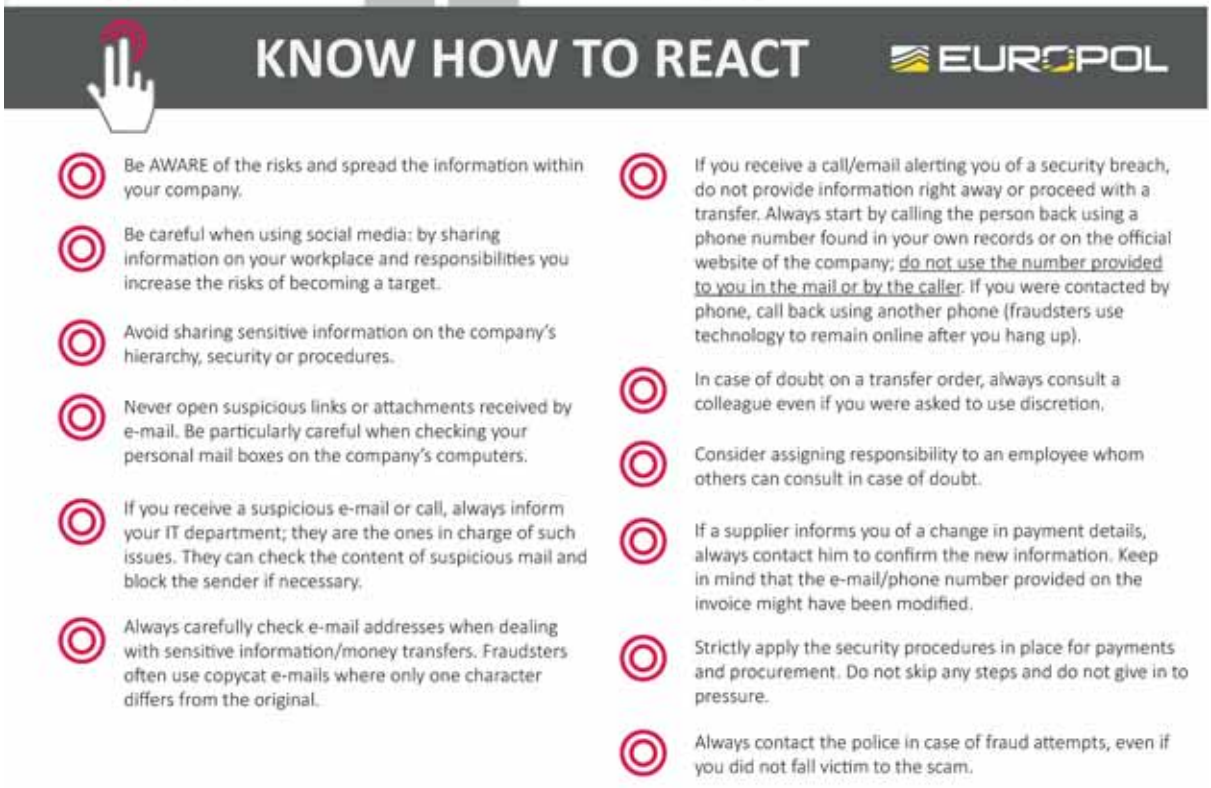
6 Thomas R. Peltier. 'Social Engineering: Concepts and Solutions', last modified 20.6.2018. Retrieved on: http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm#.Wy-RU6YUk7M.

7 Nate Lord, 'What is Social Engineering? Defining and Avoiding Common Social Engineering Threats', *Digital Guardian*, 27.7.2017. Retrieved on: https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.



Graphic: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees


KNOW THE SIGNS
EUROPOL
• Unsolicited call/e-mail requesting information on internal procedures for payment or procurement
• Unsolicited call/e-mail requesting financial information (account numbers, access codes)
• Feeling of emergency
• Pressure
CEO IMPERSONATION
•Direct contact by a senior official you are normally not in contact with
•Unusual request in contradiction with internal procedures
•Request for absolute confidentiality
•Threats or unusual flattery/promises of reward
SECURITY BREACH SCAM
•Use of particularly alarming tone by an IT/security officer
•Request to download external software (e.g. remote access software)
•Offer of a safe-keeping account
SUPPLIER FRAUD
•Sudden change in contact/payment details of an international supplier (would normally be announced a few weeks/months in advance)
•Change occurring shortly after a significant order was passed or shortly before a deadline for payment
MALWARE
•Unsolicited e-mails with generic greetings
•Unsolicited e-mail containing suspicious links/URLs


KNOW HOW TO REACT
EUROPOL
Be AWARE of the risks and spread the information within your company.
Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
Avoid sharing sensitive information on the company's hierarchy, security or procedures.
Never open suspicious links or attachments received by e-mail. Be particularly careful when checking your personal mail boxes on the company's computers.
If you receive a suspicious e-mail or call, always inform your IT department; they are the ones in charge of such issues. They can check the content of suspicious mail and block the sender if necessary.
Always carefully check e-mail addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat e-mails where only one character differs from the original.
If you receive a call/email alerting you of a security breach, do not provide information right away or proceed with a transfer. Always start by calling the person back using a phone number found in your own records or on the official website of the company; do not use the number provided to you in the mail or by the caller. If you were contacted by phone, call back using another phone (fraudsters use technology to remain online after you hang up).
In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
Consider assigning responsibility to an employee whom others can consult in case of doubt.
If a supplier informs you of a change in payment details, always contact him to confirm the new information. Keep in mind that the e-mail/phone number provided on the invoice might have been modified.
Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

Social engineering attacks

Social engineering is recognised as one of the greatest security threats facing organisations. Targeting employees of an organisation through social engineering tactics allows hackers to bypass advanced defences and technologies. Social engineering attacks that target companies or individuals are most easily and successfully launched through **email**. But malicious emails require two triggers to be effective. The first is a cleverly worded subject line that will engage the recipient's curiosity and encourage them to open the email. Once the recipient opens an email, the message has to be compelling enough to encourage the recipient to click on a link or open an attached file in order to initiate or deliver the attack.

The success of a social engineering attack depends on how well the attacker can persuade the victim to perform some action on their behalf, and they may employ a number of influencing techniques (see text box 1). Cyber criminals can seek to provoke emotions such as fear, greed, hope and curiosity to make their attacks more effective. Social engineers use several avenues and techniques for attack. Here are examples of some of the common techniques.

Box 1. Influencing techniques

The psychologist and author Robert Cialdini defines a number of influencing techniques through which social engineers can affect their targets:

1. **Reciprocation:** Manipulating somebody to feel grateful and thus obligated to the social engineer. This often results in the victim feeling that they owe the social engineer a favour.
2. **Scarcity:** Many social engineering attacks invoke scarcity of a resource such as time or money to influence their targets.
3. **Consistency:** Human nature means that people generally try to stick to promises, so as not to appear untrustworthy.
4. **Liking:** People are more likely to comply with someone they like.
5. **Authority:** People comply when a request comes from a figure of authority.
6. **Social Proof:** People comply if and when others are doing the same thing.

(Cialdini, R. B. Influence: Science and practice (5th ed.).
(Boston: Allyn & Bacon, 2008).

Social engineering comes in several forms such as:

- Phishing
- Pretexting
- Baiting
- Quid Pro Quo
- Typosquatting

Phishing

Phishing attacks are the most prevalent way of obtaining information or access to a network. The most effective technique is sending an email with a **phishing link**. Attackers usually send well-crafted emails with seemingly legitimate attachments and an individual will open the email, and either click on a link that leads to a malicious site or download an attachment which contains malicious code, thereby compromising the system.

Pretexting

Another common method is a technique called '**pretexting**', where an invented scenario, or pretext, is established for the target to perform an action for the attacker. These attacks often involve scammers who pretend that they need certain information from their target in order to confirm the latter's identity[8]. Subject lines are carefully chosen to inspire a response and emotional reactions can often be enough to make an employee forget about basic security measures. Pretexting attacks rely on building a false sense of trust. This requires the attacker to create a credible story that leaves little room for doubt in their target's mind.[9]

A classical scenario in pretexting is that someone calls a company claiming to represent a phone company, an IT help desk, an internet provider, and starts asking questions. They claim to have a simple problem or know about a problem that can be fixed quickly but they just need a piece of information. It could be as innocuous as asking for a username

8 David Bisson, 'Social Engineering Attacks to Watch Out For', *Tripwire*, 23.3.2015. Retrieved on: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

9 Nachaat AbdElatif Mohamed, Aman Jantan and Oludare Isaac Abiodun, 'An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network', *Proceedings of the International Multi Conference of Engineers and Computer Scientists* Vol I. IMECS 2018, (March 2018), Hong Kong.

or someone's schedule or as blatant as asking for a password. Once the attacker has this information, they call someone else in the organisation and use the information obtained to refine their attack. They may even combine this with information publicly available on the company's website. After a few calls, they can often pass themselves off as an employee, working for instance in IT support or as the assistant of someone in the organisation's hierarchy, and request access to information or more detailed information *immediately*. The unsuspecting employee, not wanting to annoy anyone in the hierarchy, then bypasses security protocols and complies with the request before they have had time to think[10].

Baiting and Quid Pro Quo

In *baiting* the hacker deceives the victim by enticing the latter with the promise of a reward or good. There are two classic scenarios where baiting is used. In the first scenario, the attacker uses a malicious file disguised as a software update or as generic software. Baiters may also offer users free music or movie downloads if they surrender their login credentials to a certain site. In the second scenario the attacker leaves infected USB sticks on a table or even in a parking lot of a target organisation in the hope that staff will insert these devices into the organisation's computers. This tactic takes advantage of an individual's curiosity. The USB device might be labelled 'confidential', 'salary information' or indicate the name of a person in the organisation's hierarchy. The devices carry malicious software, resulting in the victim's machine being compromised.

A *quid pro quo technique* differs from baiting. Instead of baiting a target with the promise of a good, this technique promises a service or a benefit based on the execution of a specific action. A quid pro quo attack occurs when an attacker requests private information from someone in exchange for something desirable or some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift.

Typosquatting

Typosquatting is when the attacker sets up a website with a similar domain name to a legitimate site. For example, instead of www.e-visa-usa.com, the attacker may register www.e-visa-usa.org. The fake site will match the look and feel of the original. The

10 Keith Casey, 'What is Social Engineering? Defining and Avoiding Common Social Engineering Threats', interview by Nate Lord, *Digital Guardian*, 27.7.2017. Retrieved on: https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

Graphic: https://www.europol.europa.eu/newsroom/news/safer-internet-day

idea is to trap users who mistype a URL in their web browser. They will often be prompted to enter information, such as passport information, which is then captured by the attacker. The victim is then forwarded to the legitimate site and logged in, but without realising that they were redirected and that their information is now compromised[11].

How to combat social engineering?

The threat of social engineering is very real. This very profitable industry seeks unauthorised access to information or unlawfully extracts information for its customers. Social engineering is the hardest form of attack to defend against because it cannot be countered using hardware or software alone. Technology can be used, but not in isolation. A successful defence will require an effective information security architecture, starting with policies and standards and following through with vulnerability assessment processes. Technology provides automated safeguards and processes determine the series of actions to be taken to achieve a particular end. However, even organisations with strong security practices are still vulnerable to human error. Consequently, there are three categories that are considered to mitigate the risk of social engineering; people, processes and technology.

Graphic: https://twitter.com/europol/status/968832613912891392

11 Curtis Peterson, '23 Social Engineering Attacks You Need To Shut Down: Device Left Behind', *Smartilife.com*, 16.3.2016. Retrieved from: https://www.smartfile.com/blog/social-engineering-attacks/.

Traditional IT security activities such as patch management and system hardening are essential to prevent cyberattacks. However, **awareness** is crucial to the reduction of human error in information security. If users are made aware of the threats and risks they face, they can make decisions that are more informed and they will be less vulnerable to falling for well-known ruses. Therefore, the most important advice for organisations is to **train their employees in cyber security**. As a rule, organisations should put in place a security culture that comprises ongoing training which consistently informs employees about the latest security threats. Behavioural change is more effective than technological defence in countering attacks on the human mind. If employees learn how to protect their data and the organisation's confidential data, they will be better able to identify an instance of social engineering and avoid its damaging consequences. They will then be more vigilant and so play a much-needed role in ensuring security.[12]

12 Lily Teplow, 'Breaking Down the Dangers of Social Engineering', *Continuum IT management platform*, 24.3.2017, Retrieved from: https://www.continuum.net/blog/breaking-down-the-dangers-of-social-engineering.