Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (4) Week 7 Unit (Module) name: (Social Engineering)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discussion forums and within the organized sessions with trainer/mentor, e-portfolios
Learning Responsible	• David Sommer • Ileana Hamburg
Learning Activity Goals	1. Social engineering attack techniques 2. Importance of Social Engineering Training 3. How to Protect from Phishing Attacks 4. Social engineering from an interdisciplinary view
Skills to be Gained	• **TS3 Network security** • **TS4 Penetration (exploitable vulnerabilites) testing** • **SS3 Cognitive and behaviour analysis**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Brief information about the module

Description
Social engineering is an important and verry often threat to information security. This module explains shortly the Lifecycle of social engineering, how an attack occurs and can be prevented. Particularly phishing is described, as one of the most popular social engineering attacks. Many companies use technical solutions to prevent attacks, but technological measures are not very effective if staff is not trained correspond. This is one of the aims of this unit. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training

Content of the Learning Material

What is social engineering?

Social engineering can be defined as manipulating human beings, most often with the use of psychological methods, to gain access to data, documents, and information that the attacker should not have access to obtain. Various forms of social engineering can be found years ago but due to increased use of technology in main aspects of business and life, the threats grow and became a complex process difficult to stop. Social engineering is one of the leading threats to information security today and is an effective form of cybercrime. Potential repercussions of a successful social attack can be very dangerous for people and organizations. In 2019, for example, phishing, a form of social engineering crime, was responsible many data breaches, more than any other type of attack.

Many social engineering attacks have financial scops and sop organizations lost considerable money amounts. In 2020, for example, U.S. losses $4.2 billion, according to the FBI (Abbate, 2020).

Companies could suffer business disruption — loss of productivity, a decline in employee morale and difficulties for organization to recover. This process can have consequences, often an incident response team is fired, security software to help prevent future attacks should be provided and employees must be

requalified. Companies, in case of a social engineering attack could suffer also damage of reputation because customers are not convincing that the organization can protect itself.

Importance of Social Engineering Training

It is difficult to protect against social engineering because the tactics that attackers use are based on individuals' behaviour and if employees do not have corresponding training to recognize social engineering attacks, the risk of falling victim is great.

Social engineering training could be included in security awareness programs and gives employees the knowledge and tools they need to recognize these types of attacks and protect both themselves and their organization (Weßelmann, 2008).

Due to importance of social engineering training in minimizing threats, many organizations particularly SMEs which have less resources should be helped to take cyber awareness training including social engineering very seriously and offer their employees possibilities to follow it (Mimecast Contributing Writer, 2021).

By 2022, for example, it is planned that 60% of large organizations will consider security awareness (Gartner Magic Quadrant for SAT 2019).

Social Engineering Attack Lifecycle

Often social engineering attacks are done in more steps. The attacker first investigates the intended victim to gather necessary background information, such as points of entry and weak security protocols which are needed to the attack. Then, the attacker tries to gain victim's trust and provide stimuli for actions not usually security practices, such as become sensitive information or granting access to critical resources. Figure 1 explains the Lifecycle of an attack.

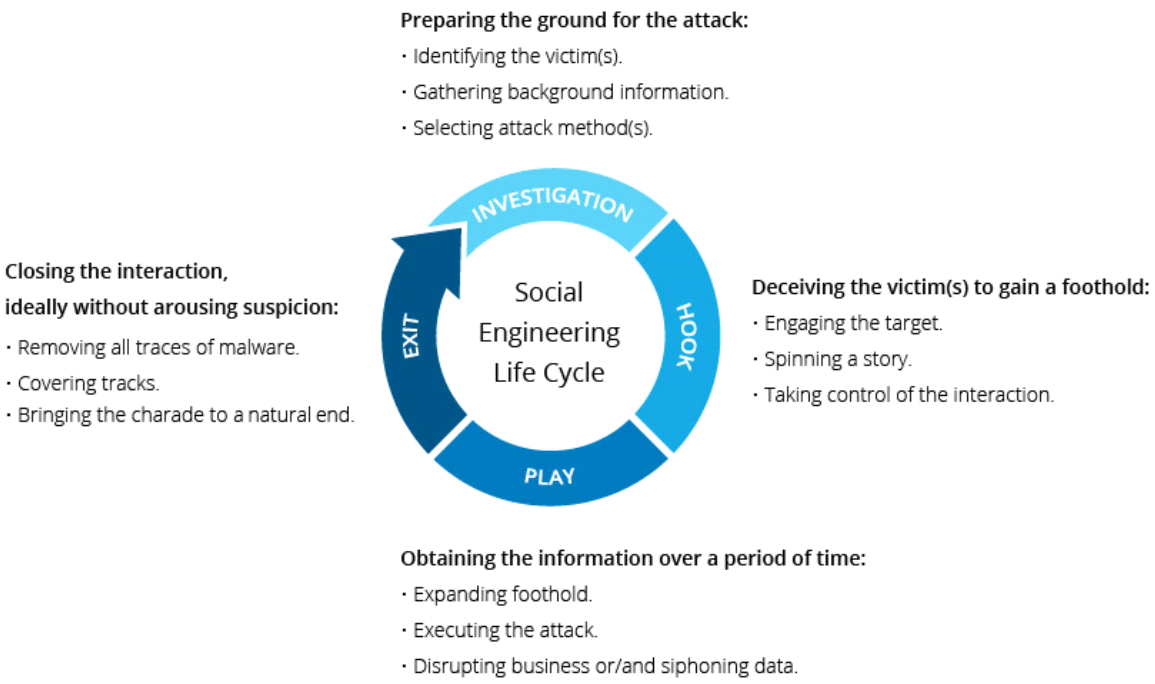

Figure 1: Attack Lifecycle (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Social engineering is particularly dangerous because it is based more on human error, not on vulnerabilities in software and operating systems. It is more difficult to predict mistakes made by legitimate users, identify and stop these than a malware-based intrusion.

Social engineering attack techniques

Social engineering attacks have different forms and can be done anywhere where human interaction is involved. The most common forms of digital social engineering attacks are the followings:

Baiting

Baiting attacks try to achieve a victim's curiosity. They attract users into a trap stealing their personal information or infecting their systems with malware. The most often form of baiting uses physical media to disperse malware. For example, malware-infected flash drives, in conspicuous areas where it is sure that potential victims see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look, such as a label presenting it as the company's payroll list. Victims pick up the bait and insert it into a work or home computer, resulting in an automatic malware installation on the system. Baiting attacks don't necessarily be done out in the

physical world. Online forms of baiting consist of tempting ads that lead to malicious sites, which encourage users to download a malware-infected application.

Scareware

Victims become false alarms and fictitious threats. Users think their system is infected with malware and they must install software that has benefit only for the attacker or is malware itself. Scareware is considered as deception software, rogue scanner software and fraud ware. A common scareware example is the legitimate-looking popup banners in own browser while surfing the web with text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) or direct the victim to a malicious site where own computer will be infected. Scareware is also distributed via spam email that makes offers users to buy worthless/harmful services.

Pretexting

Attacker obtains information through a series through lies. The scam (fraud) is often initiated by a perpetrator underlying to need sensitive information from a victim so as to perform a critical task. The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. Attacker asks questions that are required to confirm the victim's identity, through which they gather important personal data. Many important information and records can be gathered using this fraud, i.e., social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

Is one of the most popular social engineering attack types; phishing scams (frauds) are emails and text message campaigns aimed to achieve curiosity or fear in victims and encourage them to give sensitive information, clicking on links to malicious websites, or opening attachments that contain malware. An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action, such as a required password change. It includes a link to a not legitimate website—nearly identical in appearance to its legitimate version— and the user enters their current credentials and new password. The information is sent to the attacker. Because identical, or near-identical, messages are sent to many users in phishing campaigns, detecting and blocking them are easier for mail servers having access to threat sharing platforms.

Spear phishing

This is a special form of the phishing attack because an attacker chooses specific individuals or enterprises. Attackers adapt their messages to characteristics, job positions, and contacts of their victims to make their attack less conspicuous. Spear phishing requires more effort from the

perpetrator (person who commits the illegal act) and could take weeks and months to prepare it. It is much difficult to detect such attacks and they have better success rates. As an example, a spear phishing scenario involves an attacker who, as an (existing) organization's IT consultant, sends an email to one or more employees. It is signed exactly as the consultant normally does and recipients think it's an authentic message. The message requires victims to change their password and provides them with a link that redirects them to a malicious page where the attacker steals their credentials.

Detect Phishing

Scammers (people making fraudulent business) use email or text messages to trick persons to communicate their personal information. They try to steal passwords, account numbers, or social security numbers. If they get that information, they could gain access to email, bank, or other accounts. Scammers launch thousands of phishing attacks like every day — and they're often successful. Scammers often update their tactics, but there are some signs that help victims to recognize a phishing email or text message, like following:

- Phishing emails and text messages can look like they're from a company you know or trust. They look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.
- Phishing emails and text messages often tell a story to trick victims into clicking on a person link or opening an attachment. They may say they've noticed some suspicious activity or log-in attempts, claim there's a problem with the account or payment information, say that person must confirm some personal information, include a fake invoice, want the person to click on a link to make a payment, say the person is eligible to register for a government refund, etc.

Figure 2 shows a real-world example of a phishing.

The email looks like it's from a company the person know could and trust: Netflix. It even uses a Netflix logo and header.

The email says own account is on hold because of a billing problem.

The email has a generic greeting, "Hi Dear." If the person has an account at the business, it probably wouldn't use a such generic greeting.

The email invites the person to click on a link to update your payment details.

This email might look real, but it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can damage the reputation of the companies they're spoofing.

Protect against phishing

Own email spam filters could keep many phishing emails out of own inbox. But scammers are always trying to outsmart spam filters, so it is useful to add extra layers of protection.

Methods to protect:

- To protect own computer by using security software, software should be updated automatically to deal with security threats.

- To protect own mobile phone, software should update automatically.
- To protect own accounts, multi-factor authentication should be used.

The additional credentials to log in to own account can be grouped into:

- A passcode gets via an authentication app or a security key.
- A scan of own fingerprint, retina, or face.

Multi-factor authentication makes it harder for scammers to log in to other accounts if they do get corresponding username and password. It is important to protect own data by backups which aren't connected to own home network. Own computer files should be copied to an external hard drive or cloud storage. Also, data on own phone should be copied.

Act to a Suspect a Phishing Attack

- If an email or a text message comes that asks to click on a link or open an attachment, ask: Do I have an account with the company or know the person that contacted me?
- If the answer is "No," it could be a phishing scam. You have to review the tips in How to recognize phishing, look for signs of a phishing scam, report the message and then delete it.
- If the answer is "Yes," contact the company using a phone number or real website without put the information in the email because attachments and links can install harmful malware.

Responding to a Phishing Email

There are specific steps to take based on the information lost

- Run a scan.
- If a phishing email or text message is received, report it.

Social engineering from an interdisciplinary view

The networked today's world and the intensive use of the internet and technology are catalysts for social engineering attacks. System protections are helpful to mitigate some social engineering attacks, but it is not enough. The Federal Bureau of Investigation's internet crime underlined the increased use of social engineering and business email fraud schemes resulted in billions of dollars in losses over the past several years (Abbate, 2020). Again, methods of hackers, it is necessary to use an interdisciplinary approach to understand this phenomenon and all its complexities,

especially in the context of how it affects businesses. Literature reviews highlight perspectives from different disciplines: information technology, psychology, business and ethics. Figure 3 illustrates this view (Washo, 2021).

Information technology discipline

Social engineering cannot be discussed unless in the context of the actual information systems and their use in the business. Technical defences can be used as a form of risk mitigation and control strategies are recommended to be used. Multi-factor authentication is a common and often effective way for organizations to confirm that the person accessing the systems should actually have that access. For example, a login process with a username and password would be one way for the user to be authenticated. An additional factor could be the use of a virtual private network (VPN) login to further validate the user.

Psychology discipline

Social engineering is connected with deception, so a psychological approach to understanding the concept is important to understand the thoughts and behaviours of both the attacker and victim. The use of psychological methods is important to social engineering because they are used to support the protections such as firewalls and systems used to identify intruders (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). The entire information technology network at a particular company is only as strong as the individual user of a particular system. In fact, the behaviour and actions of employees are one of the leading causes of data breaches.

Business Perspective

Social engineering impact many types of businesses and have implications for the way that organizations are structured and managed. The topic can be considered from the business perspective to determine the factors that impact social engineering attacks. This viewpoint is beneficial if it is related to the following areas of business: training and development, documented policies, internal audit procedures, budgets, and organizational culture. A deficiency in any of these areas can contribute to attacks.

Ethical Perspective

Ethics is important in the context of social engineering and the related research on the topic. The idea of manipulating another human being violates many ethical principles. In case of a social engineering occurrence, treatment of the victims can vary, but often, they are not sufficient treated allowing the attack to occur. Unfortunately, the qualities usually found in ideal employees such as trust, the willingness to please others such as managers, customers, co-workers, and visitors, and

the readiness to obey authority, are usually the same characteristics that make an individual susceptible to social engineering (Mouton, Malan, Kimppa, & Venter, 2015).

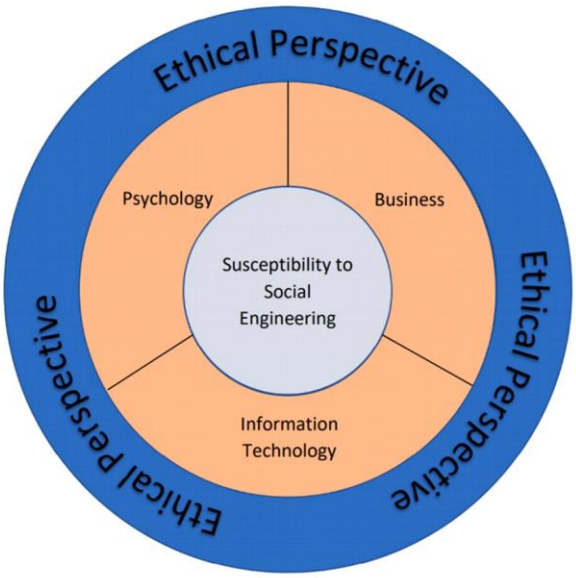

Figure 3: Social engineering from an interdisciplinary view (Washo, 2021)

The literature review from different disciplines explains the need for an integrated approach to study the complex subject of social engineering. Each discipline, provides information on how to understand and interpret the topic, protect against various types of attacks, and understand the impact of social engineering from both a human and organizational standpoint. However, each discipline's interpretation of the topic is only useful when viewed in the context of the other disciplines.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. How to recognize Phishing: i.e. Phishing emails and text messages often tell a story to determine victims to click on a link or open an attachment.
2. How to protect from Phishing Attacks
3. Please name some disciplines connected with Social Engineering and explain shortly these connections

Attachments:

1. Presentation
2. Video movies

References:

Abbate, P., (2020). Internet Crime Report 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J.W.H, Montoya, L., Pieter, W., Junger, M, Hartel, P. (2017). On the anatomy of social engineering attacks – A literature-based dissection of successcul attacks. *Journal of Investigative Psychology and Offender Profiling. 15. 20-45.*

Lee, T. (2020). Hire the Right Teachers for the Better Security Awarness. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Contributing Writer (2021). Social Engineering Awarness Training for Emploeyees. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114–127. https://doi.org/10.1016/j.____HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: Datenschutz und Datensicherheit. DuD. 601–604.