Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Social engineering – users are the weakest link

By CTS Customized Training Solutions & CASE

Erasmus+

Objectives and Goals:

At the end of this module you will be able to:

- define social engineering
- recognize and distinguish the most commonly used social engineering techniques
- understand the manipulative mechanisms used by the attacker
- locate potential sources of attack
- analyze the risk of social engineering attack on your company

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Index

Unit 1: What is social engineering?

Section 1.1: Definition
- Are you safe?
- The weakest link

Section 1.2: What is social engineering attack?
- What kind of data is considered sensitive?

Section 1.3: Principles of social engineering attacks
- What happens during the attack?

Section 1.4: Who may become a victim?

Unit 2: **Social engineering techniques**

Section 2.1: Message from a friend
- Why John did it to you?
- When you can be attacked with this technique?

Section 2.2: Phishing
- How the scenario may look like?

Section 2.3: Vishing
- How the scenario may look like?
- When you can be attacked with this technique?

Section 2.4: Baiting
- How the scenario may look like?

Section 2.5: Summary

Unit 3: **Social engineering prevention**

Section 3.1: Dos and don'ts

Unit 1: What is social engineering?

Section 1.1: Definition

Social engineering in the IT context is a term used for various malicious activities made through human interactions. It is based on psychological manipulation. The point is to push a user to make a security mistake. In other words, the social engineering attack is possible only if the user is not aware of harmful intent.

Are you safe?

Social engineering attacks can hit you any time, no matter how big or small of a business you build.

The weakest link

The weakest link in the whole process is the user: you, your employees, your business partners. To minimize the risk you need to maximize awareness. **How to do that?**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: What is social engineering?

Section 1.2: What is social engineering attack?

Understanding social engineering attacks is the first step to increase your and your employees' awareness. First of all, you need to remember that cybercriminals and fraudsters organize those attacks. However, it is not always about money. Any amount of information (like password) or **sensitive data** is enough to make a fraud.

What kind of data is considered sensitive?

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- trade-union membership
- genetic data, biometric data processed solely to identify a human being
- health-related data
- data concerning a person's sex life or sexual orientation*

*Source: European Commission > What personal data is considered sensitive?

Unit 1: What is social engineering?

Section 1.3: Principles of social engineering attacks

Usually, a social engineering attack has **3 steps**...

step 1: the attacker targets a victim

- identifying victims
- background research
- choosing attack methods

step 2: the attacker earns the victim's trust

- engaging a victim in a story
- taking control of the interaction
- gaining a foothold

step 3: the attacker achieves the goal, stealing data or breaking security practices

- executing attack
- removing all traces
- vanishing

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: What is social engineering?

Section 1.3: Principles of social engineering attacks

In a social engineering attack, the attacker makes use of psychological manipulation. That is why it is even more dangerous than a cyberattack on your system. Why? Because you need to be sure that you and your employees can discern between manipulation and standard advertising. It is not easy because we are only humans.

What happens during the attack?

The attacker plays on the victim's weaknesses. So let's think about the social engineering attack like the dirty game, where only one person knows the rules, moreover, sometimes also creates them!
Like every game, this one also has some general mechanisms that should increase the chance of winning.

Most social engineering attacks are based on 5 principles: **authority, social proof, scarcity, urgency, familiarity.**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: What is social engineering?

Section 1.3: Principles of social engineering attacks

authority:
the attacker presents
himself / herself
as an authority figure

scarcity:
the attacker uses
the mechanism that
the victim will miss out
if they won't do anything

familiarity:
the attacker convinces
the victim to execute
specific operations
by gaining his / her trust

social proof:
the attacker uses peer
pressure to force the victim
to take an action

urgency:
the attacker uses the idea
that the victim will miss out
if they won't act
as soon as possible

Erasmus+

Unit 1: What is social engineering?

Section 1.4: Who may become a victim?

You have just known 5 principles of social engineering attacks. Those principles are linked with people's psychological drivers and motivation. These ones, of course, are created deep in our subconscious.

Robert Cialdini, a psychologist, speaker, and author of the book entitled "Influence: Science and Practice" described how people can be influenced by others. According to Cialdini, key factors are:

Reciprocation

Generally, people feel obliged to pay back after they get some help. This characteristic seems to be so natural for all cultures that we don't feel uncomfortable when someone asks us to return favors.

Cialdini mentioned that so-called compliance professionals often offer a small gift to potential customers to play on this trait. Studies show that even the unwanted gift will influence the recipient to reciprocate.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: What is social engineering?

Section 1.4: Who may become a victim?

Commitment and consistency

People often stick to their habits and first choices. They want to look consistent in their behavior. They also appreciate consistency in others.

Cialdini mentioned it is also linked with people's strong desire to stand by commitments made by providing further justification and reasons for supporting them.

Social proof

We have already mentioned that mechanism speaking about principles of social engineering attacks. Social proof means that people trust other people similar to themselves when making decisions. That is more obvious in uncertain or ambiguous situations.

Cialdini mentioned that so-called compliance professionals provide fake information on what others are doing playing on this trait. For example, they prepare staged interviews, false data, or case studies.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: What is social engineering?

Section 1.4: Who may become a victim?

Liking

Well, that is not a secret — people need to be liked. In consequence of playing on this trait, people are more likely to agree to offers from people they like.

Cialdini mentioned that liking people can manifest itself in several ways, e.g. it may be a physical attraction or tending to a similar person.

Authority

That is probably the most dangerous influence factor, giving the attacker the biggest power. Generally, people follow those who seem to be strongest, better, self-confident in their eyes; who have something that they don't have. Studies show that people usually react in an automated mode to instructions from authority and even to symbols of authority (like expensive cars, uniforms, diplomas, academic degrees, etc.). That happens even when instinct hints that the instructions should be rejected.

Unit 1: What is social engineering?

Section 1.4: Who may become a victim?

Scarcity

Again, we mentioned this mechanism speaking about principles of social engineering attacks. Scarcity is based on people's desire to possess less available things. Less available may be exclusive or time-limited.
This trait helps e.g. advertisers to promote goods as "limited availability", or "short time only".

So, who may become a victim of social engineering attacks?

In general — anyone. However, a person's psychological background and actual condition matter.

Always keep in mind that social engineering base on manipulation.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: Social engineering techniques

Section 2.1: Message from a friend

Imagine that you are at work, writing some reports in Excel in your company's cloud, and in the meanwhile, you take a look at your social media accounts. So, in one browser you have opened both, Excel and Facebook. You are filling these boring charts and, suddenly, your best friend (let's call him John) writes you on Messenger. John wrote you that your naked photos are available on the attached website — and he sent the link. You click the link and...

You probably just lost access to your account on Facebook and/or your business site as well. Maybe you have also compromised some data stored on your computer.

Why John did it to you?

Well, let's be honest. **That wasn't John...**

Erasmus+

Unit 2: Social engineering techniques

Section 2.1: Message from a friend

Probably it was a bot created to steal data. Your friend John was the victim same as you. The attacker used his identity (in this case, social media account) to gain your trust. After all, you know John very well, you grew up together, and you are best friends. How does the attacker could know that?

Maybe you have many pictures together, speak a lot via Messenger or maybe it was a coincidence — but it worked. Now you are the next victim in the long chain called **phishing.**

When you can be attacked with this technique?

Using social media, instant messengers, chats, e-mails, SMS, etc.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: Social engineering techniques

Section 2.2: Phishing

Nowadays, the most popular social engineering technique is phishing. Phishing is any kind of messaging campaign planned to redirect the victim towards a particular form, site, or checkout. The attacker fakes a trusted source (e.g. friend, bank, insurance agency, investment funds) and prepares a reasonable scenario. The strong emotional theme usually helps with the suspension of disbelief.

How the scenario may look like?

like urgently asking for your help

Your "friend" got stuck abroad, has been robbed, beaten, and is in the hospital. He needs money and instructs you how to make a transfer.

OR

Your "friend" saw your naked pictures on the Internet and sent you a link.

Erasmus+

Unit 2: Social engineering techniques

Section 2.2: Phishing

like actions with legitimate-seeming background

Your "bank" sent you an SMS with the link asking about the balance confirmation.

OR

Your "hosting provider" sent you an e-mail claiming that their data storage was hacked, and you need to contact them via the attached form.

like asking to donate to their charitable fundraiser, etc.

Some authority figure asked you for your support in repairing the effects of a terrible natural disaster, political campaign, or charity.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: Social engineering techniques

Section 2.3: Vishing

Vishing is a variation of phishing done using voice technology such as a phone call, Messenger/ Zoom call, or fraudulent voice message. The manipulation mechanisms are the same as in phishing, but the attacker uses urgent voice mails or calls to convince the victim to make the move.

How the scenario may look like?

huge danger

After the attacker's statement about an enormous danger, like bank account hacking or unpaid taxes, the victim feels the pressure to act quickly. Caught in the moment, the victim shares their sensitive data and passwords during the call.

Erasmus+

Unit 2: Social engineering techniques

Section 2.3: Vishing

When you can be attacked with this technique?

Having a public profile / site of your company with your phone number (not only yours but also your employees), sharing your phone number in social media, using instant messengers and apps with a voice call option, etc.

Section 2.4: Baiting

Sometimes instead of danger, there is a huge opportunity. You are the winner, the lucky one, you can invest small amount of money and in a short time turn it into a fortune! It is good to remember that attackers often use baiting under the cover of various European funds. You may be attacked by online form, phone calls, or even in person.

Unit 2: Social engineering techniques

Section 2.4: Baiting

How the scenario may look like?

there is something you want →

The attacker chooses something that people desire, e.g. downloading a new movie. Many people will take the bait to find something they want.

great deal! →

The attacker may create an announcement informing about an amazingly great deal on classified sites, auction sites, etc. Usually, the attacker opens a seller account with a good rating to minimize your suspicion.

If the victim takes the bait he / she will be infected with malicious software. It usually generates further actions against the victim and his / her contacts.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 3: Social engineering prevention

Section 2.5: Summary

Of course, all mentioned scenarios are just examples of social engineering techniques. You need to remember that the attacker is a clever, technology-oriented person who has explored manipulative techniques.

Phishing, vishing, and baiting can have endless scenarios. It all depends on the ingenuity and creativity of the attacker.

Check the news regularly for current social engineering techniques to stay up to date.

Erasmus+

Unit 3: Social engineering prevention

Section 3.1: Dos and don'ts

As you can see, social engineering techniques are effective and powerful because of psychological manipulation, lack of awareness and proper knowledge. The whole attack may happen only if the victim is susceptible to chosen mechanisms.

So what you can do to prevent social engineering attacks?

Increase awareness of malicious activities among yourself, your employees, partners and clients. Remember that social engineering techniques change across time and space, so it is necessary to update your knowledge regularly.

Unit 3: Social engineering prevention

Section 3.1: Dos and don'ts

Teach your employees, partners, and clients how valuable are passwords and sensitive data. Remember that a funny post on Facebook asking you about your date of birth may be used against you. Think how many times you used your date of birth in a password...

Do not locate all sensitive data and crucial information in one place. If the attacker is able to steal them with one print screen, you need to work on your security system.

Do not click on any links and pictures you receive before you check the source. Even if the source looks familiar, do not rush. Take a double look at an e-mail address, IP, link, etc.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 3: Social engineering prevention

Section 3.1: Dos and don'ts

Prepare transparent security standards for your company. Plan the protocol in the case of attack and teach your employees, partners, and clients what to do.

Do not cause unnecessary fear among your employees, partners, and clients. Fear helps the attacker manipulating people. Awareness and knowledge are the opposite.

Are you ready to face social engineering techniques?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bibliography and relevant links

European Commission > What personal data is considered sensitive

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Webroot > What is Social Engineering? **Examples & Prevention Tips**

https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Seon > **What is Social Engineering? Attacks, Techniques & Prevention**

https://seon.io/resources/protect-against-social-engineering-attacks/?utm_term=&utm_campaign=%5BS%5D%20Blog%20-%20dynamic%20%5BEMEA%5D&utm_source=google&utm_medium=cpc&hsa_acc=9367189488&hsa_cam=12655034312&hsa_grp=119030291966&hsa_ad=511148698722&hsa_src=g&hsa_tgt=dsa-41475539813&hsa_kw=&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwvuGJBhB1EiwACU1AibG5GowOFa1Q_FazH8_RDbrb3OEI7k7fQacOcLKrty9ZFQw-b7i_7hoCDWcQAvD_BwE

Imperva > **Social Engineering**

https://www.imperva.com/learn/application-security/social-engineering-attack/

Verizon > Data Breach Investigations Report > **2021 DBIR Master's Guide**

https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Terranova Security > **9 Examples of Social Engineering Attacks**

https://terranovasecurity.com/examples-of-social-engineering-attacks/

Thank you for your attention!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.