

Introduction to Information Security, INTROSEC  
Autumn Term 2018

**Report of Social Engineering  
Assignment 2**

# Summary

<b>Introduction</b>	<b>3</b>
<b>Social engineering scenario 1</b>	<b>4</b>
Scenario description	4
Scenario analysis	4
Interviews	5
Results	6
Discussion	7
<b>Social engineering scenario 2</b>	<b>9</b>
Scenario description	9
Scenario analysis	10
Interviews	10
Results	12
Discussion	13
<b>Other studies</b>	<b>14</b>
<b>Conclusion</b>	<b>16</b>
<b>References</b>	<b>17</b>
<b>Time summary</b>	<b>17</b>

## Introduction

Which is the most unsusceptible entity that could bypass our security? We do not have to think about the hidden bugs or vulnerabilities between the lines of code of the operating systems or software used. We do not have to focus on the various malware that can be created and disseminated via the web. The real weak link in the cybersecurity chain is represented by the user: as more and more reports by industry analysts show, it becomes increasingly easier for hackers to break in networks or computer systems exploiting the good faith of Internet users.

In order to diffuse the malware, and to perform other attacks, hackers take advantages of the human factor. Users, very often unconsciously, play on the role of a viral computer vector: just clicking on a fake advertisement or downloading an unsafe app, it is possible to find yourself with the computer infected because we opened the door to an attacker. Or, in the worst case, with your email account or social profile hacked. In short, even if we protect ourselves with the best antivirus, our personal information is at risk if we are imprudent.

This category of attacks belongs to social engineering, that is like attacking the human mind. This is something that in many ways can be much simpler than finding a new software vulnerability and using it as a gateway to penetrate a company's systems. These vulnerabilities can cost tens of thousands of dollars in the hacker environment, money that can be saved if you can deceptively persuade the potential target to install a virus directly on his computer. After all, there is no need to tamper with a lock when it may be enough to convince someone to let us enter his home.

We set up two possible scenarios with an attacker, who tries to manipulate a victim using social engineering to analyze this phenomenon.

In particular, the goal is to evaluate three characteristics: the likelihood of success, the potential damage caused and the potential victims' awareness

We asked ourselves some questions:

1. Could these attacks be put into practice?
2. How likely they would be to succeed?
3. What is the potential damage that they could cause?
4. Are targets aware of the possibility of an attack of this kind?
5. Did they attend any course aimed at preventing social engineering?

In order to test both the scenarios and answer these questions, we designed and performed interviews to target people. So that the interviewees do not prepare themselves to the questions or feel in a constraint in answering, the meeting and the conversation with the potential victims take place without a true clarification about what will be the object of study. A related topic is presented, so that they were not induced to focus on giving the "right" answer, instead of the truth.

# Social engineering scenario 1

## Scenario description

An attacker wants to get credentials to access the bank profiles of his victims. In order to succeed in his goal, he pretends to be the largest bank in the country, so that he has more possibilities to find users of this bank. He starts sending emails to attack his victims: the message pretends to be sent by the aforementioned bank. The intent of the email is to warn the user that, in the last 48 hours, 4 withdrawals have been made. The sum of these takings amounts to 200 euros each and they were made in Bangladesh. The email reproduces the original layout of the bank site with the link to the login in order to invite the user to check your bank account. The linked page is not the bank's, in opposite, it is a page that fakes the actual login access page. It steals and stores login credentials when the victims try to verify the episode.

## Scenario analysis

In this attack, there are many psychological artifices involved so that the hack succeeds:

- *Sense of urgency*
- *Sense of trouble*
- *Panic*
- *Trust in authority*
- *Ignorance*

The attacker arranges the message to attract user's attention. The text of the email is not composed in a random way: in order to suggest the victim visit the specific website, the email body presents a sense of urgency in the attempt to resolve a state that could get worse without the victim's interaction. The situation causes a sense of trouble which the user has to handle. In fact is the panic of the moment that leads the victim to act instinctively not respecting a natural security protection.

The email message pretends to be authentic. In fact, the authority is due to the trusted source: the hacker uses the spoofed identity of the bank, in addition, he copies contents such as texts, logos, images and styles used on the legitimate website so that it looks like the truthful. People will tend to obey an authority figure without thinking so much about the legitimacy of the requested actions.

Even if this situation is tricky, the victim has to avoid his smartness and enter in an ignorance area. To get the login credential, the user has to believe that this is an actual email. It's not possible that your bank reports a suspicious activity by email in this way. If they really suspect that there is something anomalous in your management, probably there would be a

different approach. Anyway, there is nothing strange in 4 withdrawals if you are allowed to access that sum. You could be on holiday in a specific country, and your bank has no reason to warn you. The email triggers the instinctive reaction of the victim. In fact reading that someone, who is supposed to be you, takes your money from a different and far country makes you worry and focus on the alarm.

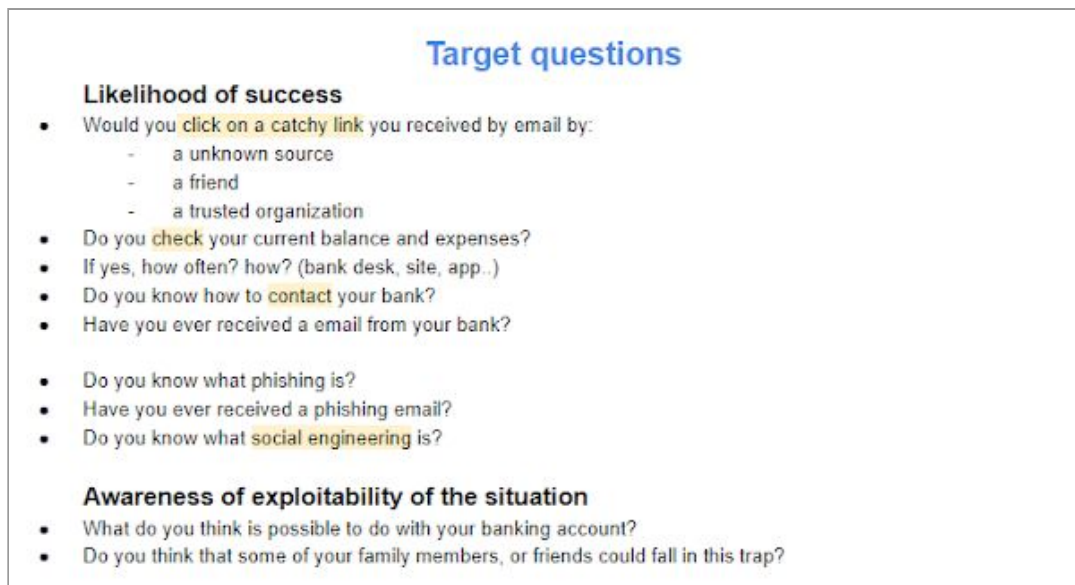
## Interviews

In this section three interviews are presented. In particular, we want to diversify the target in order to inspect and analyze different outputs, then we selected these three people (according to our possibilities and contacts):

1. SU student, M, 22 years old
2. An Italian bus driver, M, 51 years old
3. Accountant, F, 32 years old

The recruitment of people took place with the excuse of a research on the opinion and the use of online banking. We told them the real objective after the interview so that they were not induced to focus on security.

The target questions are reported in *Figure 1*.



**Target questions**

**Likelihood of success**

- Would you click on a catchy link you received by email by:
  - a unknown source
  - a friend
  - a trusted organization
- Do you check your current balance and expenses?
- If yes, how often? how? (bank desk, site, app..)
- Do you know how to contact your bank?
- Have you ever received a email from your bank?
- Do you know what phishing is?
- Have you ever received a phishing email?
- Do you know what social engineering is?

**Awareness of exploitability of the situation**

- What do you think is possible to do with your banking account?
- Do you think that some of your family members, or friends could fall in this trap?

Figure 1 - Target questions scenario 1

## Results

The interviews lead to different results.

The youngest interviewed person was the student. He generally checks the balance and his bank transactions through the app downloaded on his phone. He is trained to understand how he could check easily his account. Probably an email with wrong transactions will result immediately fake for that reason. In addition, he receives a phone message every time he makes a bank debt. He seems also prepared for this kind of attacks. He knows what phishing is and in the past, he has received many untrusted emails. He explained also his spam filter in the email box, so he usually skips email like this in an automatic way. He didn't know the expression social engineering, but talking about it he recognized the manners and some attacks. He appears really advised about IT attacks by emails. He usually does not trust an unknown source, but he could trust friends or known organization. Therefore, the fact is that usually he is in contact with friends, and he knows what to expect from the main organizations. After all the conversation, explaining the scenario, he admitted that it could be difficult to recognize a well-counterfeited source. In this way, the fake bank address could be seen as authentic. But the body of the email is telling something that can't be believable. The first reaction would be to check instantly in his app, in fact, he thinks that he would see the email from his phone and he would skip the false bank link. In the case he would open the email from his computer, he admits that he could open directly the link in order to verify. That's because he thinks that it is not so probably even receive the email in his principal box, instead of in spam. He said that probably his parents as example would fall in this trap and would open the link without reasoning so much: the emergency of the situation would act as an enhancer.

The second interviewee is an Italian middle-aged bus driver. He admitted that he is not a computer expert. He never used internet banking neither from the mobile phone, neither from a computer. His bank sends him his balance and transactions report monthly by traditional mail and he always checks the balance but not all the expenses.

He has an email account and he knows how to check his emails but he seldom does it.

If he received an email of that kind he might believe it and he would be scared because he has all his savings on his bank account. By the way, he would probably ask someone to help him to solve the problem it. So he would be a possible target but he would probably avoid the trap by luck if the person he will ask help from will detect the fraud. When we talked about phishing and social engineering he appeared confused. He didn't know anything about this topic and after an easy presentation, he appeared more scared than aware.

For last, we interviewed an accountant. The woman sends and receives many emails every day. She is aware of phishing. She would click on a link she received from a trustable source, or from a friend if the text is convincing. By the way, she doesn't even open emails from unknown, especially when they have a really appealing object. She knows these emails are very likely to be fake, but she feels protected because she says that she has a good antivirus. She knows something about computer security but probably she feels too

confident just because she has an antivirus. She is not aware that there are threats from which an antivirus cannot protect her.

She knows about the existence of an app but she does not use it and she never downloaded it. She usually does not even login in her internet banking account, except on some occasions. She said that she trusts enough the strength of her bank and she wants to rely on that.

## Discussion

What we did not investigate in the scenario is actually the starting point. How can an attacker get to our email?

In reality, there are many sources to draw from. First of all, newsgroups are chats in which millions of users connect every day. Spammers use programs that enter the pages of newsgroups and chats, simulating what a normal user would do, with the difference that they memorize every email address they find on the screen.

Another way to search for email addresses is through Spambots, that is, programs that search all over the web for words that have within them the @ symbol that indicates almost unequivocally an email address. Another alternative is to persuade people to register on sites, obviously typing their email address.

One of the latest inventions of spammers is to use the big dictionaries of the largest mail servers in the world (Yahoo, MSN, Gmail). Using appropriate software they can connect to these servers and begin to submit emails using names generated randomly. If the server discards the email it means that the address entered is non-existent. If it is accepted by the server, the spammers add it to their list of valid addresses.

Moreover, during the registration on some sites or the purchase of products, the pages often contain a checkbox requesting authorization to send advertising emails. Very often the checkbox is not noticed by the user (because it is placed at the end of the page or in less visible areas of the site) or is preset so that the user does not notice and implicitly give permission. In this way, without knowing it, people authorize Spammers to use their email box and begins to receive emails.

The most famous email servers already have a setting to discard spam messages. We can filter the subject of the email and discard it if it contains terms that we think are used by spammers (Example: Sex). We can define IP addresses as spammers and discard any mail received from these addresses regardless of the terms contained in the text and the object. To avoid being filtered, they use synonyms or acronyms (for example S-E-X instead of sex) that are not detected by the anti-spam software. To prevent their IP from being reported, they change it quite frequently and in this way they evade the problem.

An idea of Spammers is to use viruses (such as the famous SOBIG) that once activated on the victim's PC, use his address book to send spam emails. The result, in this case, is twofold, spam occurs and each of the recipients, in turn, becomes (and unbeknownst to it) a spammer as soon as the virus is activated.

Ultimately massive virus attacks are being carried by spammers to antispam sites. Sites such as Anonymous Postmaster Early Warning System (apews.org) or Spam Open Relay and Blocking System (sorbs.net), which provide the blacklist IPs mentioned above, have declared suffer repetition attacks on their servers and often have to close down their services to prevent a virus from infecting them. The solution that many large companies are adopting is to no longer provide their email address but to fill and send users a special form. So we assume that in this scenario, the attacker has thought about how to get the desired victim's address and not to end his email classified as spam.

So we assume that in this scenario, the attacker has thought about how to make sure that his email is not classified as spam.

The false banking address must be credible, so as to gain confidence. A victim like our first interviewee, the student, will not suspect because the email has not been discarded from his spam system and the address it comes from seems reliable. This attack would not succeed with this interviewee because of his habits: he is used to check his bank account with the phone app. It is unlikely that the student would open the email from the computer, believe in the text or is not sure about the message so that he clicks the link to check.

The most unaware interviewee is the bus driver, but his ignorance in computer and technology saves him from the attack. It is even difficult to open the email since he is not comfortable with that system and he receives his balance by traditional mail. Probably it would be another person to check the email, so it is not easy to understand if that victim could be hacked. The third victim is probably the easiest to attack. She feels very confident and thinks she is protected sufficiently. If the mail arrives in the main mailbox and is not discarded in spam, she thinks it is safe. In addition, the address seems truthful, she would probably believe in the content of the message and check it. She probably would open the link, because it is the easier way to verify immediately. The sense of urgency and the trust in the authority are maybe the feelings that make her proceed. The most worrying thing is that she thinks she is aware of every trick and in this way she doesn't pay attention.

So, what we got from our results is that that social engineering is not well known. Also, internet security is a topic that most people learn by themselves, but are not expert. Even worse, sometimes they feel confident, even if they don't know much about IT security. By the way, this scenario had as target ordinary people, who do not work with computers. So we did not expect them to have ever received training. Nevertheless, nowadays IT security attacks in general and also social engineering are a serious threat, because we have a lot of personal information stored on the computer, and also bank accounts. Given the evolution of the IT sector, it would be good if someone took charge of educating people about the risks involved. To reach the biggest number of people the state should take responsibility for introducing compulsory computer security courses from the first years of school. Obviously, with this approach, you don't reach the adults, but if it's carried forward in the long term it would be a good investment.



## Social engineering scenario 2

### Scenario description

A student wants to access a teacher's account to inflate his grades (and to profit, possibly increasing those of others). In order to do this, he tries to circumvent a secretary by using social engineering to obtain the professor's password.

To make sure that the professor will not be aware of the intrusion, the attacker must then persuade him that his password has been reset.

To better define the scenario we report the attacker's plan.

- **phase 1: connection**

Enter the office and identify a potential secretary. Start to know him by pretending to chat randomly (out of work).

- **phase 2: trust**

Gain the secretary's trust meeting him around the office, pretending to have met by accident. During these meetings, chat in a friendly way and introduce yourself as a Ph.D. student who works closely with the target professor. Try to gain more and more trust and if possible invite the secretary to have lunch together and pay for him, so as to make him feel in debt. During all the conversation mention the target professor in order to make it clear that you work with him and you have a trust work relationship.

- **phase 3: attack**

Show up in the secretariat when the victim secretary is on duty and say that the professor had some kind of family problem and moreover he lost the password and then sent you to reset it. Theoretically, the employee should say no but the relationship of trust created and his feeling in debt could lead him to a light-minded decision. If the preparation is done well, with some luck the victim will reset the password and give the hacker a new one.

- **phase 4: profit**

Now the attacker can exploit the professor's account to inflate his votes, and maybe also sell votes to other students. This phase should be done as quickly as possible in order to proceed with the next step and cover his tracks.

- **phase 5: vanish**

The goal seems to have been reached but in order not to be discovered, one last step must be quickly performed. The attacker creates a fake email account with a name which looks like the university's secretaries. Using this account he sends an email to the professor, claiming to be a secretary who informs him that for security reasons his password has been changed. The email contains the one-code password used by the student to access the professor's account. The professor will be likely to believe that the mail is reliable because the new password will give him access.

## Scenario analysis

This plan might sound like something that couldn't happen in real life. Nobody thinks that this could happen to themselves, but there have been cases in which social engineering leads people to even more inconsiderate actions. We should remember that humans, as opposed to machines, have feelings that could lead them non-rational choices.

The psychological artifices involved in this attack are:

- *Trust in a friend*
- *Sense of empathy*
- *Reciprocity*
- *Ignorance*
- *Trust in authority*

This plan allows the student to access the professor's account without using any IT tool.

The attack is based on the circumvention of the secretary, achieved by establishing a trustworthy relationship.

The attacker focuses on the human factor: it is about manipulating people so that they voluntarily do something or give away their confidential data. Obviously, the success of the attack depends strongly on the ability to persuade, on the care in seduction and on the cunning of the student in making himself credible.

The secretary will be more likely to cooperate because the attacker is now a friend. The student is in a position of credibility and the story that he tells is not doubted. As a friend, the student provokes compassion in the secretary: the attacker must solve a problem and the only person who can help him is his victim in getting the professor's access credentials. If the phase of connection and trust has succeeded well, the secretary will feel empathy towards the student, he could even think to owe a favor for the time spent together and for being friends.

In order to obtain a success, the victim avoids the classic security policy and at that moment his ethics change helping the student he trusts. In a second case, the victim could be actually ignorant about the correct security procedures and he could think that a professor's assistant can legitimately get that information.

We should consider that also the professor himself will be circumvented in the last part of the attack. In fact, he will receive an email that provides a new password. The professor should be worried about this unexpected mutation but he maybe ignores the correct procedure in changing the password. Moreover, he trusts in the authoritativeness of the sender and he does not pay attention to details if the provided password actually works.

## Interviews

In this section three interviews are presented.

In particular, we have two clear target to investigate and analyze:

1. Secretaries, that could be related to receptionists too
2. Professors

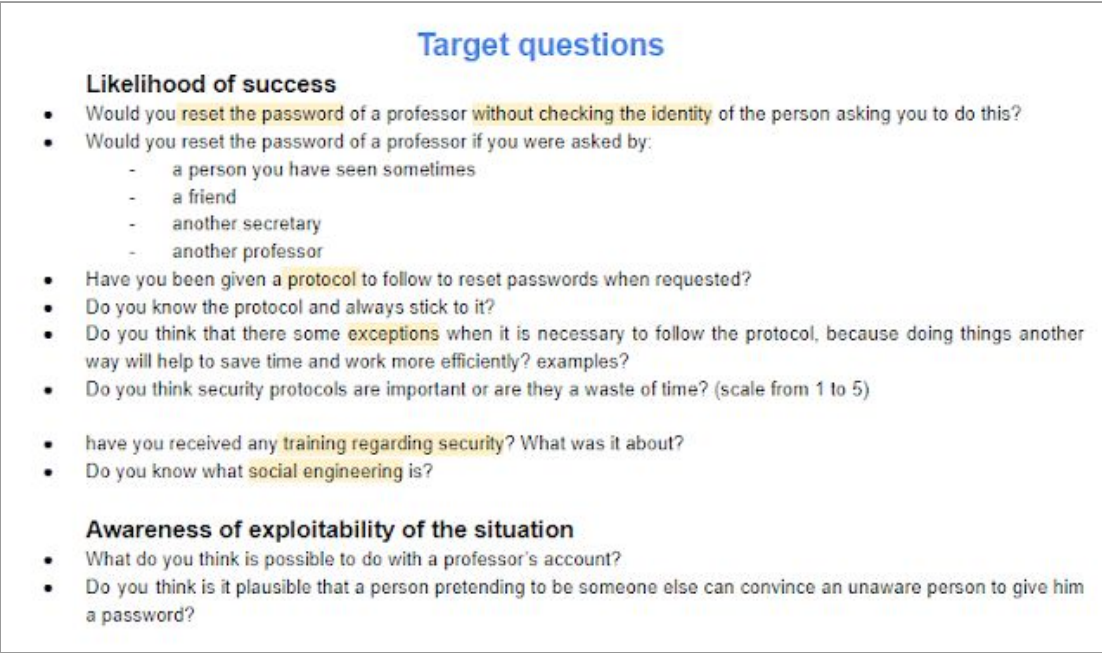
In this study, we focus on the first target because it is the victim who plays the major role. The professor is cheated to not discover the attack, but he is not the person who provides information. The role of the secretary seems to be more interesting, in fact it has more psychological implications and actions.

The recruitment of people took place with the excuse of a research about the trust between colleagues. In order to make sure that the interviewee feels comfortable and free to express himself, we started the approach with some easy questions. In addition, we presented some situation of trust in which the person has to identify himself and imagine a reaction. Therefore, we started our target questions in order to understand more about his awareness and responses to the topic.

So that we could understand more about the implications of the attack to the victim target 1, we interviewed three different people:

1. Secretary of an IT company 42 years old
2. Italian university secretary, 58 years old
3. Gym receptionist, 29 years old

The target questions are reported in *Figure 2*.



**Target questions**

**Likelihood of success**

- Would you **reset the password** of a professor **without checking the identity** of the person asking you to do this?
- Would you reset the password of a professor if you were asked by:
  - a person you have seen sometimes
  - a friend
  - another secretary
  - another professor
- Have you been given a **protocol** to follow to reset passwords when requested?
- Do you know the protocol and always stick to it?
- Do you think that there some **exceptions** when it is necessary to follow the protocol, because doing things another way will help to save time and work more efficiently? examples?
- Do you think security protocols are important or are they a waste of time? (scale from 1 to 5)
- have you received any **training regarding security**? What was it about?
- Do you know what **social engineering** is?

**Awareness of exploitability of the situation**

- What do you think is possible to do with a professor's account?
- Do you think is it plausible that a person pretending to be someone else can convince an unaware person to give him a password?

Figure 2 - Target questions Scenario 2

## Results

To analyze this scenario, the first person we interviewed was a secretary in a small IT company. This woman does not produce a password for users, so we tried to inspect how easily would a malicious person gain her trust, in order to use her computer.

She relies on the IT knowledge of her colleagues everytime she has difficulty in using any technological device. When for example she cannot print document she checks for basic problems, like the absence of sheets. But if she is not able to solve the problem she asks someone for help. The office is small, so everybody knows each other. She trusts anybody inside the company and she would let any of his colleagues to use her computer, even in her absence. The only person she wouldn't let use her computer to help her are the ones that she thinks that would not be of any help.

She received an IT security training during her first year of work and she says that it was helpful because she did not know much about it before.

She did not know what social engineering is. When we explained it, she said that she had heard of some tricks of this kind used for unbelievable threats. However, she thinks that this is a limited phenomenon, used only by professionals, who hunt for big targets. So she believes she is not a potential target of social engineering.

The second person we interviewed in this section was a secretary in our Italian university. She said that she knows security protocols and she usually sticks to them. She told us that she knows that they are important in her job, but she said that a smart secretary knows when sticking strictly to the protocols is just a waste of time. Furthermore, she admitted that sometimes she doesn't follow the protocol to be able to complete more tasks in less time. In fact, she also said that if she never did so, she wouldn't be able to do her job during her working time. For example, she said that she would probably skip the bureaucratic part and give directly the needed information to a friend or to another secretary, as she trusts them. On the other hand, she wouldn't help a person she never met before, who claimed to be a professor, without asking for his ID.

She never received a training about information security but she knew something before starting to work as a secretary at the university. While waiting for official training, she was educated about computer security by a colleague during the first month of work. By the way, she is working as a secretary at the university since 1998 and still, she didn't receive any IT security training from the university.

The gym receptionist actually seems to be less worried about possible attacks, and it sounds reasonable because his main task is to give people access to the gym. By the way, if a stranger accessed the gym illicitly it wouldn't cause much damage to the business, except the fact that he is accessing the service without paying for it. But we should also consider that in his computer he records and administrates personal information of users. A malicious person might want to access the customers' sensible data. When we mention the customers' data the receptionist seemed aware of the confidentiality of personal data and he said that he wouldn't share this information with anybody, except the manager.

By the way, when he doesn't have any mansion to do, (especially during the night shift) he surfs the net to kill time. He doesn't think that this might open a breach in the security system.

He did not know what social engineering is and even after we explained this phenomenon he seemed reluctant to believe that something like this could happen to someone.

## Discussion

The people we interviewed in this second scenario usually work with a computer. So we expected them to be at least more acknowledged about IT security. By the way, this wasn't always the case. The university should invest money in training all its employees on IT security and social engineering attacks. Spending money in this area will let the University save all the money that could be lost in case of a successful attack. Especially if we think of the fines provided for by GDPR, if an intruder could steal personal data the University might have to pay an expensive fine.

The secretary of the company was trained about IT security and has many colleagues she can rely on. Trusting your colleagues and let them help you can be really useful, but it might also be a weakness. If one of her colleagues wanted to access the woman's computer for illicit purposes, it would be very easy. The secretary should be careful. what we advised her, was to always be present when a colleague fixes her problem. In this way, observing how the problem can be solved, she can learn something new, and at the same time check that the colleague does not take advantage of her computer for illicit uses.

The gym receptionist's task that we focused on is recording, saving and modifying the customers' data in order to investigate the scenario. He was completely aware of the confidentiality of these data and he claimed that he wouldn't share any personal information with anybody else than the customer itself. He knows how the protocol works. Basically, he has to ask for ID before access and refer to the personal page of a customer. Maybe he is not an expert in IT security but he would not be an easy target for a social engineering attack if he said us the truth.

## Other studies

Interviews can be just seen as an example because they are too few to be generalizable and people have been chosen according to our possibilities and contacts. In addition, it is difficult to interview a person in this way and get completely honest answers. People are unwilling to admit inconvenient truths, they often try to look good. Sometimes it is difficult to get confident and let them trust us. Finally, Asking people how they would behave in real life doesn't always give the same results that you could get if you put those persons in that situation for real. Furthermore is not easy to understand how a person would react to a specific situation, like the one we set up.

To better understand the likelihood of success of a social engineering attack the best way is probably to simulate the described scenarios. Obviously, there is some ethics implication. In addition, the second scenario takes a very long time to implement, but the first scenario might be put into practice easier on a large number of people. In fact, once you develop it, it's easily replicable on more targets with little effort. By the way, we didn't implement it, even if we wouldn't really save people's password we wouldn't feel comfortable doing it.

Other studies have been done following this approach and they lead to alarming results.

In a study included 1000 American people conducted by TNS Global for Halon in 2013, an email security service, the results show that 30% would open an email, even if they were aware that it contained something suspicious. This percentage may seem not so high, but we must consider that an attacker does not have big costs: it is important to remember that for a success all he needs is one victim with a vulnerable browser that gives the access. 30% is still a very strong percentage that needs to be decreased.

Halon's North American CEO and co-founder, Jonas Falck, alarmed "Spam email is an unfortunate fact of life in the computer age. Users have become more aware of the threats they face, but spammers have also become craftier in disguising these messages."

A different study by researchers of the University of Luxembourg tested how likely people were to give away their password to strangers.

The interviewed people were willing to share their passwords with strangers just because they had clothes that made interviewees believe they belonged to a reputable organization. Furthermore, when they were given a little incentive (some chocolate) they were even more likely to give their password. When people were not given chocolate 29.8% of them shared their password with the interviewer. If people were given chocolate the percentage raised to 43.5%. The study was focused on underlying how reciprocity can be used in social engineering. Even a simple incentive like chocolate made people more inclined to share their password with a potential attacker. In addition to showing how effective this system is, the results reported by the group that had not received chocolate are also alarming. This study underlines how easily a social engineering attack can be performed.

Another study commissioned by Check Point at Dimensional Research in 2012 revealed that 43% of the 853 IT professionals around the world state that they have been targeted by social engineering attacks. The survey also found that new employees are the most susceptible to attack, in fact, 60% of interviewed answer that they classify inexperienced colleagues as high risk in social engineering. Unfortunately, training does not seem to be in step with threats since only 26% offer regular training, while 34% say they have no education on their employees for that topic. People need to be trained and informed about social engineering attacks and they need to understand their security policies.



## Conclusion

Social engineering is a real risk, also because not everybody is aware of its existence. Our interviews show some experience of people that could be possible targets of social engineering if the attacker is able to exploit their unawareness and ingenuity.

In the case of the first scenario, the victims are customers of a bank, so the bank itself should take care of its clients. Informing the customers about social engineering and the risks connected would make them more likely to avoid this sort of tricks. Whereas people tend to underestimate the dangers of these attacks, it would be good to report previous cases emphasizing the severity of the loss suffered by victims of this type of attack.

It is also important to inform customers on which contact methods the bank uses. We assume that the bank would contact its customers by phone in the event of suspected fraud. The clients should be aware of that. And they should also be encouraged to call the bank themselves, if they receive important or unexpected communications that could be malicious.

The second scenario describes a situation less linked to technology, instead, it is based on manipulation and victim psychological vulnerabilities. The success of the attack depends strongly on the ability of the attacker to become credible and gain confidence. Information is obtained with the consent of the secretary, that does not suspect anything. A trick is applied to deceive the professor that needs to be informed about the password change. It is important to respect protocols that are given and always check the identity of the person asking for something without thinking it obvious. Security policies exist to ensure the secrecy of information too. It could be really useful to teach workers about the possible attacks related to the company or the organization. In addition, we need to sensitize about the severity and the damage that an attack can bring.

Our exploratory study underlines how social engineering is a theme that is only dealt with by some companies. And, except sometimes from their work, the most part of ordinary people did not receive any education about social engineering. The youngest persons we interviewed seemed more aware of some social engineering techniques like as phishing. By the way, also their knowledge of the subject was often limited.

Therefore wider instruction of the risks of social engineering would be needed, both in companies and for everyday life.

To conclude, the greatest weakness of the victims of this kind of attacks is their unawareness.



## References

Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies. **Security in Computing (5th Edition)**. Prentice Hall Press, Upper Saddle River, NJ, USA, 2015.

Christian Happ, André Melzer, Georges Steffgen. **Trick with treat – Reciprocity increases the willingness to communicate personal data**. *Computers in Human Behavior*, 2016.

### Websites:

[https://en.wikipedia.org/wiki/Social\\_engineering\\_%28security%29](https://en.wikipedia.org/wiki/Social_engineering_%28security%29)

<http://www.sorbs.net/>

<http://www.apews.org/>

<https://www.corrierecomunicazioni.it/digital-economy/social-engineering-all-attacco-della-mente-umana/>

<https://news.softpedia.com/news/Study-Shows-What-Types-of-Malicious-Emails-Men-and-Women-Are-More-Likely-to-Open-379023.shtml>

<https://halon.io/blog/>

## Time summary

Choose scenarios : 5 hours

Scenario 1 interviews: 10 hours

Scenario 1 results: 2 hours

Scenario 1 discussion: 5 hours

Scenario 2 interviews: 12 hours

Scenario 2 results: 3 hours

Scenario 2 discussion: 3 hours

Other studies: 5 hours