Social Engineering

Tuğberk Kocatekin, Ph.D.

Spring 2023

Contents

1 Introduction

- Social engineering is a tool. It can be used for good and bad, just like everything else.

- Knowing that is also good so that you can secure yourself to social engineering attacks.

- A very good book on the subject is Kevin Mitnick's **A Ghost in the Wires**. A definite recommendation!

- Cost for a social engineering attack is very low. Risk is even lower if you are careful. But the potential payout is very big. A very big percentage of attacks has a social engineering element to them.

- A social engineer tries to make you make a decision without thinking about it. If you think, you will understand that you are being manipulated, attacker doesn't want this. It is about psychology. Research nudge theory and behavioral psychology. It is the same with advertisements. They would show you stuff which would trigger your emotions and later will ask you to make a decision. It is common in social engineering too.

- Definition: Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests. [1]

- Oxytocin is the hormone and is very related to trust. Oxytocin is released not just when we trust someone, but when we **feel** that someone trusts us. This is being used by those who apply social engineering.

- Social engineering attacks can be divided into four vectors: SMS Phishing, Voice Phishing (Vishing), Phishing, Impersonation. Sometimes social engineers like to do combos, combining multiple of these vectors.

[1] Social Engineering: The Science of Human Hacking by Christopher Hadnagy

2 OSINT

- Short for Open Source Intelligence. Information is very important in social engineering, therefore getting and obtaining information is crucial as well. When you want to impersonate someone, you need information on those people and Internet is vastly big. This is also important to show you that you should not put every information about yourself online. Applications and software tried to do this especially with Facebook, Foursquare, etc. Making us select every movie we like, every place we go, etc.

2.1 An example of OSINT

- At one time, someone wanted to find whether a former FBI director James Corney had any social media accounts. It was not public knowledge whether he had one or not, probably if there is it was not in his own name. So, the story enfolds.

- Researcher listened to the interviews and talks Corney gave. In one of them, he stated that he had Twitter and Instagram accounts. That is good for the researcher, because now instead of dozens social media, she can concentrate on just two.

- However, she could not find a Twitter account in his name. But, she found one for the director's son. Okay, how to understand if that is the son? Well, by looking at the account. He congratulated his father once. From there, she thought to look for the Instagram account for the son. It was locked.

- However, when you send a friend request, Instagram tries to help you by showing relevant accounts in order to help you befriend people. If you know this person, it is possible that you can know *these* too. Well, Instagram suggested number of people and one of them was **reinholdniebuhr.**.

- When you do internet searches by that name, you can learn that he was an American theologian and political commentator. However, he died in 1971. A little more research showed that actually former director did a study and wrote a paper on Reinhold Niebuhr!

- With that information in hand, researcher checked out Twitter and found seven accounts using that name. Of all, there was one with the handle @ProjectExile7. A little more research showed that "Project Exile" was the name of a program which former director started when he was a US attorney.

- All of this is found in legal ways, by OSINT.

2.2 Nontechnical OSINT

- When you gather information without using computer or using nontechnical means, it is nontechnical OSINT. It is about **observational skills**.

- For example, if you want to enter a place you do not need a computer. You need to observe everything. What are people wearing? Are they using a card or a passcode to enter a building? Are there security cameras? Is security personnel working correctly or just playing with their phones?

- Remember when we said physical security is also very important. This is an example. Kevin Mitnick actually demonstrates some of these attacks online, which can be found in Youtube. For example, for a certain type of entrance card, they can remotely copy that card while they are standing next to you! If that is possible, maybe you should not put your card in your front pocket!

- In real life, not everything goes as planned. You need to be ready to act and talk. That is why everything you see, every information you gathered is very important. You should keep all that in mind ready to use.

- For example, many people share their work places or pictures about their work on Instagram. Sometimes it is very easy to understand which OS they use, what are the programs they use. Maybe they even write their password information on a piece of POSTITS. In short, don't share pictures like that. Do not try to give information about yourself!

2.3 Technical OSINT

- There are a lot of applications for OSINT. Some of them can be found in Kali Linux OS. However, applications themselves are not going to be enough. As shown previously, nontechnical OSINT is also very important. A simple Google search can give some websites.

- Social Media is very crucial in OSINT. They are here and not going to leave. However, we can still make sure we are not sharing unnecessary information on them. People do! If you want to store information on people, make sure you are not using cloud and store them in a secure way.

- Social media gives a lot of information about us. Linkedin gives us the information of our work related acquaintances, our work places etc. Facebook gives us information about our favorite media stuff, our friends, vacations, places, etc. Twitter gives information about our location, our emotional state, what we are doing at that time, etc.

- Google-fu! Learn how to use google. intext, filetype, inurl, cache, info, site. There are a lot of keywords which can help narrow down your search. Many websites were hacked because of Google-Fu.

- IoT devices are very important. Many people buy these devices and since they were not regulated and had bad password practices, it was possible to exploit them. Some people used generic usernames and passwords.

- Whatever you buy, you must change your default username and password on the machine. It doesn't necessarily mean it is going to be secure, but it will be more secure.

- When you are designing systems, make sure that you actually **force** the user to change the generic username and passwords. These are very good attacking points for malwares and making IoT devices into Bots.

- Webcams are such devices. If you just connect them to the Internet with the default username and password, people can connect to those devices and see them online. This would be very helpful for burglars! Google fu can help you find such webcams!

- Your photos also have some metadata. Metadata means data about data. When you upload a picture to the internet, it is possible even to find your coordinates. Even if the image does not store the coordinates, there are websites which can find where you are by checking the image.

- Let's say you are a VIP. You are sharing photos and stuff all the time with the people on the Internet. Now, we can learn where you go to everyday, where are your favorite restaurants and places, and maybe even your address.

2.4 Robots.txt

- The way search engines work is by using robots. These robots crawl and scrape the websites. However, there is a file called robots.txt which gives information to search engines. For example, sometimes they put Disallow which means robots are not given permission to cache that folder.

- These files also can give information about a website. For example by looking at a robots.txt, you can find out which software they are using for their webmail or their website. Later, you can check for exploits on those software, and if you are faster than them; maybe you can infiltrate.

3 Types of attacks

- Pretexting, Phishing, Vishing, Smishing, Baiting, Scareware, Ransomware, Dumpster Diving, Shoulder Surfing

3.1 Pretexting

- It means becoming anyone you want to be. You present yourself as someone else to obtain private information. It is more than a lie, it involves creating a new persona.

- Improvisation skill is good and needed for this job. Education is not enough, one must have experience. A method acting or improv class can help. You need to be good at communication.

- If you are trying to be someone else, you need to know a lot of details about that line of work. Kevin Mitnick was an expert in phone systems, therefore he can easily get in the role of a phone compnay technician.

- Not easy to do. Try to imitate real life people. If you have a son, do not try to lie as if you have a daughter. You should also not forget the things you said even in short term.

3.2 Phishing

- An attack used to steal user data, login credentials, personal information, credit card numbers etc. In order to do phishing, the attack poses as a trusted entity. The victim is tricked into opening an email or a file.

- Some of these attacks target those who are not tech savvy. They can show notifications similar to ones we know, saying that you win a prize. At the end, they want your credit card number to do a provision. Then, it is too late.

- Sometimes the attackers will use the sense of urgency. They will say there is a deal for a limited amount of time. Or they can say until you do something in X amount of time, your credentials will be deleted! An example can be user information update. They may send you a fake website where you write all your information again.

- They can create fake websites where you enter your login credentials. They can even buy certificates and domain names which are similar to the original domain to trick you. Using mobile applications for some tasks is better. These are usually done on the web.

- They use attachments and trick you into downloading them. They can contain ransomware, malware or other stuff. Generally, it starts by sending an email!

3.3 Vishing

- It is voice phishing. There are different versions. There can be a real life person on line to talk to you or maybe they can use pre-recorded voices. In Turkey, they claim that they are law enforcement and they also claim that your name is involved with terrorism. In order to delete your name, they ask money for it.

- In abroad, there are a lot of computer scams where they claim they want to help you secure your computer. They call you and want to connect to your computer in order to check whether your computer is secure or not. By doing so, they can access your computer and later ask for money. There are a lot of youtube videos about these scammers.

3.4 SMS Phishing

- Scammers can also send SMS to you claiming to be someone else. Do not forget that they will want to use what you hold dear. Maybe they will say that you did not pay your bill and will give you a web address. When you click, it will go to a similar website and will ask for your user credentials.

3.5 Baiting Techniques

- Attackers would put down USB drives, download links claiming to be free movies, music etc.

- They would sell something very cheap compared to the original price.

- These are too good to be true!.

3.6 Dumpster Diving

- Attacker can dig through the trash looking for important information about a person or a company. It would be good to **shred** documents instead of just trashing them.

- Especially efficient in the old times. Maybe everything was documented physically. It is possible that you can find a pattern in the files.

3.7 Shoulder surfing

- It means looking over a person's shoulder to gather personal information.

- It is very easy nowadays. If you are in a bus or a crowded place, one can easily see what you are writing to your friends. They can also know your facebook, instagram and twitter handle.

- It is even possible that someone can memorize your cc number by looking at it while waiting in the line!

4 Defense

4.1 Against pretexting

- Never give out private information about yourself or anybody else over the phone or internet.

- Legitimate organizations are not going to contact you and ask for your password. In other terms, never give out your password. It would be even better if you even don't know it yourself.

- If you think it is possible that someone is trying to get information from you, end the conversation. You can also inform the real company about this event.

4.2 Against phishing

- Do not trust anyone just because they said so.

- Do not open links or attachments from people that you don't know. Also, be very careful even if that someone is someone you know, because it is possible that they hacked him/her too.

- Do not enter personal information on any screen you see. Make sure you are in the right website or software.

4.3 Against Baiting

- Do not click links you don't know.

- Use reputable websites to buy genuine stuff. If it is too cheap, think again.

- Do not use untrusted websites to download any software, etc.

- Do not stick any USB or external device to your computer. If you must, use sandbox.

4.4 Against Scareware

- Always keep your system updated. Antivirus, operating system, etc.

- Use necessary browser extensions such as AdBlockers, uBlock Origin. Browsers nowadays come with pop-up blockers.

- Be careful with running Javascript code. Client side scripting can be dangerous.