SOCIAL ENGINEERING PRACTICAL - OVERVIEW

JOAS ANTONIO

WHAT IS SOCIAL ENGINEERING?

- Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.
- Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

LIFECYCLE

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

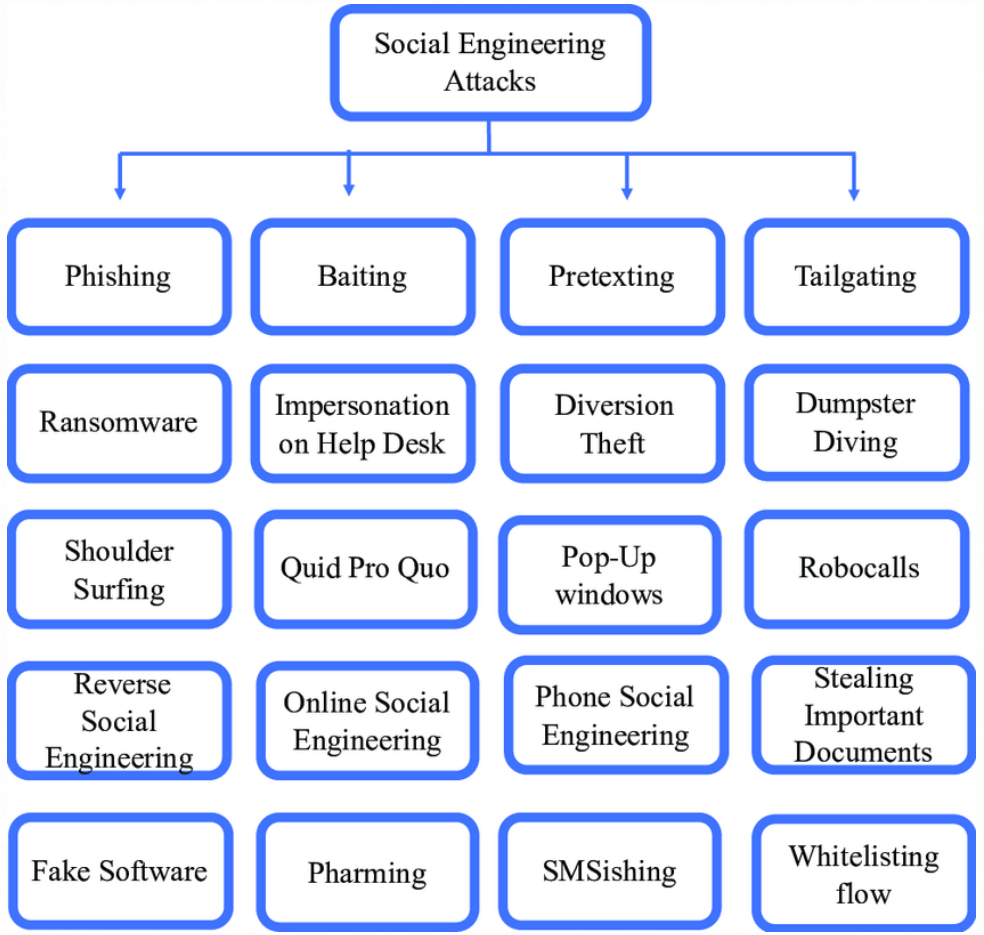
Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

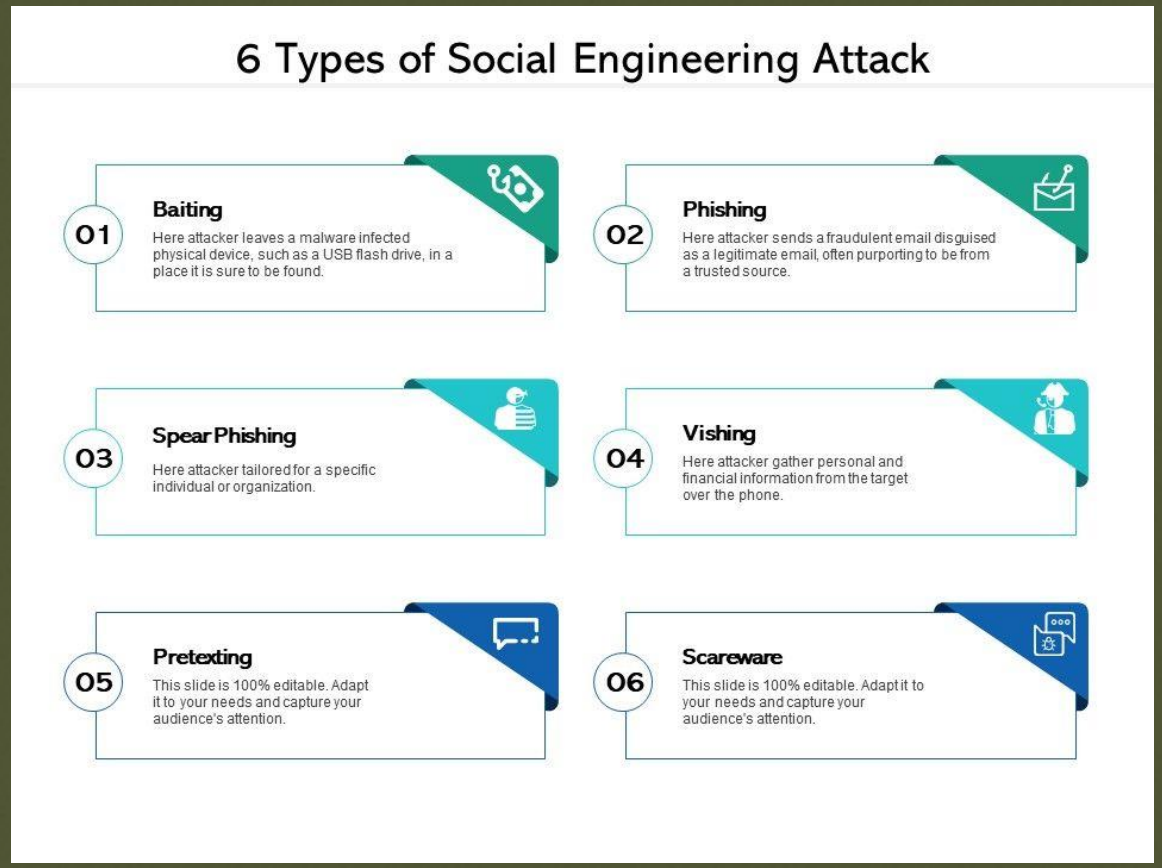
Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

TYPES OF SOCIAL ENGINEERING



6 TYPES OF SOCIAL ENGINEERING



HUMAN DEVICE INTERFACE

- The HID standard was adopted primarily to enable innovation in PC input devices and to simplify the process of installing such devices. Prior to the introduction of the HID concept, devices usually conformed to strictly defined protocols for mouse, keyboards and joysticks; for example, the standard mouse protocol at the time supported relative X- and Y-axis data and binary input for up to two buttons, with no legacy support. All hardware innovations necessitated either overloading the use of data in an existing protocol or the creation of custom device drivers and the evangelization of a new protocol to developers. By contrast, all HID-defined devices deliver self-describing packages that may contain any number of data types and formats. A single HID driver on a computer parses data and enables dynamic association of data I/O with application functionality, which has enabled rapid innovation and development, and prolific diversification of new human-interface devices.

BAITING

- Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that malicious actors use to entice victims. Baiters may leverage the offer of free music or movie downloads, for example, to trick users into handing their login credentials.
- Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media.

- https://www.youtube.com/watch?v=6HghzgPNIiA
- https://www.youtube.com/watch?v=Iot9pR4t1bY
- https://www.youtube.com/watch?v=M6bhXx75RMs

BADUSB

- BadUSB is an attack that exploits an inherent vulnerability in USB firmware. Such an attack reprograms a USB device, causing it to act as a human interface device; once re-engineered, the USB device is used to discreetly execute commands or run malicious programs on the victim's computer.
- The BadUSB exploit was first discovered and exposed by security researchers Karsten Nohl and Jakob Lell at the 2014 Black Hat conference. The BadUSB code is currently available to the public via the code sharing site, Github, meaning that anyone—even those with little or no expertise—can launch a full-blown BadUSB attack.

PHISHING

- As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing 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 on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.
- https://www.youtube.com/watch?v=3u5G_tmrwi4
- https://infosecwriteups.com/sending-emails-using-social-engineering-toolkit-setoolkit-97427712c809

SPEAR PHISHING

- This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.
- A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

- https://www.youtube.com/watch?v=S6S5JF6Gou0

PRETEXTING

- Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending 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. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.
- All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.
- https://osintframework.com/

SCAREWARE

- Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.
- A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, “Your computer may be infected with harmful spyware programs.” It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.
- Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.
- https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html

VISHING

- Vhishing is a combination of "voice" and "phishing." It’s the phone's version of email phishing, where a bad actor calls instead of emails to steal confidential information. These calls often leverage fear and urgency to get quick, impulsive callbacks.
- https://vimeo.com/340994716

PHYSICAL PENTEST

Physical PenTest

- Physical penetration tests are meant to simulate real-world scenarios to help assess the vulnerabilities and risks that could compromise a company's physical security. Specialists often carry them out in this field who know how to access sensitive information, bypass controls, intercept network traffic and EM waves and more!

- Physical penetration testing is a vital part of any company's security. This article will tell you what physical penetration tests are, why they're important and how to do them.

Physical Penetration Testing Methods and Examples

Tailgating into a facility

- This happens when outsiders hide in another employee's car or vehicle until they reach their destination or enter behind someone else who has legitimate access. Sometimes it is just a matter of asking someone inside the organisation to let them in once they get close enough. Some even find a person getting off an elevator and follow them through the exit door. There are multiple ways based on the physical access controls and awareness of the security and staff onsite. In real crime scenarios, breaking through an open window or door is done tactically to avoid motion detectors.

Lock Picking

- Lock picking is an essential part of physical penetration testing. Testers should look for locks that are most often improperly installed or not used and try to open them. Most popular tools include tension wrench or torsion wrench used to lockpick mechanical locks.
- Flash drives can be plugged into USB ports when employees don't realise it, allowing a test hacker to control computers by using malware-loaded flash drives.
- Blowing up cameras or other computer equipment is too suspicious and leaves people with no doubt about what has happened.

Physical Penetration Testing Methods and Examples

RFID Cloning

- A penetration tester clones RFID badges and uses them to get into areas they shouldn't be in. Criminals can walk up to the door and use a hidden RFID reader to steal employee access. They can then clone the stolen card ID using appropriate equipment, such as an off-the-shelf RFID cloning device. Then, they'll be able to gain access into secured facilities without risk of detection

Physical Penetration Testing Methods and Examples

- Access Control Bypass – Penetration testers look for ways to get past the physical security controls in place, including setting off motion-activated alarms from the outside, using a tool to open doors from the inside or other various methods.
- Bypassing a human firewall – Various checks are included to observe the employee awareness against walks around the facility (different locations include data center, server rooms and sites), open access areas such as kitchen, cafe, reception areas, waiting areas, after-hours check-in.
- Network access – Attempts to access the internal network bypassing security controls, including business-critical assets, once initial access is achieved. It would include access through common areas, meeting rooms, conference halls or places with network access.
- Sensitive data discovery from open areas, desks or other information troves with papers, sticky posts and other visible stationery with sensitive information.
- Dumpster diving is another sub-set of physical penetration testing. In case the organisation has disposed of sensitive information, it might still be found in nearby dumpsters. A dumpster diver can easily access the documents and get a head start on penetrating the network even if it's currently secure. The most common items found during these tests are papers with passwords and personal information such as addresses or home phone numbers needed to conduct social engineering attacks. Other various remnants from lunchtime meals, sticky notes with phone numbers or emails, business cards left behind by people who have visited your facility. You will also find out how well-disciplined employees are when disposing of this type of paper waste from a quick test.
- https://thecyphere.com/blog/physical-penetration-testing/

HARDWARE HACKING

HARDWARE HACKING

- https://medium.com/predict/the-future-of-hardware-hacking-reverse-engineering-be2575d28875
- https://www.youtube.com/watch?v=LSQf3iuluYo
- https://www.youtube.com/watch?v=PYeYxQqBTLo
- https://securityboulevard.com/2019/01/hardware-hacking-101-lesson-1-beauty-your-home-lab-and-basic-electronics/
- https://drive.google.com/file/d/1wrmZ1xlJ_zeZu8PPs1p2cLVBDcN4Pi2u/view?usp=sharing
- https://www.youtube.com/watch?v=aHLJRcI5jcU
- https://www.youtube.com/watch?v=Qn_fhyxdzO8
- https://www.youtube.com/watch?v=HuCbr2588-w
- https://www.youtube.com/watch?v=3AhC46iLRy8
- https://www.youtube.com/watch?v=AQpv_6Se6VM

HAK5 – HARDWARE HACKING

- https://www.youtube.com/watch?v=qsVaC6v3NoU
- https://www.youtube.com/watch?v=LqmVaf2KHYA
- https://www.youtube.com/watch?v=HUzd40arX3g
- https://www.youtube.com/watch?v=4kX90HzA0FM
- https://www.youtube.com/watch?v=nmOTSd7fYdY
- https://www.youtube.com/watch?v=Fk1Bpy5ccPU
- https://www.youtube.com/watch?v=CcnCbxoUWps
- https://www.youtube.com/watch?v=WR5ve7cQEpY
- https://www.youtube.com/watch?v=KX_0c9R4Fng

PRACTICE

SPEAR PHISHING

- https://www.youtube.com/watch?v=oByOp-QCL5o
- https://www.youtube.com/watch?v=u9dBGWVwMMA
- https://www.youtube.com/watch?v=C_Aa1yCPHF0
- https://www.youtube.com/watch?v=r0XRdScQWoc
- https://www.youtube.com/watch?v=Qje-zGcCV6M

VISHING

- https://www.youtube.com/watch?v=xuYoMs6CLEw
- https://www.youtube.com/watch?v=PWVN3Rq4gzw&t
- https://www.youtube.com/watch?v=Hc01oZPvByg
- https://www.youtube.com/watch?v=YnWgvsksLUc
- https://www.youtube.com/watch?v=fHhNWAKw0bY

PRETEXTING

- https://www.youtube.com/watch?v=HfPKe98UqEI&
- https://www.youtube.com/watch?v=nUPkH9yqF78
- https://www.youtube.com/watch?v=BIIvsJ3yi8o
- https://www.youtube.com/watch?v=4rDTnRGmVBs
- https://www.youtube.com/watch?v=j5j6c05Btfc

BADUSB

- https://www.youtube.com/watch?v=e_f9p-_JWZw
- https://www.youtube.com/watch?v=T787I_itGmA
- https://www.youtube.com/watch?v=nuruzFqMgIw&t
- https://www.youtube.com/watch?v=7skDckKti6w&t
- https://www.youtube.com/watch?v=_yJWwKO3_Z0
- https://www.youtube.com/watch?v=LDb1PwAhVkw
- https://www.youtube.com/watch?v=KCFk56-g1wo
- https://www.youtube.com/watch?v=Hn11WpwEk38&list=PLGKwaxWykfnYdiQ5hh9QUHoWg9KweIjgR

AWESOME AND TOOLS

- https://github.com/undergroundwires/CEH-in-bullet-points/blob/master/chapters/10-social-engineering/social-engineering-types.md
- https://github.com/v2-dev/awesome-social-engineering
- https://github.com/topics/social-engineering
- https://github.com/enaqx/awesome-pentest#social-engineering
- https://github.com/infosecn1nja/Red-Teaming-Toolkit