An Overview of Social Engineering

3. Social Engineering Attacks

3.1. Attacks Classification

Social engineering attacks can be classified into two categories: human-based or computer-based as illustrated in Figure 2.

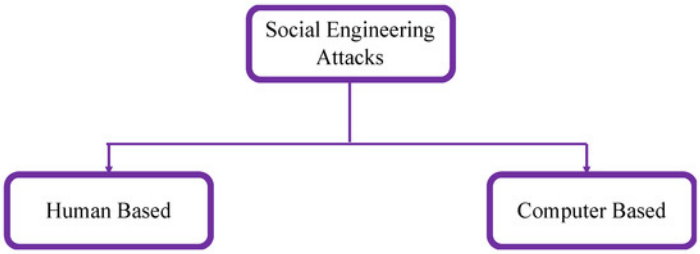


Figure 2. Social engineering attacks classification.

In human-based attacks, the attacker executes the attack in person by interacting with the target to gather desired information. Thus, they can influence a limited number of victims. The software-based attacks are performed using devices such as computers or mobile phones to get information from the targets. They can attack many victims in few seconds. Social engineering toolkit (SET) is one of the computer-based attacks used for spear phishing emails. Social engineering attacks can also be classified into three categories, according to how the attack is conducted: social, technical, and physical-based attacks, as illustrated in Figure 3.

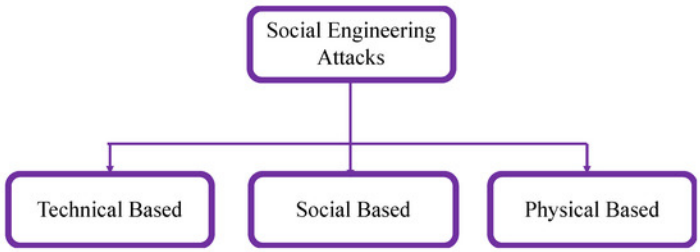


Figure 3. Social engineering attacks classification.

Social-based attacks are performed through relationships with the victims to play on their psychology and emotion. These attacks are the most dangerous and successful attacks as they involve human interactions. Examples of these attacks are baiting and spear phishing. Technical-based attacks are conducted through internet via social networks and online services websites and they gather desired information such as passwords, credit card details, and security questions. Physical-based attacks refer to physical actions performed by the attacker to collect information about the target. An example of such attacks is searching in dumpsters for valuable documents.

Social engineering attacks may combine the different aspects previously discussed, namely: human, computer, technical, social, and physical-based. Examples of social engineering attacks include phishing, impersonation on help desk calls, shoulder surfing, dumpster diving, stealing important documents, diversion theft, fake software, baiting, quid pro quo, pretexting, tailgating, Pop-Up windows, Robocalls, ransomware, online social engineering, reverse social engineering, and phone social engineering. Figure 4 illustrates the classification of these attacks.

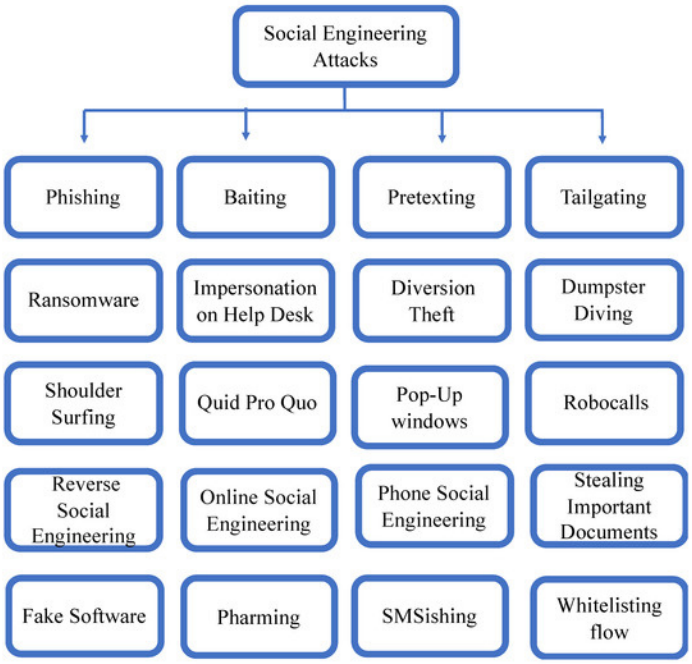


Figure 4. Social engineering attacks.

Social engineering attacks can be classified into several categories depending on several perspectives. They can be classified into two categories according to which entity is involved: human or software. They can also be classified into three categories according to how the attack is conducted: social, technical, and physical-based attacks. Through analyzing the different existing classifications of the social engineering attacks, we can also classify these attacks into two main categories: direct and indirect. Attacks classified under the first category use direct contacts between the attacker and the victim to perform the attack. They refer to attacks performed via physical contact or eye contact or voice interactions. They may also require the presence of the attacker in the victim's working area to perform the attack. Examples of these attacks are: physical access, shoulder surfing, dumpster diving, phone social engineering, pretexting, impersonation on help desk calls,

and stealing important documents. Attacks classified under the indirect category do not require the presence of the attacker to launch an attack. the attack can be launched remotely via malware software carried by email's attachments or SMS messages. Examples of these attacks are: phishing, fake software, Pop-Up windows, ransomware, SMSishing, online social engineering, and reverse social engineering.