Adrian N
an9905@rit.edu
CSEC.468.01
Risk Management for Information Security
Project Group – Social Engineering – Blog Post

If an employee falls victim to a social engineering attack it could potentially compromise an entire company. As the following statistic shows, a social engineering attack could do serious damage to enterprises:

- According to the Verizon 2019 Data Breach Investigations Report, 33% of data breaches were social engineering attacks (Smith, 2019).
- FBI data shows that social engineering attacks cost companies an average of $130,000 with damages climbing into the millions of dollars for many companies (The "Five Agonies", 2020).
- Socially engineered cyberattacks are just under 80% effective. The costliest socially engineered cyberattack is business email compromise – its 64 times worse than ransomware!

What is Social Engineering?

Social engineering cyberattacks can be considered a kind of psychological attack that attempts to persuade an individual (i.e., victim) to act as intended by an attacker. These types of attacks exploit weaknesses in human interactions and behavioral/cultural constructs and occur in many forms that will be discussed further later. The effectiveness of current security technologies has made social engineering attacks the go to gateway to exploiting cyber systems. Most research in social engineering has mostly focused on understanding and/or detecting the attacks from a technological perspective, however there is currently no systematic understanding of the psychological components of these attacks which perhaps explains why these attacks are roughly eighty percent effective.

How Social Engineers study people:

Before discussing psychological attack vectors, we should also take moment to look at how social engineers study people. This often means that these professional social engineers are more like actors and actresses versus the classic 'computer nerd'. They understand and are well acquainted to studying body language, voice control, and group dynamics. Social engineering depends on the victim's logical thinking toward the information given by the cybercriminal and how well the victim can be persuaded.

Seven Psychological Triggers:

Strong Affect: Applies when the cybercriminal makes a statement or provides information that triggers strong emotions. If the victim is feeling a strong sense of surprise, anticipation, or anger, then the victim will be less likely to think through the arguments that are being presented or develop a counter argument (Gragg, 2002).

Overloading: Overloading is about attempting to overload a target with information in order to reduce their decision-making abilities.

Reciprocation: Reciprocity deals with people's tendency to return favors. Social engineers will aim to do favor for the target and then ask for one in return.

Deceptive Relationships: Can be applied wherever there is a relationship of trust. When a cybercriminal and a victim have similar characteristics, it provides a strong incentive for the victim to help the cybercriminal

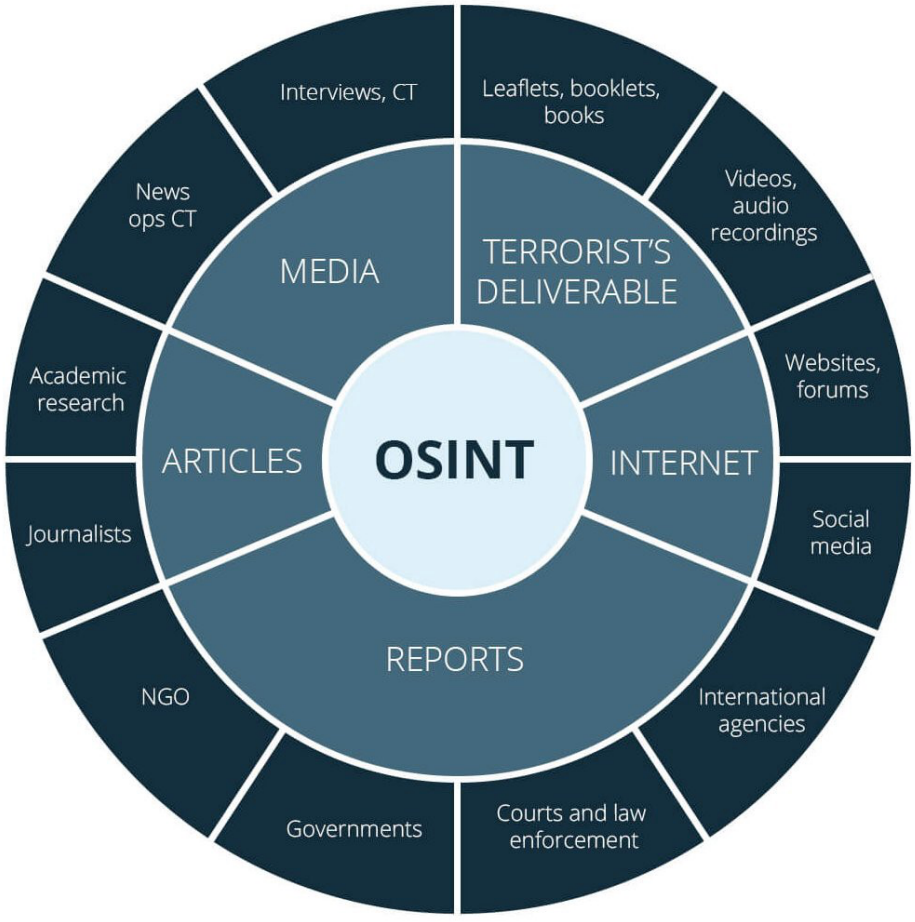
Diffusion of Responsibility: When the victims are made to feel that they are making decisions that will be the difference between the success or failure of the company.

Authority: Authority looks at people's tendency to obey authority figures. Social Engineers may assume the role of an authority figure to direct their target to act.

Integrity & Consistency: These are applied when people tend to believe that others are expressing their true attitudes when they make a statement (Gragg, 2002).

Open-Source Intelligence:

One can see that a social engineer will gather as much information as they can about your life and behavior. This is commonly known as Open-Source Intelligence which according to United States public law is produced from publicly available information and is collected, analyzed, and disseminated in a timely manner to an appropriate audience. These social engineers will create a database of information that is specific to the victim. This can be thought of as a game of connect the dots in which each dot represents some sort of information about your life (Abouzeid, 2019).



Psychological Influences:

After the social engineer collects this database of information they will focus on psychological influences. As humans we naturally pay attention to key details when someone first interacts with us. Based on our first interaction with someone new we can sense if we can trust this person or not. In doing so, we might ask ourselves some basic questions. These include whether it makes sense for this person to reach out to me, whether this person behaves in a trustworthy manner, or whether this person has any authority (Abouzeid, 2019). These characteristics like

- Consistency
- Commitment
- Obligation

is what social engineers focus on for the sake of making sure their target is more susceptible to manipulation. This can be a trial-and-error type of process in which the engineer needs to portray confidence in each of the characteristic they choose. These engineers also focus on building rapport with a target.

Rapport

A rapport is a close and harmonious relationship in which the people or groups concerned understand each other's feelings or ideas and communicate well. In terms of social engineering, this includes a successful utilization of the following factors:

- Validation
- Asking Questions
- Time Constraints
- Ego Suspension

These types of factors help build this idea of a false relationship by creating a sense of comfort that humans naturally are attracted to. This could include a threat actor potentially employing sympathy as their subtle attack by requiring help from the target.

Exploitation

The social engineer will use persuasion to request information from their victim, such as account logins, payment methods, contact information, etc., that they can use to commit their cyberattack. A person's natural tendency to avoid doing something wrong or to get in trouble will be exploited. If an attacker can make an employee feel that he or she caused a problem or performed a task incorrectly, then the employee may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols.

Four Distinct Attack Vectors based on Human Cognition

Careless Attack Vector:

Often the first phase of a more complex overall attack, this is where the attack escalates as the attacker's knowledge is expanded about the target. Reconnaissance is most often seen in this vector, and examples of this include:

Dumpster Diving: Act of taking trash from commercial dumpsters outside of office buildings

Password theft: Where passwords are written down and left out in the open

Comfort Zone Attack Vector:

This is where exploits often occur due to the fact that the victim is in an environment they feel comfortable, therefore leaving them to have a lower level of threat perception. Examples of comfort zone attack vectors include but are not limited to:

Impersonation: Impersonation is a common attack in which hackers impersonate everything from janitors to fellow co-workers from a victim's own IT staff.

Should Surfing: Shoulder surfing is the act of looking over a user's shoulder to observe the entries to the keyboard as the username and password are being typed

Helpful Attack Vector:

Used on the premise that people will generally try to be helpful, even if they do not know whom they are helping. Examples of this include:

Piggybacking: Piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area or pass a certain checkpoint.

Impersonation: Impersonation could entail an attacker calling a number they might have gotten from dumpster diving earlier, and impersonating an employee, and trying to pressure and use their psychological tactics to get information or change passwords etc.

Fear Attack Vector:

An attack that is based on attacking the victim in such a way that the user provides the attacker with the information or access needed due to putting the user in a state of anxiety, pressure, stress, and fear. Examples of this are:

Conformity: Conformity is a situation in which the attacker puts the user in the uncomfortable position of being the only user to not help them out as the others have in the past.

Time Frame: Time frame is an attack that uses a fictitious deadline to obtain user compliance from a Helpdesk Operator (Lively, 2003).

Importance: Importance is a technique employing impersonation in which the attacker pretends to be someone important or someone who is acting on behalf of someone important.

Lively, Jr., C. E. (2003). *Psychological based social engineering - GIAC*. GIAC. Retrieved October 14, 2021, from https://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780.

Abouzeid, E. (2019). *Hacking human psychology: Understanding Social Engineering Hacks: Relativity blog*. Relativity. Retrieved December 3, 2021, from https://www.relativity.com/blog/hacking-human-psychology-understanding-social-engineering/.

Gragg, D. (2002, December). A Multi-Level Defense Against Social Engineering. Computers and Security. Retrieved October 12, 2021, from

http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf.