Social Engineering

CISC 3325 — CUNY Brooklyn College
Lecture Notes

Social Engineering

In this chapter, we will:

1. Define the term "Social Engineering", and explain why this topic should be covered as part of a security course.
2. Explain what human traits lead to the social engineering attacks.
3. List the methods that social engineering attackers use to carry out their attacks.
4. Suggest how to reduce the possibility of falling prey to such attacks.

Social Engineering

The Merriam Webster dictionary defines **Social Engineering** as social methods (such as phishing) that are used to obtain personal or confidential information which can then be used illicitly. That is, Social Engineering is when attackers search for or solicit information from a person to use it for illegal purposes (such as stealing money) or further security attacks (accessing one's accounts).

Social Engineering attacks are increasing in our well-connected world, so discussing them in an information security course is a must.

For example, social media websites such as Facebook are used by attackers to collect information about people, which in turn can be used in their attacks, or can be used to initiate attacks. Moreover, many of the images posted on social media, like family photos or photos of the company picnic, can reveal lots of information that is otherwise unavailable to the outside world.

Unlike in other attacks, the targets here are not primarily computers but human beings.

Social Engineering

Since the target of Social Engineering is a person, the success of this sort of attack highly depends on the human factors. Specifically, several truths about people increase the chances for a successful Social Engineering attack:

- Human beings are helpful by nature and want to help out people in distress or in difficult situations.
- Human beings, by instinct, trust others.
- Human beings tend to obey the orders of their superiors or persons with authority in their organization.
- Human beings by nature are afraid of consequences of not having followed the rules/orders of the company, particularly of losing their jobs.

Pages 309 - 312 of the Nayak & Rao textbook include several scenarios exepmplifying attacks that take advantage of each of the above traits.

Policies, awareness, and trainings are the only major means of ensuring that the people are not easily conned through social engineering attacks.

Social Engineering

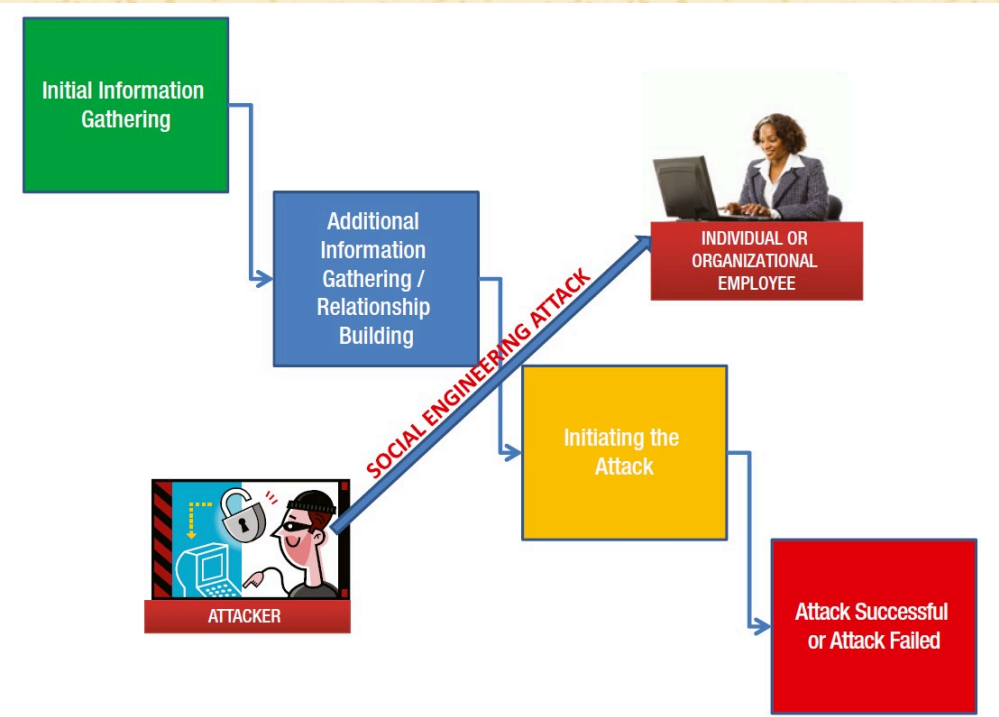

Figure 15-1. *Typical Social Engineering Attack Life Cycle*

The life cycle of a typical social engineering attack. "Figure 15-1: Typical Social Engineering Attack Life Cycle" (page 308), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Social Engineering: Attack Methods

Different methods are used by the attackers when it comes to social engineering attacks:

- **Pretexting**: Pretexting originates from the word “pretext”. “Pretext” means “for some reason” and most of the times a reason which is not genuine. This involves the use of intelligently thought out well-crafted lies with the bad intention of collecting information about an individual or organization to initiate the attacks.
- **Phishing**: “Phishing” means “fishing," that is, “fishing” for useful personal information about the user which will be used by the attacker for identity theft. These attacks target primarily the obtaining of login credentials: user ids and passwords, or other personal information, e.g., social security number, banking account number, and credit/debit card details.
- **Spear Phishing**: Just a more targeted and well-crafted phishing attack.
- **Vishing**: A short for “Voice Phishing” and uses phone calls instead of phishing emails.
- **Baiting**: An attack where CDs, DVDs, or USB drives are infected with malware that steals a user's info.
- **Tailgating**: Getting access to a building by following an employee. Discussed on Slides 8 - 9 of Access Control.
- **E-mail Attachments**: Opening an attachment of an email sent from an attacker might lead to the installation of malware.

Social Engineering: Attack Prevention

Some of the measures that individuals have to take to avoid becoming prey to social engineering attacks are:

- Avoid publishing any of your personal information.
- Do not give your personal information over the phone unless you know for sure the other party to whom you are talking. Banks, for instance, won't call you and ask your personal info over the phone.
- Do not believe in any request for your personal information. When in doubt, notify the bank or financial institution named in the request via an official phone number gleaned from a verified legitimate source.
- Always create strong passwords. Never have same passwords for various systems. Ensure that you invariably change your passwords periodically.
- Do not write down your passwords anywhere.
- Ensure to cover up if you have to type your passwords / PIN in front of others.
- Ensure that your screen is clear or is locked when you have to discuss with strangers at your desk.
- Verify regularly your financial statements to ensure that no unauthorized transactions are reflected on them.
- Destroy papers with any unneeded personal information written down by you.

Social Engineering

Any questions?

Social Engineering: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 15: Social Engineering." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 307-323. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+15:+social+engineering

Salomon, David. "Chapter 10: Identity Theft." *Elements of computer security.* Springer Science & Business Media, 2010, pp. 255-271. URL: https://link-springer-com.brooklyn.ezproxy.cuny.edu/content/pdf/10.1007/978-0-85729-006-9.pdf#10+identity+theft

Salomon, David. "Chapter 11: Privacy and Trust." *Elements of computer security.* Springer Science & Business Media, 2010, pp. 273-290. URL: https://link-springer-com.brooklyn.ezproxy.cuny.edu/content/pdf/10.1007/978-0-85729-006-9.pdf#11+privacy+and+trust