LUCIDEUS

Deep Insight into Social Engineering

Pradyumn Khanchandani

Rushil Saxena

INTRODUCTION

This document is intended to provide a detailed explanation of as to what is Social Engineering and what it consists of. It also covers a case study to give a better understanding of how Social Engineering plays an important role in real-life attacks.

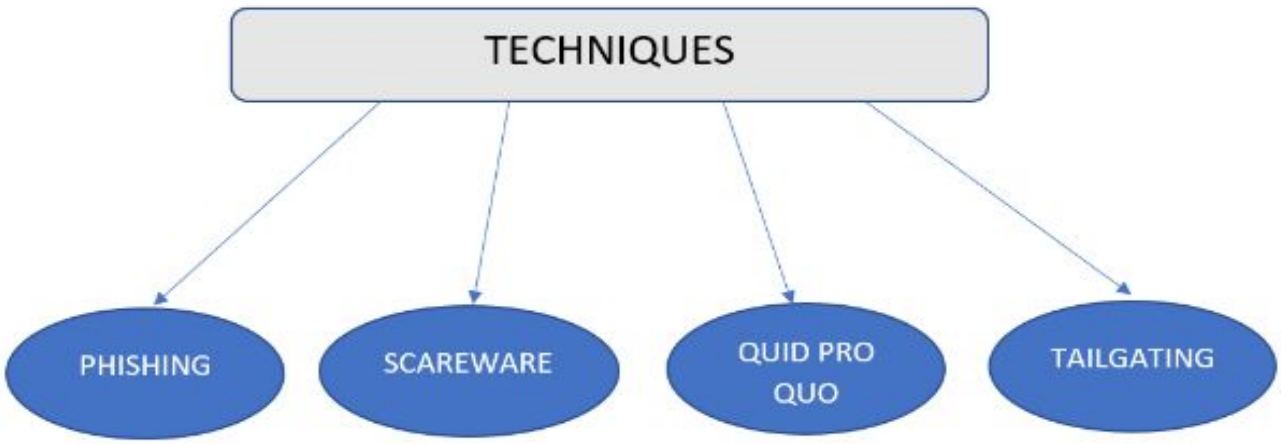
KEY TERMS

Vishing, Phishing, Smishing, Impersonation, Pretexting, Water Holing, Baiting, Tailgating, Quid Pro Quo

DEFINITIONS

SOCIAL ENGINEERING - In the context of Cybersecurity, social engineering is the manipulation technique that exploits the human error to gain private information or access. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

These are a few popular Social Engineering techniques used by attackers and APT groups to gain confidential information and data.



Vishing - Vishing, also known as “Voice Phishing”, is a method of Social Engineering over telephone communication to gain access to personal, private, or financial information from the target for the purpose of financial reward. It is also used for reconnaissance purposes to gather details of the target or the organization.

Phishing - Phishing is a method of Social Engineering where the attacker obtains private information typically by disguising oneself as a trustworthy entity in an electronic communication. This is mostly done via e-mails, The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN or a credit card number.

Smishing - Smishing is the Social Engineering technique involving the use of SMS to lure victims to a specific course of action, it is the practice of phishing using SMS.

Impersonation - Impersonation is the Social Engineering practice of pretending to be another person with the motive of gaining access to a specific area, building, or even a device.

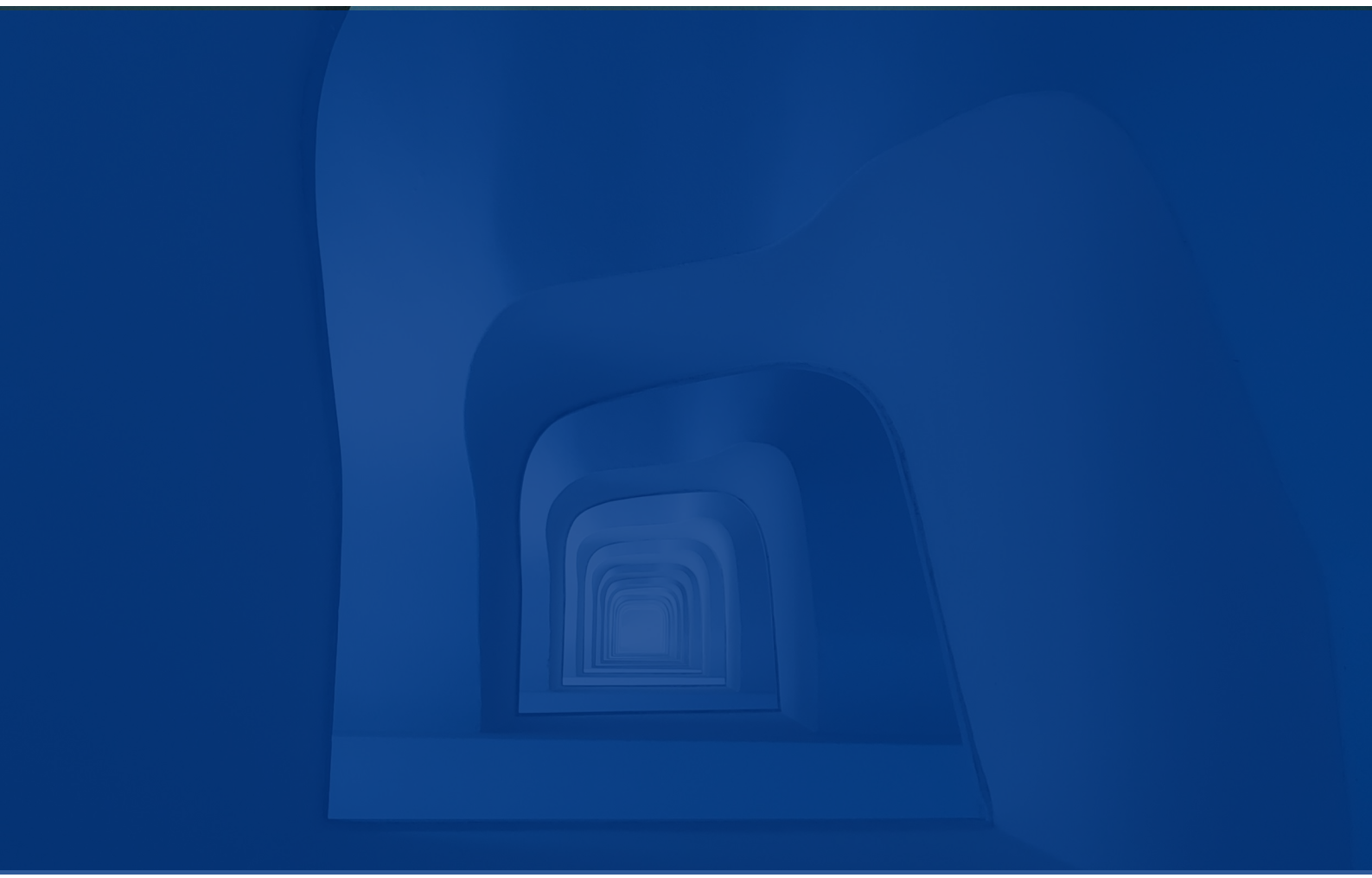
Pretexting - Pretexting is the act of creating a fake scenario to engage a targeted victim in such a way where the chances of the targeted victim divulging information and performing actions that will help the attacker gain access to their system, increase drastically.

Water Holing - Water holing is a targeted Social Engineering strategy that works on the trust users have on the websites they regularly visit. The attacker leverages the trust of a victim to a trusted website and infects the website with malware which will further be used to get access and/or information from the victim’s device.

Baiting - Baiting is the Social Engineering practice of luring victims by working on the inherent nature of greed and curiosity. An attacker leaves a malware-infected USB drive (called Rubber Ducky) at a hotspot location and waits for a victim to fall for the trap and pick up the USB. Once the victim picks it up and plugs it in his personal or corporate device, his device will be infected with the malware and the attacker will have access to all the personal information he needs.

Tailgating - Tailgating is the Social Engineering technique of seeking entry to a restricted area or building by simply walking behind a person who has access to that particular location.

Quid Pro Quo - Quid Pro Quo is a common Social Engineering attack, where the attacker requests the exchange of critical data or login credentials in exchange for a service (often disguised as technical support).

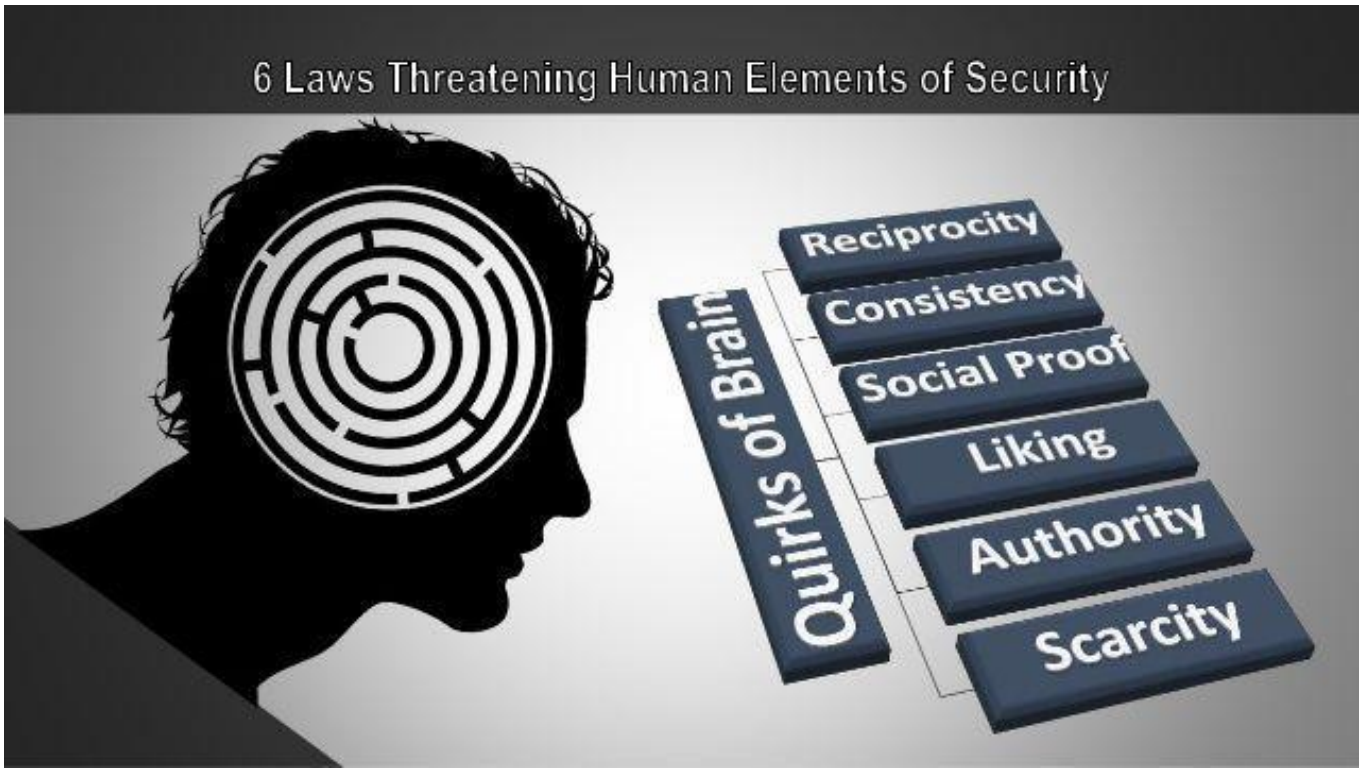


SOCIAL ENGINEERING VECTORS

1. VISHING
2. PHISHING
3. SMISHING
4. IMPERSONATION

KEY PRINCIPLES

There are 6 key principles of any Social Engineering attack, these were established by Robert Cialdini.



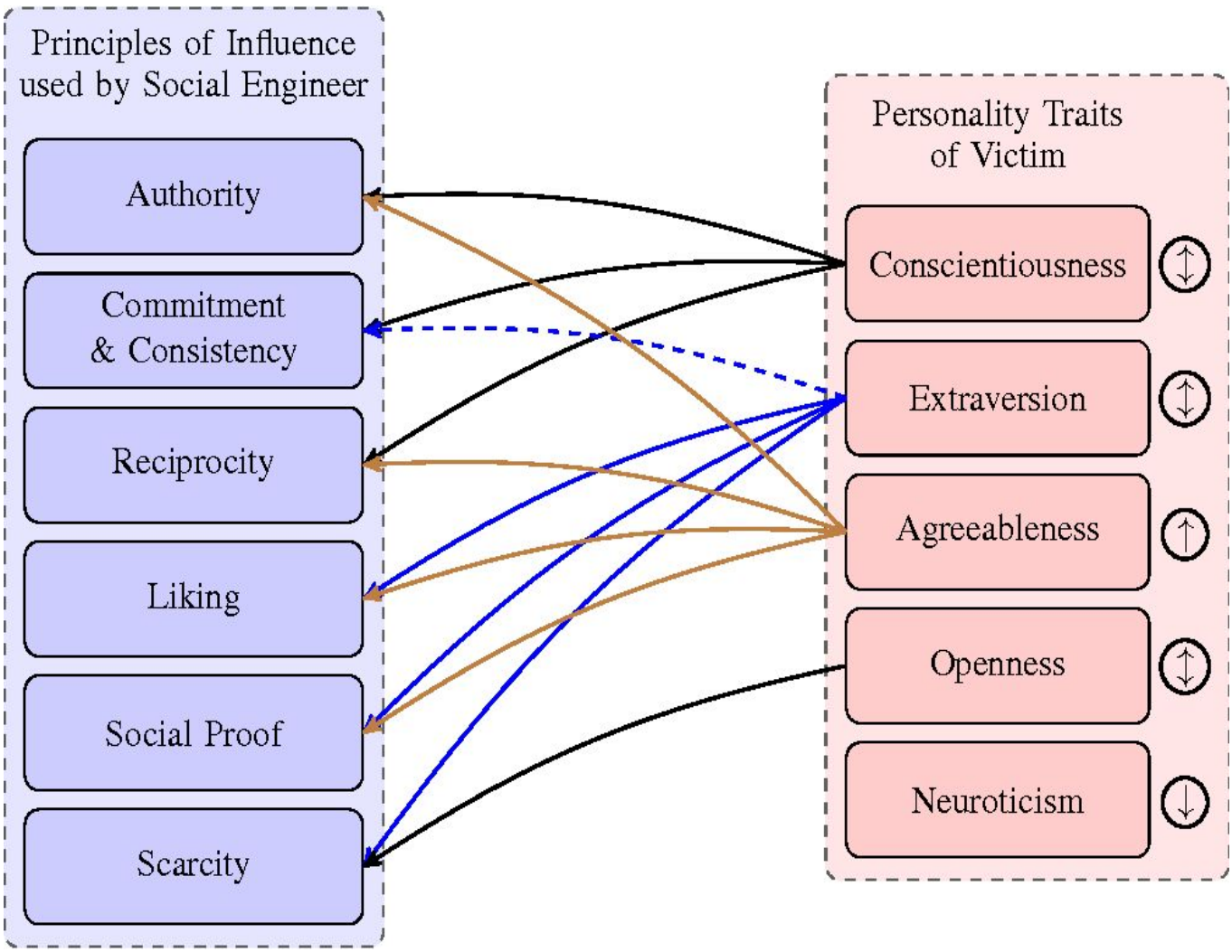
RECIPROCITY - People have a nature of returning any favor anyone has lent them, people reciprocate deeds and acts done towards them. The good cop/bad cop strategy is based on this principle.

COMMITMENT - If people commit to something, orally or in writing, they are more likely to commit and stick to their agreement as it represents their self-image and commitment.

SOCIAL PROOF - "Monkey See, Monkey Do", people will do things that they see other people doing as they have a need to fit in the society and get accepted.
AUTHORITY - People have an inherent nature to respond to leadership, hence they will tend to obey authoritative figures even if they are asked to perform objectionable acts.

LIKING - People are easily manipulated and influenced by other people whom they admire or like.

SCARCITY - Noticing scarcity will generate demand among people.



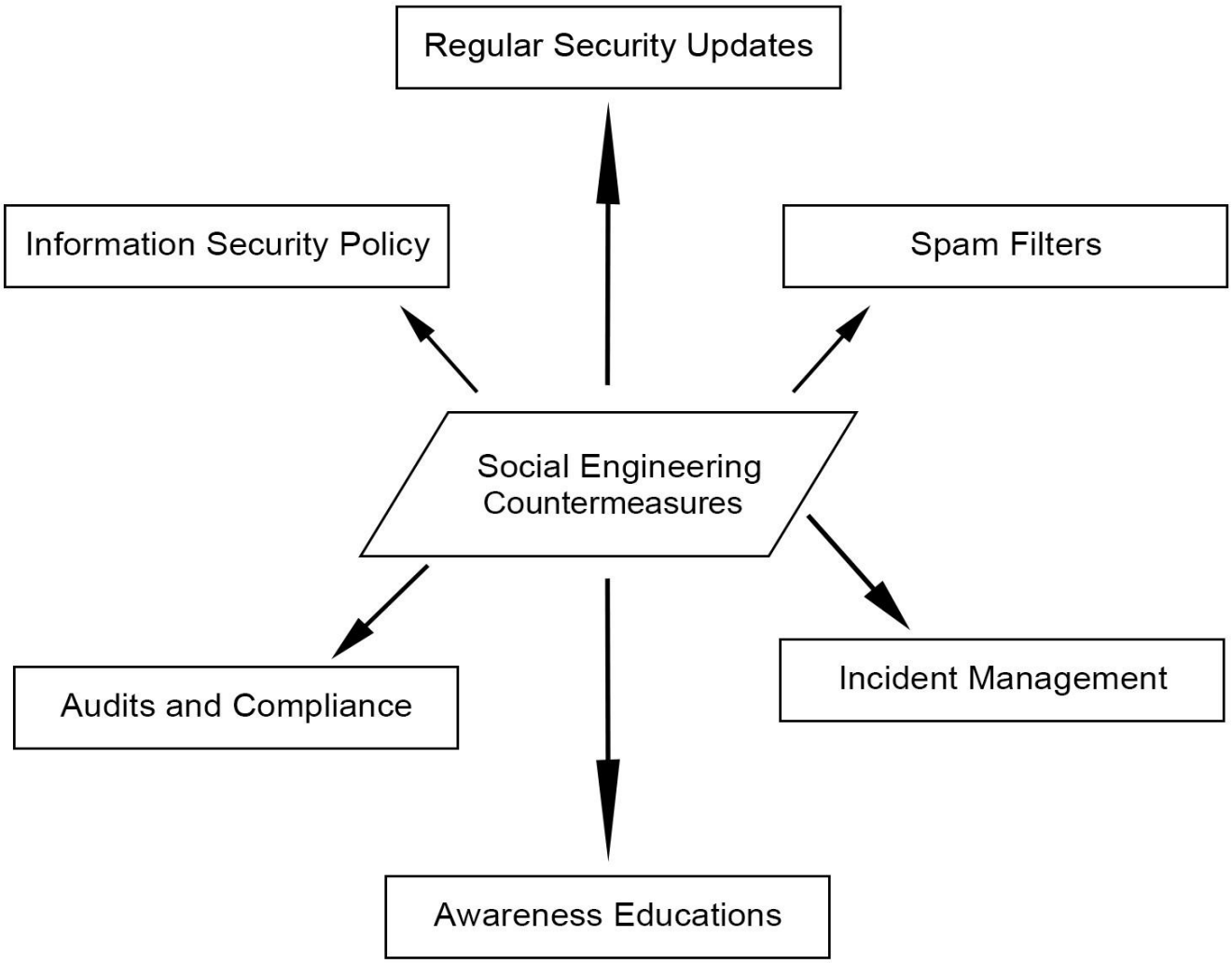
CASE STUDY ON SOCIAL ENGINEERING (THE “PIZZA” Method)

Hackers posing as pizza delivery service carried a successful social engineering attack on the warsaw branch of a well-known international company. In a few minutes, they hacked the IT system by deploying malware.

It all started by sending the information to the email addresses listed on the company's website. The information that was sent was the opening of a new pizza parlor in the neighborhood and that there would be a discount of 30% for the first few customers. Employees tempted by this offer quickly organized a "pizza day" and ordered 8 pizza boxes.

After some time the pizza delivery man appeared with the 8 pizza boxes and a free gift in the form of USB plugged LED lamps that changed colors to the rhythm of the music. Surprised with the gift, the employees plugged the USB into their computers. They were unaware that in this way they gave the hackers remote access to the company's infrastructure and with one computer the hackers were able to compromise the entire network.

COUNTERMEASURES



1. Employees should be trained in various security protocols and techniques.
2. Messages asking for security details should be removed and reported, as these messages are likely to be fraudulent.
3. Spam filters for electronic mail should be implemented.
4. Only safe websites should be accessed.
5. Anti-virus software should be updated regularly.
6. Regular unannounced periodic tests of security frameworks should be conducted.

REFERENCES

- https://en.m.wikipedia.org/wiki/Social_engineering_(security)
- https://www.itsecurityawareness.ie/a-z-glossary-of-information-security-and-social-engineering-terms


LUCIDEUS™