SOCIAL ENGINEERING

INTRODUCTION

A company may have

Purchased the best security technologies that money can buy,

Recruited the best trained security team

Hired security guards from the best security firm in the business.

The company is still totally Vulnerable because of the Human Factor - Security's weakest link.

(Kevin D. Mitnick)

WHAT IS S.E?

Social engineering is a manipulation technique that exploits human error to gain private **information**, **access**, or **valuables**.

WHAT IS SOCIAL ENGINEERING ?

Social engineering involves the use of social skills to manipulate people to garner information they would normally not disclose.

It can also be defined as an art of deception.

The process preys upon two common characteristic traits:

- Acceptance of authority
- Willingness to cooperate with others

What are the broad types ?

- **Phishing**
- **Vishing**
- **Tailgating**
- **Dumpster Diving**
- **Shoulder Surfing**
- **Eavesdropping**
- **Pretexting**

The act in which an individual lies to obtain privileged data of an individual to impersonate.

TYPES OF SOCIAL ENGINEERING ATTACKS

- **Spear phishing** → malicious emails sent to specific target
- **Whaling** → targets CEO's, Presidents, Dignitaries
- **Quid Pro Quo** → Promise of favor in exchange of information

Physical Aspects

- At the workplace
- Over the phone
- Trash Area
- On-line Portals
- Out of Office

Psychological Aspect

- Persuasion
- Impersonation
- Friendliness

Unfortunately,

Almost anyone is potentially capable of mounting a social engineering attack

It is not easy to decipher a Social engineering attack

Characteristic Traits:

Refusal to give contact information,

Rushing,

Name-dropping,

Intimidation on questioning,

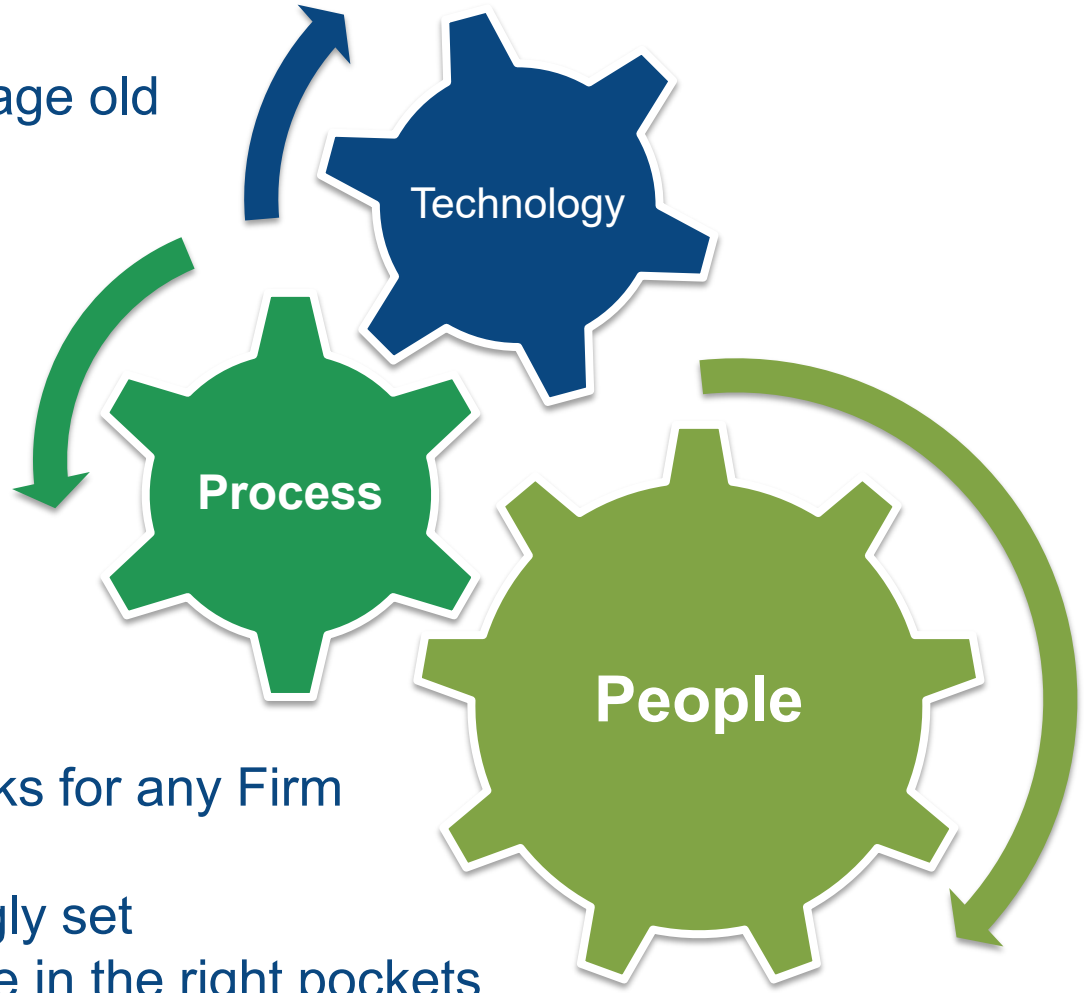
Committing Small mistakes

Requesting forbidden information

What do I do ?

- Solution is simple and age old

PPT ➔



- The three building blocks for any Firm

- Our priorities are wrongly set
- Investments to be made in the right pockets
- Awareness needs to be the key tactical as well as strategic Goal

Technology - Important

- It is only as good as the people who use it and the process which defines its usage or boundaries
- Will technology add value? - is no longer a question but rather a factual statement.
- We need to maintain the balance between investment and requirement.

Process – Very Important

- Defines what People and Technology do to make a system work
- A flawed process leads to the other two components failing, though they might be the best in themselves individually
- This needs to be defined at the early stages
- Has a bad habit of defining itself, if not managed and defined properly

People – Most Important

- Core building block to each and everything in an Organization,
- They control processes, control technologies as well as manage other people
- Any flaw in the People component will indirectly affect all the three components in the long run
- It is highly important that people are trained in their respective fields to take informed decisions.
- It is also important that right people are mapped to the right systems as wrong mappings can crash the whole system.

SMISHING

Fraudulent practice of sending text messages showing it's from a reputable company to lure individuals to reveal personal information such as passwords, credit cards, address, DOB, etc.

Example

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

https://office.postingwebsite.com

(Please reply to 1, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)

The US Postal team wishes you a wonderful day

PHISHING SITE ANALYSIS

- check https://beriteck.com/ on https://urlscan.io
- Visit https://urlscan.io/result/6a996827-72cb-411a-93f8-fae974604906/

- What clues do we have that this may or may not be a credential harvester?

PHISHING STATS

Phishing attacks continue to pose a significant threat to individuals and organizations alike. According to recent statistics, phishing accounts for over 80% of reported cyber-attacks. It is estimated that billions of dollars are lost each year due to successful phishing campaigns.

REAL-WORLD EXAMPLES OF SOCIAL ENGINEERING ATTACKS

The infamous "Nigerian Prince" scam, where individuals were promised a share of a large sum of money in exchange for providing their bank account details.

The "Tech Support" scam, where fraudsters impersonate technical support personnel and convince victims to grant remote access to their computers, leading to unauthorized access and potential data theft.

REAL-WORLD EXAMPLES OF SOCIAL ENGINEERING ATTACKS

The infamous "Nigerian Prince" scam, where individuals were promised a share of a large sum of money in exchange for providing their bank account details.

The "Tech Support" scam, where fraudsters impersonate technical support personnel and convince victims to grant remote access to their computers, leading to unauthorized access and potential data theft.

WHAT SHOULD YOU DO IF YOU RECEIVE A PHISHING EMAIL?

- **STOP , LOOK & THINK**

and verify before taking an action

- **Don’t Click Any Links,**
- **Don’t download and open files**
- **Don’t share any personal information !!!**

https://www.phishing.org/phishing-examples