International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 3, May-June 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Social Engineering: Cracking People Before Cracking Systems

Disha Tiwari

Assistant professor, University Institute of Computer Science and Application (UICSA)

Rani Durgavati Vishwavidyalaya, Jabalpur

Ddishatiwari8@gmail.com

1. ABSTRACT:

Human brain cannot be automated or hacked, it can be convinced or influenced by one of the cybercrimes, like Social Engineering Attack. Cyber-crime grows to become part of almost every human's life, due to lack awareness and knowledge. As cybercrimes are not limited to social engineering attacks; rather phishing, spoofing, spamming, vishing, DDOS attacks, cyber terrorism, ransomware attack, identity fraud, unauthorized system access, identity theft; are some other cyber-attacks.

Social Engineering is an art work of collecting facts and manipulating human being, not directly the technology. As human's psychological behaviour subjects maximum in these attacks. It is taken into consideration as a initial medium of terrorism, in which hacker performs with human consciousness. Usually, human being end up sufferer of these attacks, because of loss of cyber focus and knowledge. It is one of the handiest non-IT strategies for an attacker or hacker, to collect fact or to show credentials and breach protection protocols.

Dumpster Diving and shoulder surfing are very often took place social engineering assaults. The one that carry out social engineering attacks are referred to as social engineers, who does each attack with a motive. In this research report various types of social engineering attacks are covered, its examples, categories and a few illustrations with the help of a chart. That chart explains about various attacks occurs by which level.

"Social Engineering is directly proportional to individual's weakness."

2. KEYWORDS:

- Levels of Social Engineering
- Social Engineering Attack; it's phases and categories
- Social Engineering skills
- Social Engineer's motive
- Information gathered from social engineering attack.
- Advanced social Engineering Attack
- Its examples
- Illustration of Attacks

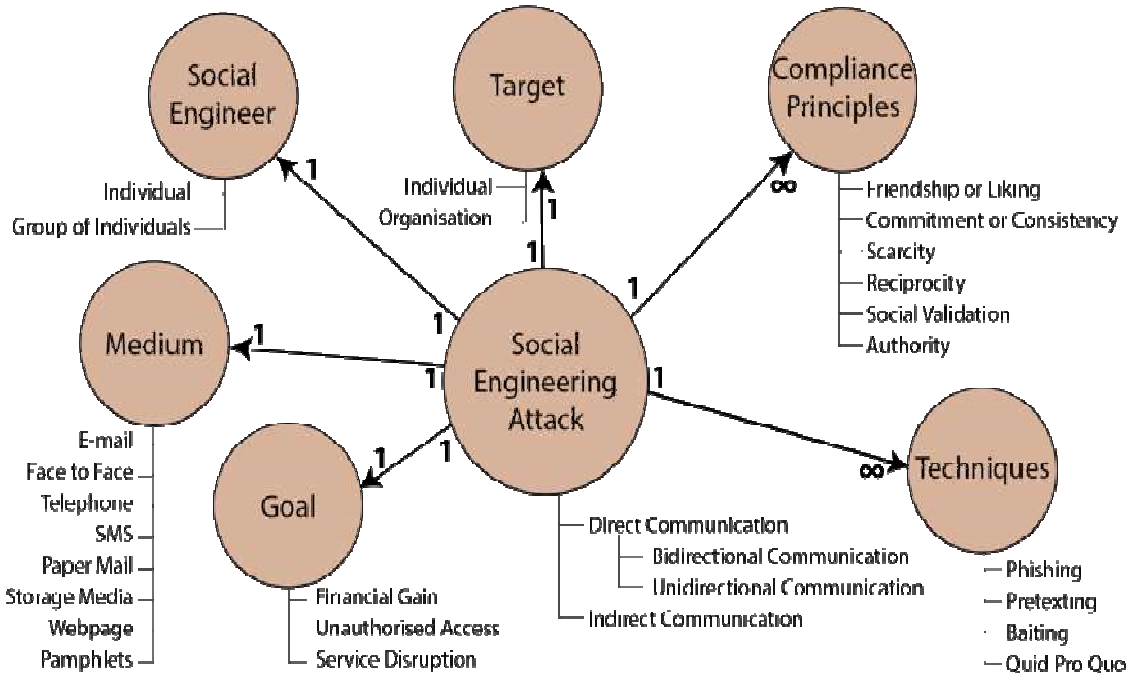
3. INTRODUCTION:

Now a days, one of the most practised and efficient penetration attacks are social rather than technical. Social Engineering takes place on two levels:

- **Physical**
- **Psychological**

In physical level, any authorized person of authentic organization perform social engineering to extract the desired information, like; Dumpster Diving. Hacker may seek credentials, secrets, user name, passwords, etc.. In Psychological level, hacker perform manipulation of natural human tendency to trust, they show like they are the one whom you can trust. **Here, they crack a person before his system**. Hacker tries to convince the victim to present credentials of individual or an organization, at any cost, whether they have to offer a bribe.

Social Engineering is considered as a bigger attack surface with more attack opportunities. In any other attack like phishing, spamming and spoofing; people know, how to stay safe from it, but in social engineering attack, people don't know they are facing such kind of attack. Humans are considered as the weakest link to keep any secret or credential.



As system is completely handled by humans, for example password of a particular system. About 70% of information theft is carried out consciously or subconsciously within the organization; (e.g.: Verification of particular institute from an outsider). It could be performed to give a way to malicious intentions of an information gatherer, to exploit any individual or authenticity of an organization. Such kind of attempts by influencing, convincing his target are considered under Social Engineering attack.

4. HACKERS AND SOCIAL ENGINEERS:

Somehow, hackers and social engineers are related. As social engineering is applied by social engineers, to gather private information, secret credentials, confidential data manually, by tricking with human mind. But hackers could attack both manually (by performing social engineering attack) and technologically (spamming, spoofing, phishing, vishing, etc). Motives of hackers and social engineers is same to some level, i.e., need of data and information. **Social engineers are known as "People hacker"**.

Social Engineering Attacks look like, taking advantage of your curiosity and trust, these messages or mails will contain a link, that you just have to check out and because it looks like an authentic mail, send from your friend, you will be extremely curious to open it. That guy can click that infected link, which could be loaded with malware or any other virus like trojan virus, which can infect computer system or sever, if our system is publicly hosted. Credentials of particulars also be stolen or system would be remotely handled.

Social engineering attack also contain a download of any of your certificate, music file, notes file, digital book; that has malicious virus embedded. These can be performed very easily, as some virus creator software/ tools are available free of cost. Virus either self-replicates itself in victim's system or provide every bit of information to the attacker. Even if any notification arises in victim's system and he cancels it, but attacker got the notification, as attacker provides you every remote access to particular Attacker. We must install anti viruses software in system, by which if our system is publicly hosted as a server, so its database could be completely secure.

5. PHASES OF SOCIAL ENGINEERING ATTACK:

Social Engineering Attacks can be performed in a well planned manner. It can be performed remotely and physically both. Technique of social engineering attack follow the procedure of Research, Hook, Play and then Exit, which are explained as follows:

- **RESEARCH/INVESTIGATE**:

Technically, this term is known as Reconnaissance. This is the first task in the approach of social engineering attack. Attacker is the one, who must know each and every information about his target. He can gather information from social media platforms, or he could send spoofed mails to victims with a malicious link loaded with such kind of virus which can reveal every information of victim's screen.
He could be capableof get the credentials like PIN and passwords. One of the high-quality quotations "KNOW YOUR ENEMY" fitsflawlessly to this attack. Research may be in any suchmanner, like attacker may want tounderstandeachparticularstatistics, with outunderstanding the victim.

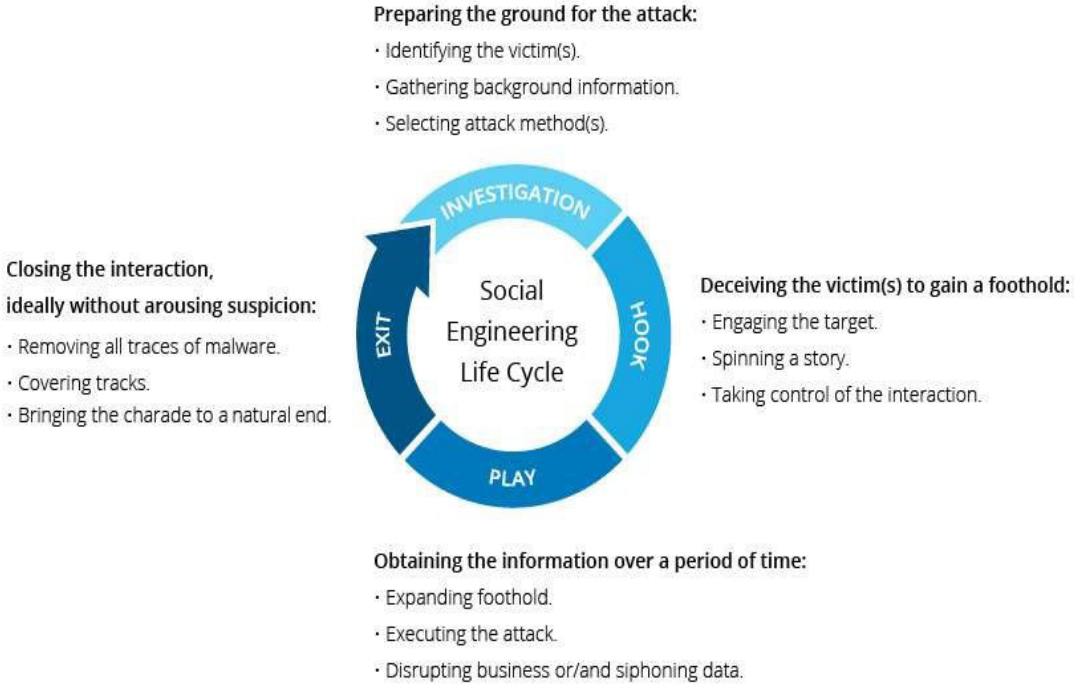
In this section basically, attacker attemptsto set up a reference to the goalwithout delay or indirectly, psychologically deprave or attempts to extract statistics. He may alsoshare such type of downloadable files, that are of your hobbyand also youhave to be curious to it. May be a fewin-built virus are connected to it, hidden in it; like an image, virus is hidden in it.

- **PLAY:**

This is the section where, attacker subsequentlyprovide a manner and execute to all his collections made in reconnaissance process, to get out the credentials, exclusive and passwords. He could make all feasible ways, to get into devicewhether or not from any malicious script of with the aid of using a call, if you want tooffer you an differentprovide or any deal.

- **EXIT:**

Attacker subsequently exits like, he was no longer who compromised the man or woman or organisation and attempts to erase all of theinstalled connection technically. As after revealing, attacker can clean all his virtual footprints, like as no thirdperson was over there.



6. CATEGORIES OF SOCIAL ENGINEERING ATTACK:

Farming and Hunting comes under the category of Social Engineering Attacks, let we have a few descriptions about these two categories.

- **HUNTING**:

In this type of Social Engineering Attack, attacker does not directly interact with the victim rather, he tries to reveal authentic secret credentials from victim's connection, as he directly does want to be a part of it.

- **FARMING**:

In this type of Social Engineering Attack, individual directly interacts with the target, and try to exploit, rather if caught up, he offers bribe or pressurise to provide the credentials. Technically, Attacker directly sends malicious scripts to victim to reveal passwords and credentials. He can also find documents which would be helpful for an attacker to exploit particular.

7. SOCIAL ENGINEERING SKILLS:

- **EAVESDROPPING:**

It is the process of revealing secrets in front of group of people, assuming that they are authorized people. But, here person himself wants to publicise the secret. Keeping an eye on e-mails and calls.

Eavesdropping also include an unauthorized person, who only silently hearing what is going on around and try to extract the information, credentials or passwords which could lead to an illegal task. One of the best method of Eavesdropping is VOIP (Voice Over IP Calls), which can basically steals IP Address of any system or server to hack particular data. Prevention of digital Eavesdropping are Building more secure networks, contributing to digital literacy, encrypted talks, etc..

- **SHOULDER SURFING:**

It is one of the social engineering techniques, which refers to direct remark from **a** personin the back of or surf from individual's shoulder usually to extract PIN, passwords, mysteryfacts, credentials. Shoulder surfingalso can be done, remotely, individual's gadget or cellular phone. Shoulder browsingalso canresult ineconomicWipeout.

Some of the doings from which, shoulder surfingmay beavoided are, sit back to the wall at any economic or public places, ensure to take your receipt after economic transaction, cover the keypad of the ATM while entering PIN, lock your laptopdisplay screenwhile youvisita fewdifferentarea and share your financial details to authentic person in a private area.

- **DUMPSTER DIVING:**

Extracting sensitive and useful information from trash or garbage, like recycle bin, hardisk, with a malicious intent to destroy individual's system or an organization. It depends upon human weakness, lack of security knowledge. Even CDs, hardisks also can be found at the time of Dumpster diving. It is considered as one of the major branches of Cyber Forensics, in which evidence / proofs against any criminal can be collected from trash of any system. Even any used but thrown hard disk must have important evidence, which can be used to present in court of law.

8. SOCIAL ENGINEER'S MOTIVE:

Any hacker , attacker or social engineer, definitely keep a motive to cyber-attack on any individual. Not any single task can be accomplished without any motive. Here, motive could not for the welfare of the

society, even it can degrades information or to extent someone life also. There could be either any personal motive or a political issue. Some how social engineering attacks are performed by script kiddies, who can do it for learning purpose only.

Some of the following motives of social engineers are discussed below:

- **PERSONAL INTEREST:**

One of the motives of social engineers could be his personal interest, like he may be script kiddie, who is trying to learn and explore the technology or a person who have some relationship issue with the attacker. By using his credentials may be he is trying to get advantage of confidential. A person who is a beginner in the field of cyber security, he somehow creates malicious virus by using different tools, like; SVM virus maker, trojan horse virus maker, to create a virus and make it publicly available to the users. Some users, don't know the protocols of using internet, like, which site, they could not visit, which websites can cause harm to their systems and unknowimgly they install that malicious virus into the system.

- **FINANCIAL GAIN:**

Person or attacker could try to get the bank details, due to financial issue to trick a person. He must try to get the credentials or bank account number. For sake of this he must perform phishing attack, he provides the link in the mail, which could be loaded with infected virus, like, malware or trojan horse, which can observe your screen functioning and can easily observe what individual is performing. Even attacker can control the victim's system. He can even operate camera, microphone and capture any password he is putting in any social networking sites or any bank account details.

While capturing bank account credentials, he use that credentials to take off money from bank account and even being anonymous publicly by using proxy servers. Proxy servers helps to change IP-addresses two to three times and no one is able to capture the real Attacker. To some level, it might be impossible.

- **INTELLECTUAL CHALLENGE:**

Here, attacker must target to any specified system or server to steal the credentials and to completely hack the system and to ask for Ransome as a bribe for not to disclose it in public. As now a days, data and information are considered as the most precious valuables. Cyber thieving of data is most common and richest illegal work in the world.

- **EXTERNAL PRESSURE:**

External pressure is like, suppose that, attacker hired an another person for specific illegal task. So it might be possible, that another person is innocent and doing only for sake of money. Cyber terrorism is also included in external pressure. Some people only for sake of money can choose this field for feeding their family, which is wrong obviously. They unintentionally have to create some virus and trojans. They have to make it available publicly with an anonymous identity by using proxy servers. Gradually they became as Cyber Terrorist.

- **POLITICS:**

Any political reason can also be responsible for social engineering attack, to satisfy anyone political plessure. For example, if two software cam into a market with almost of same properties, but difference is one is made in his own country and another one is foreign made. So here, it is completely depend upon the individual like which software is compatible to individual. But to increase the publicity of any one software, that party tries to degrade another party software, by try to hack their system or server and to publicly available private information of their customers. So, here the motive of this crime is to satisfy political issues.

9. GATHERED INFORMATION FROM SOCIAL ENGINEERING ATTACK:

- Employees' name
- Username
- Password
- E-mail address
- Server name
- Manuals
- IP-address
- Organizational Logo
- Organizational Policies and Procedures

10. ADVANCED SOCIAL ENGINEERING ATTACKS:

Major tactics of Advanced social engineering are as follows:

- BYOD policy (Bring Your Own Devices)
- IOT (Internet Of Things)
- Wearable devices (Gadgets)
- AI (Artificial Intelligence)

Due to digitalization, BYOD (Bring your Own Device) policy, use your own network, use your own wearable digital gadgets, for your own sake, is newer trend now a days. Our homes would be completely digitalized, like by capturing any device through video, we can operate it through our devices. We could be completely handling it remotely, which is known as IOT (Internet Of Things).

In future we will be handling all these through our WEARABLE DEVICES; like from our smart watches. So attacks could be increasing day by day due to this connected technology of devices. If any of our device could be hacked, control of our home would be completely in Hacker's hand, which would raise to another cyber crime.

Social Engineering Attacks could be performed so easily, as that smart device could be used by the children of that home also. As we are getting phishing messages or spammed mails in our system, now a days. But, in future it could be possible, we will be getting those in our mini smart gadgets. Due to lack of awareness and knowledge, it would be misguided.

If that small devices are hacked by the hacker, so he would control everything of home; namely electricity, gas stove, refrigerator, AC, oven; by which hacker would definitely take its advantage.

Hacker could try to get every possible information, credentials. Hacker can even use their own children, for their own kidnapping. As every has its positives and negatives also, so we have to be very aware, specially in this world of digitalization.

11. SOCIAL ENGINEERING EXAMPLES:

- **URGENTLY ASK FOR YOUR HELP:**

Like some of your closest one got trap into a kidnapping or any accident and he need an urgent help of money, so you kindly go through below mentioned link and do a payment. That payment link could be infected or loaded with virus, which can capture your bank a\c details.

- **USE PHISHING ATTEMPTS:**

An attacker or a phisher could share you a mail, text message, that appears to be from an legitimate and authentic person, which could be an infected one.

- **ASK YOU TO DONATE TO THEIR CHARITABLE FUND:**

They could send you a mail or message full of kindness and generosity, like any one could be trapped into it and willing to pay such a small amount. But they really don't need money, they actually have the hunger of data and information like; bank account details.

- **PRESENT A PROBLEM THAT REQUIRES YOU TO "VERIFY" YOUR INFORMATION BY CLICKING ON THE DISPLAYED LINK:**

The link, that could be given for verification, it would end with a legitimate extension like .com, .edu or .in ; any specified logo could also be mentioned over there to gain trust. We must use filter option in our mail box, as every e-mail, come from that specified filter and mail with an malicious content, could not drop in our mail box.

12. ILLUSTRATION OF SOCIAL ENGINEERING ATTACKS:

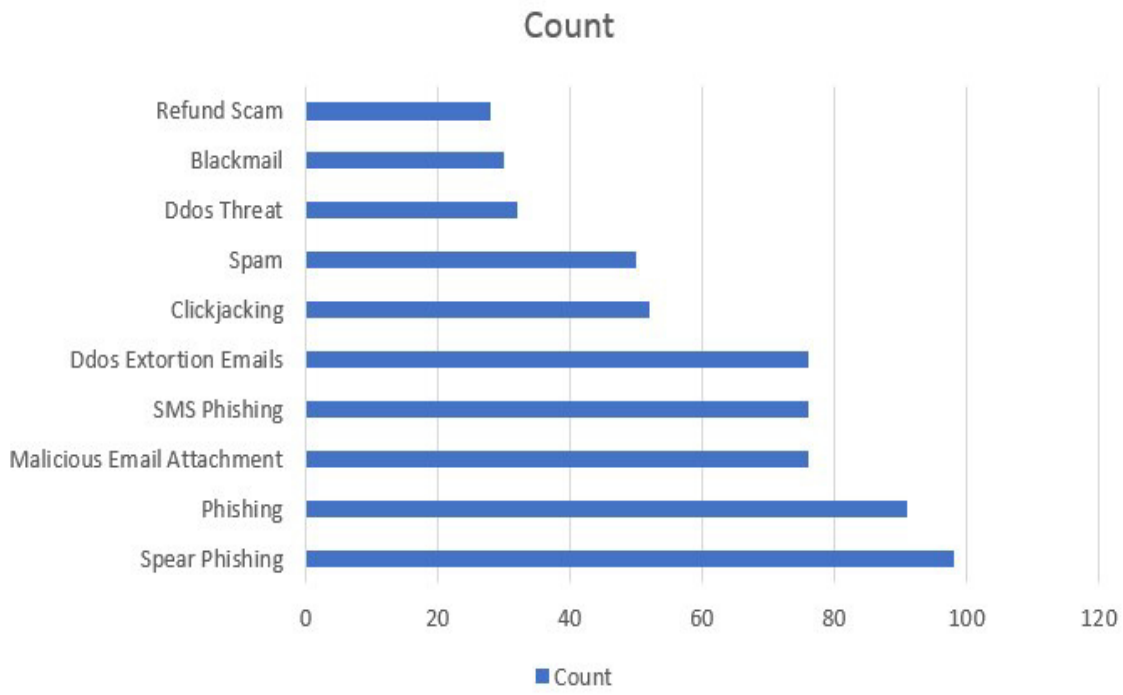
Major Tactics of these attacks are as follows:

- Spear Phishing
- Phishing
- DDOS Attacks
- Malicious e-mail attachments
- Spamming
- Click hijacking

As mentioned in the diagram, Spear phishing has the largest count, which is sending fraud messages or e-mails, from an illegitimate person, pretending to be from a legitimate person. Phishing mails contain documents and attachments, in which virus can be hidden within.

Phishing has lower count from Spear phishing. Phishing e-mails are directly from unknown person from bad intentions, which could be malicious attachments. SMS phishing is sending fraud offer or deals through text messages, which could contain malicious scripts.

DDOS attacks, can be performed by remotely connecting through any system, which is sending millions, billions of requests to server, like server may stop responding or may crash down. Ransomware attacks are those, in which attacker asks for Ransome, i.e., bribe, for returning the stolen credentials. In DDOS Attacks, proxy servers are used, in which actual IP address is impossible to catch. If person is sitting in Singapore and he can use IP address of Netherlands and even not able to caught up.



13. CONCLUSION:

In this world of digitalization, the need for data privacy and protection is quite more important. Successful social engineers make an attack more effective by using people, instead of just using the telephone. During this pandemic situation, social engineering attacks are increased rapidly, as everyone stuck to work from home or online classes and instantly, use of e-mail is rapidly increased, where around 50% of malicious content was shared over their by attaching virus to the desired attachments you need. In future, these attacks are going to be increase due to complete digitalization in future, as technology are at its supremum level now a days. Technology is being raised in the domain like Artificial Intelligence (AI), Internet Of Things (IOT), Smart Gadgets. As, we know that, AI and IOT has various positives, specially in the medical field; but is has some negatives also.

To be technically safe, we need to have a system, throughout disconnected from internet, where our every credential could be saved. Our systems could communicate with the help of shared folders and our every document, password must save in that system, then only our credentials could be safe. It could not be hack over here, anyhow. We must delete any request for financial information or passwords, we must reject requests for any help or offer, we must secure our computer devices by installing anti-virus

software on devices, keep updating our software regularly and keep changing our passwords frequently within two months; to protect ourselves from social engineering attacks.

Now, information security professionals recognized that the organization's information security should be more important than computer system, software or hardware's security. There are no tools available to analyse whether Social Engineering Attack has been performed or not, whether our credentials (user name, password, IP-address, server IP) are safe from malicious attempts or not. Still, we can follow the measures mentioned in above paragraph to be safe from social engineering attacks, as PREVENTION IS BETTER THAN CURE.

'We may not realize we have a problem, but that does not stop us from having one.'

REFERRENCES:

- Bernard Oosterloo, University of TwenteEnschede, The Netherlands.
- Mosin Hasan, NileshPrajapati, SafvanVohara; BVM Engineering College, VV Nagar.

