WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Social Engineering: A Threat to Cyber Security

P. Jeevetha

B. Com, LLB. Dr. Ambedkar Law University Tamilnadu, India

A B S T R A C T

The Internet Boom has been a boon for several Industries as it has disrupted the markets and created new avenues for business. But this Boom has resulted in an exponential rise in the number of Cyber Offences. Due to a lack of awareness, these offences usually go unreported. One such cyber offence is Social engineering, which is a form of deception that hackers use to acquire sensitive information and access unauthorized infrastructure and facilities. When malicious activities through the internet with a personal touch, it is termed Social engineering. This paper focuses on the concept of social engineering and how cybercriminals cause a threat to cyber security using social engineering techniques. Some of these techniques are pretexting, phishing, quid pro quo, baiting, scamware, Tailgating, and watering holes. Cybersecurity is the action or process of defending against and recovering from cybercrimes on computer systems, networks, devices, and software. To further understand the social engineering concept, this chapter will then discuss some of the real examples of social engineering and necessary measures to prevent social engineering and necessary measures to prevent social engineering attacks.

Keywords: Internet, social engineering, cybercrime, cyber security

1. Defining Social Engineering

Kevin Mitnick, a well-known hacker, popularized the term "Social engineering" in the 1990s, however, the idea of deceiving someone into disclosing sensitive information has existed for a long time. There are numerous definitions of social engineering, some of which are ambiguous and others of which are clear; some will be discussed to clarify what the concept entails.

Wikipedia gives a definition of social engineering as,

'The practice of obtaining confidential information by manipulation of legitimate users.'

The SANS Institute's defines **Social engineering** as,

Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated. The significant part of this definition is the context within which the concept is applied. You could define social engineering as the techniques used to elicit information or manipulate behavior but that doesn't do it justice in the context of information security [1].

Appropriate definition of Social engineering would be:

Social engineering is the use of psychological means to manipulate human behavior. It works by exploiting human error to persuade victims to act against their best interests. In information security, the definition of social engineering refers to tricking people into disclosing personal data online, such as login credentials or financial information.

2. How does social engineering works?

Most social engineering attacks begin with the attacker performing recon and research on the victim. For instance, if the target is a firm, the hacker might learn about its internal processes, organizational structure, industry jargon, potential business partners, and other details. Focusing on the actions and behaviors of workers with low-level but initial access, like a security guard or receptionist, is one strategy used by social engineers. Attackers can search social media accounts for personal information and observe their behavior both online and in person. The social engineer can next use the information gathered to plan an attack and take advantage of the flaws discovered during the reconnaissance process.

If the attack is successful, the attacker may obtain protected systems or networks, money from the targets, or access to private data like Social Security numbers, credit card numbers, and bank account information. In India, credit card fraud is usually committed similarly when someone calls the users, conveys to be a bank official, and asks the users to share the one-time password received on their mobile to safeguard their financial interests or bank accounts, etc.

3. Social Engineering: Cyber threat to cyber security

Cyber Security *"means protecting information, equipment, devices, computer, computer resource, communication devices, and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction"[*2]. Cyber security is a part of information security that relates to the protection of computers, networks, programs, and data against unauthorized access. As cybersecurity includes the protection of both company and personal data, the fields of cybersecurity and data protection overlap. The security objectives of confidentiality, integrity, and availability are of paramount importance to both elements of information security. The recent data breach at the payment from Mobikwik in India is alarming. According to reports, the data breach affected 3.5 million customers, revealing know-your-customer records including addresses, phone numbers, Aadhaar cards, and PAN cards, among other things. Until recently, the corporation has claimed that no such data breach occurred. Only until the regulator, the Reserve Bank of India (RBI), instructed Mobikwik to immediately perform a forensic audit by a CERT-IN impaneled auditor and submit the findings did the business begin engaging with the appropriate authorities[3].

In a cyber security context, social engineering is the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand over control over a computer system. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering. Cybercriminals pretend to be an official representatives sending you an email or message with a warning related to your account information. The message will often ask for a response by following a link to a fake website or email address where you will provide confidential information. The format of the message will typically appear legitimate using proper logos and names. Any information entered into the fake link goes to the cyber-criminal.

4. Cybercrime through Social Engineering

The term **Cybercrime** may be judicially interpreted in some judgments passed by courts in India, however, it is not defined in any act or statute passed by the Indian Legislature. Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. The usage of computers and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience.

Professor S.T. Viswanathan has given three definitions in his book *The Indian Cyber Laws with Cyber Glossary* as follows -

1. Any illegal activity in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

The growth of social engineering crime in recent years has mainly been attributed to improvements in business firms' physical and online security.

2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

3. Computer abuse is considered any illegal, unethical, or unauthorized behavior relating to the automatic processing and transmission of data [4].

Cybercriminals that engage in social engineering are digital con artists, gaining vulnerable people's trust to steal money or data easily. Social engineering fraudsters attempt to manipulate users with a variety of tactics to perform attacks. Generally, they use people's trustworthiness to their advantage and target users that have limited knowledge with regards to keeping their personal/company data safe. Most cybercrime techniques revolve around finding and exploiting weak points in a company's digital infrastructure. Social engineering is different in that it targets employees, not the network itself. Since worker mistakes and misbehavior are the leading cause of data breaches, this method can be painfully effective social engineering attacks are typically more psychological than they are technological. Instead of using sophisticated hacking techniques or in-depth knowledge of computers, they rely on tricking people into giving away information [5].

The most commonly used SE techniques are,

I. Phishing:

The most prevalent form of social engineering used by attackers nowadays is phishing. Phishing scams have unique traits like obtaining personal information from targets, including names, social security numbers, and addresses; using fear, a sense of urgency, and threats to persuade targets to act quickly; and using embed links or link shorteners to direct targets to suspect websites through URLs that may appear authorized or legitimate.

- Most phishing scams seek to accomplish three things at a high level:
- Get personal information including names, addresses, and Social Security numbers.
- Employ shortened or deceptive links that send users to dubious websites hosting phishing landing pages; and
- Use anxiety and a sense of haste to trick the user into acting hastily.

II. Spear-phishing:

Spear-phishing, this technique, on the other hand, is the highly targeted counterpart. A spear-phishing attack can only be executed after initial research, and the content of the message is at least tailored to some extent for the individual target. Social networking sites can be used by cybercriminals to mine data on potential victims, extracting information to create extremely customized messages that would appear to be sent by close friends.

III. Baiting:

Social engineers also use greed to manipulate human operators. Often found on Peer-to-Peer sites offering a download of a hot new movie or music, social engineers dangle something people want and wait for people to take the bait. Once people take the bait, the cybercriminal uses malicious software to corrupt secure systems and steal confidential information or banking information.

IV. Pretexting:

Pretexting is frequently at the center of every successful social engineering attack, but it has several definitions, each of which adds to the confusion. Webster's dictionary describes it as "the activity of posing as someone else to order to get confidential information."

Pretexting is an attack in which the attacker fabricates a scenario to order to persuade the victim to divulge sensitive information, such as a password. A pretexting attack is most commonly seen when someone phones an employee and pretends to be someone in power, such as the CEO or on the information technology team. The attacker convinces the victim that the scenario is true and collects information that is sought [6].

V. **Tailgating:**

Tailgating is an interesting technique and one regularly used by real-world attackers and professional security consultants alike. The basic premise is to leverage an employee's access privileges by following closely behind them as they authenticate to physical security controls such as RFID [7].

Tailgating, also known as "piggybacking," is a social engineering form that involves attackers who have no proper authentication in an organization. The attackers follow employees to obtain access in a restricted area. A tailgating attack often involves attackers who pose as delivery drivers waiting at an organization's parking lot. When the attackers see an employee gaining the security's approval, the attackers who usually carry "goods for delivery" ask the employee to hold the door. Thus, they gain access from someone who is authorized to get into the building [8].

VI. Quid pro quo:

Quid pro quo attacks, like baiting, promise something in exchange for information. This benefit is typically in the form of a service, whereas baiting is typically in the shape of good. One of the most typical quid pro quo assaults is when fraudsters imitate the Social Security Administration in the United States (SSA). These imposters contact random people and ask them to confirm their Social Security numbers, allowing them to steal the identities of their victims. In other cases, the Federal Trade Commission (FTC) discovered that unscrupulous actors built up bogus SSA websites to steal those people's personal information. It is crucial to realize that attackers can utilize less complex quid pro quo offerings [9].

VII. Scamware:

This involves convincing the victim that their computer is infected with malware or that they have accidentally downloaded unlawful content. The attacker then offers the victim a remedy to the phony problem; in actuality, the victim is duped into downloading and installing the attacker's malware [10].

VIII. Watering holes:

Watering hole attacks are a sort of social engineering that is particularly specific. Rather than directly targeting a certain group of people, an attacker will build a trap by compromising a website that is likely to be visited by that group. Industry websites that are often accessed by personnel of a specific sector, such as energy or public service, are an example. A watering hole attack will breach the website and attempt to identify an individual from that target group. Once that person's data or device has been compromised, they are likely to carry out other attacks.

5. Real incidents of Social Engineering:

a) Gang hijacks the email account of UK rail operator Merseyrail

Many employees of British train company Merseyrail in April 2021 received an odd email from their manager with the subject "Lockbit Ransomware Attack and Data Theft." Also copied were journalists from various publications and tech websites. The email showed that Merseyrail had been hacked and had attempted to minimize the event. It was written by a fraudster posing as the company's director. A photograph of a Merseyrail employee's personal information was also included in the email. Although the method of compromise of Merseyrail's email system is unknown (security experts believe it a spear phishing assault), the "double extortion" used in this attack makes it exceptionally vicious. In addition to stealing the company's data and demanding a ransom to release it, The "Lockbit" gang used its access to the company's systems to launch an embarrassing publicity campaign on behalf of Merseyrail's director.

b) U.S Presidential Hacking campaign 2016

In 2016 US presidential election is one of the most famous examples of social engineering. Democratic Party emails and other documents leaked as a result of Spear's phishing attack may have influenced Donald Trump's election victory over Hillary Clinton. Hackers created fake Gmail messages with

links asking users to reset their passwords due to suspicious activity. Hundreds of emails containing important information about the Clinton campaign have since become accessible to scammers.

c) Persuasive email phishing attack imitates US Department of Labor

Bleeping Computer disclosed a sophisticated phishing effort meant to obtain Office 365 credentials in January 2022, in which the attackers impersonated the US Department of Labor (DoL). The fraud exemplifies how convincing phishing attempts are becoming. The assault impersonated the DoL's email address by impersonating the actual DoL email domain (reply@dol [.]gov) and purchasing look-a-like domains such as "dol-gov[.]com" and "dol-gov[.]us." Utilizing these domains, the phishing emails are passed via the security gateways of the target organizations. The emails, which were professionally written and featured official DoL branding, asked recipients to bid on a government project. The ostensible bidding instructions were contained in a three-page PDF with an embedded "Bid Now" button. Better email security procedures were in place at the organization.

d) 2020 Twitter Bitcoin Scam

The Twitter Bitcoin fraud demonstrated that even social media behemoths are vulnerable to cyber-attacks. Prominent Twitter users with the trusted blue verification check mark Tweeted "double your Bitcoin" promises, promising their followers that donations made through a specific URL would be matched. Among the Twitter accounts targeted were well-known leaders, celebrities, and major businesses such as former US President Barack Obama, media magnate Mike Bloomberg, Apple, and others. Because the profiles targeted had millions of followers, the bad actors reportedly got hundreds of contributions in minutes, totaling more than $100,000 in Bitcoin, according to The BBC. A series of highly focused social engineering attacks were used to take control of this account. Malicious actors used Twitter employees to infect people with malware. They then worked their way through Twitter's internal systems, gaining administrative access to a large number of verified users' credentials. Twitter employees were the company's most vulnerable point, falling victim to social engineering attacks that provided bad actors with a backdoor into highly sensitive login information. It's critical to educate your team on social engineering red flags and understand more about how social engineers deceive employees

6. Laws governing the Social Engineering in India:

Social engineering constitutes cybercrime, is punishable under Indian law. There are a lot of statutes and regulations enacted by various authorities that penalize cybercrime. The term “cyber law” is used to address the legal issues occurring in cyberspace. It is an integration of various laws to deal with and resolve such issues and challenges posed by humanity on the web every day. As cybercrime is a field still developing towards specialization, there is no comprehensive law to deal with it, anywhere in the world to date. But the Government of India has the Information Technology Act, 2000 in force to regulate the malicious activities on the web that violate the rights of an internet user. Section 43 of IT act, list out certain acts which when committed without the permission of the owner or the person in-charge of the computer and which amounts to contravention. A contravener under this section is liable to the penalty specified in section 66 of the IT act, which states as follows;

“If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both” [11].

When the IT Act is unable to provide for any specific sort of offence or if it does not include exhaustive provisions with regard to an offence, one may also turn to the provisions of the Indian Penal Code, 1860.The Indian Penal Code, 1860 (IPC) and the Information Technology Act, 2000 (IT Act) both penalize a variety of cybercrimes, and unsurprisingly, many clauses in the IPC and the IT Act overlaps. Sections 415 to 420, IPC detail the law relating to cheating, in the case of Internet Scams relevant sections relating to the crime of cheating such as cheating by impersonation (Section 416) cheating with the knowledge that wrongful loss may ensue to a person where interest if an offender is bound to protect (Section 418), etc. may be applied in case of social engineering fraud. Certain individuals were accused of theft of data and software from their employer and charged under sections 408 and 420 of the IPC and also under sections 43, 65, and 66 of the IT Act. All of these sections, other than section 408 of the IPC, have been discussed above. Section 408 of the IPC deals with criminal breach of trust by clerk or servant and states that "*whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine*" [12].

7. How to prevent social engineering incidents?

Social engineering is one of the most difficult crimes to prevent, as it cannot be defended against through hardware or software. It’s difficult to overstate the importance of preventing social engineering attacks, and the first step in defense is awareness. Precautions to be taken are;

- Research before responding: If the scam is common, you will find others talking about the social engineering method online.
- Don’t interact with a web page from a link: If an email sender claims to be from an official business, don’t click the link and authenticate. Instead, type the official domain into the browser.
- Be aware of strange behavior from friends: Attackers use stolen email accounts to trick users, so be suspicious if a friend sends an email with a link to a website with little other communication.

- Don't download files: If an email requests to download files urgently, ignore the request or ask for assistance to ensure that the request is legitimate.

8. Conclusion:

"Every action and reaction occurring in cyberspace has some legal and cyber legal perspectives"

Technology is evolving and with the evolution is coming disturbing elements surfacing on the dark web. Intelligent people are mis-utilizing their skills and exploiting the internet for evil deeds and sometimes for monetary profit. Thus, cyber law is the need of time. Cyberspace is an extremely difficult terrain to deal with and therefore some activities fall into a grey zone where there is no law to govern them. Thus, there is a long way to go before having a vast and comprehensive law for cyber crimes in India. The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law which ensures cybersecurity.

REFERENCES

[1] Source: SANS paper "The Threat of Social Engineering and Your Defense against It," dated 2003.

[2] Section 2(1)(nb) of Information Technology Act, 2000

[3] Mobikwik data breach

[4] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81.

[5] https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

[6] N.J. Evans, 2009, "Information Technology Social Engineering: An Academic Definition and Study of Social Engineering—Analyzing the Human Firewall," IOWA State University.

[7] Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense-Gavin Watson; pg 266 -267

[8] Social Engineering: *The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception*- Copyright 2015 by Vince Reynolds; pg 7-8

[9] https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for]

[10] https://www.techtarget.com/searchsecurity/definition/social-engineering

[11] https://taxguru.in/corporate-law/offences-penalties-information-technology-act-2000.html

[12] *Gagan Harsh Sharma v. The State of Maharashtra 2019 CriLJ 1398*