An Overview of Social Engineering Attacks and Protection Against Them

Dhruv Yadwadkar
Computer Science
Mukesh Patel School of Technology and Management
Mumbai, India
dhruvyadwadkar@gmail.com

Prayag Vin
Computer Science
Mukesh Patel School of Technology and Management
Mumbai, India
prayag2858@outlook.com

Maharath Sinha
Computer Science
Mukesh Patel School of Technology and Management
Mumbai, India
maharathsinha97@gmail.com

Abstract: Social Engineering is a domain of system security that has posed a serious threat over the years and has become a very effective way of exploiting individuals as well as employees. These attacks have two sides to them, a technical side and a psychological side, hence to understand the concept fully one needs to know both the technical and nontechnical part of it. This persistent threat has increased the need to be aware and knowledgeable about the issue at hand and having the necessary tools to deal with them. This review paper gives a comprehensive overview of Social Engineering and talks about the types of attacks that a system might face, the steps that can be undertaken to prevent a social engineering attack and presents a multi-layered defense model for organizations derived from real-world surveys to ensure practicality.

Keywords: Hacking; Multi-Layered Defense Model; Phishing; Social Engineering; System Security

I. Introduction

System Security has grown to become a very crucial aspect of every single information system, both commercial and domestic over the years. The significant decrease in physical communication and the rise of virtual communication over various networking platforms has aggravated the already persistent problem of hacking. Sensitive data is exchanged through cloud services with minimal security and under the assumption that the end user is a trusted entity. Due to the lack of technically fluent users, websites and social networking platforms have significantly increased their security measures over time. But, with the advancement in data security came an equally rapid development of efficient vulnerability attacks to find new loopholes and equip cyber criminals with fresh perspectives. *Social Engineering* is one of the many threats that systems and individuals face on a day to day basis and has slowly grown to become the most widely used exploitation attack. According to [1], A recent Nuix survey found that 84 percent of respondents used social engineering as part of their attack strategy while another Check Point sponsored survey revealed that 43 percent of the IT professionals surveyed said they had been targeted by social engineering schemes [1]. Every work environment comprises of a network infrastructure and end users who share information via this network. The most powerful tool an attacker can use to exploit this network and retrieve sensitive data is Social Engineering. It is superior to most other forms of hacking because it can breach the most secure systems, as the end users themselves are the most vulnerable part of the system [2]. A study that included more than 4,000 users of Facebook found that most participants are willing to provide copious amounts of personal information in SNSs (Social Networking Sites), thus exposing themselves to various physical and cyber risks [3]. Hackers very often couple Social Engineering with standard hacking techniques to perform large-scale breaches on multinational companies, for instance, the RSA breach and the Ubiquiti Networks phishing scams were one of the most high-profile attacks used to transfer millions of dollars to third party accounts. In fact, in a 2013 interview of FBI Director James Comey, the Director testified before a Senate Homeland Security Committee that cyber-attacks have surpassed terrorism as a major domestic threat, with the threat continuing to rise [4].

This review paper presents a comprehensive study of Social Engineering and contributes the following:

- An overview of social engineering attacks including human and technology-based attacks.
- Analyzing real-world occurrences of successful social engineering attacks
- Providing prevention measures to protect systems from social engineering attacks based on a market survey [5].

Furthermore, the paper provides a basic conceptual model of a defense scheme based on the findings of the previous sections. This scheme serves as a basis for companies or individuals to design their security models on as it helps prioritize assets against Social Engineering attacks, including employee protection and system stability.

II. Types of Social Engineering Attacks

Social Engineering is a multifaceted threat and therefore needs to be dealt with on multiple fronts. In order to deal with these system threats, an acute knowledge of the types of Social Engineering attacks is essentials. They can broadly be classified into Human-Based Attacks and Technology-Based attacks.

A. Human-Based Social Engineering

These are the kind of attacks that take advantage of the human nature and can be carried out by individuals with minimal technical knowledge. The psychological aspect of Social Engineering is what adds to the threat it already poses.

Direct Approach: By the sole use of convincing and psychological dominance, an attacker might obtain sensitive information such as bank credentials, social security number etc. from the victim by direct contact.

Spying and Eavesdropping: An average person is always surrounded by way too many entities that keep him occupied thus taking his attention away from the security of these entities. For example, a person may be engrossed in his mobile phone while at a public ATM and may not notice a bystander peaking and stealing his credentials.

Identity Theft: Posing as a technical expert or a fellow employee helping to 'fix' a problem that a technologically inept employee might not be able to rectify just to steal some confidential information or inject malware into the network.

The table below states various Human-Based Social Engineering techniques and their varying degrees of importance under multiple parameters [6].

Table 1. Human-Based Social Engineering Techniques [1]

Parameters vs Techniques	***Time Consumption***	***Information Provided***	***Role Playing***	***Intensity of Attack***	***Effectiveness***	***Targeted/Untargeted***	***Direct/Mediated***
Impersonation	Most	False	Yes	High	Most	Targeted	Direct
Hoaxing	Less	False	Yes	Low	Less	Targeted	Direct
Confusion	Least	False	Yes	Moderate	Moderate	Untargeted	Direct/Mediated
Dumpster Diving	Moderate	No Need	No Need	Low	Less	Untargeted	N/A
Reverse Social Engineering	Less	False	No Need	Moderate	Moderate	Targeted/Untargeted	Direct?Mediated
Shoulder Surfing	Less	No Need	No Need	Low	Less	Targeted	N/A
Tailgating	Less	No Need	No Need	Low	Moderate	Targeted	N/A

B. Technology-Based Social Engineering

The attacks which require a significant amount of technical knowledge come under this domain. System networks and Internet are often the mediums used to implement these attacks by the intruder.

Trojan Horse: A very common kind of attack carried out by the attacker is when a highly innocuous email is sent to multiple unsuspecting victims. This mail contains an infected attachment that launches a virus or a worm, which eventually infects the entire network system. The 'I Love You' virus and the 'Anna Kournikova' worm are examples of these.

Pop-Up Windows: A rogue program may randomly display a legitimate looking pop-up window asking the user for some of his credentials. This program is used to record sensitive information from the user and feed it to the intruder.

Spear-Phishing: This type of phishing is used mainly by attackers that target specific people or organizations. Threat Group-4127 used spear-phishing tactics to target email accounts linked to Hillary Clinton's 2016 presidential campaign. It is a very elaborate method of hacking as it digs into the personal lives of the victims and then targets them. This method takes an extended period of research on the target and the targets are usually high profile where there is a lot of useable information about them available for free.

Clone phishing: In this type of phishing attack, a legitimate and previously delivered email containing a link or attachment is taken and an almost identical copy of the mail is made with the links and/or attachments replaced with fake ones. The links or attachments are used by the attacker bait

the victim and retrieve sensitive data from them. This technique could be used to gain access to a different machine from a previously infected one by exploiting social trust associated with an inferred connection. In 2006, the total cost of identity fraud in the US was $56.6 billion. Of this amount, 3% was obtained through phishing attacks on home users [7].

Whaling: The term 'Whaling' has been coined for those attacks that are directed towards senior executives and other high-profile targets working for huge, global organizations that hold a lot of political/technical power. In this case, the web page or email used to channel this attack will have a more serious executive-level form. The content of such emails usually includes executive orders, issues, major client-related issue, legal subpoenas, critical business forms and such.

Link manipulation: Many attackers use clever tricks of using the mistakes made by victims to perform social engineering attacks on them. They usually make spoof websites of legitimate sites with one letter misspelled or a wrong domain name with a different address. Thus, when the user types in the misspelled URL they are directed to the false site that belongs to the attackers and they fall prey to a social engineering attack.

The following table charts the 6 most common Technology-Based Social Engineering Techniques and states their degrees of importance under multiple real-world parameter

Table 2. Technology-Based Social Engineering Techniques [1]

Parameters vs Techniques	***Time Consumption***	***Information Provided***	***Role Playing***	***Intensity of Attack***	***Effectiveness***	***Targeted/Untargeted***	***Direct/Mediated***
Pop-up Window	Less	False	No	Low	Moderate	Targeted	Direct
Mail Attachment	Less	False	No	Low	Moderate	Targeted	Direct
Phishing	Moderate	False	No	Moderate	High	Targeted/Untargeted	Direct
Brand Spoofing	Most	False	Maybe	High	Moderate	Untargeted	Direct
E-mail Scam	Less	False	No	Low	Moderate	Untargeted	Direct
Baiting	Moderate	False	No	Low	High	Targeted/Untargeted	Direct/Mediated

III. Successful Social Engineering Attacks

Why understanding and studying real-life examples/case studies based on social engineering attacks important?

In social engineering, the attacker focuses on the user's psychological factors as well as his technical incompetence. Hence, Social engineering coupled with routine security hacks is a cyber criminal's preferred way of manipulating victims. In 2 years over $ 1 billion have been hacked or stolen using Social Engineering attacks in over 100 banks, expanding over 30 countries. Now, this is just the ones which have come to the limelight, there are many others which have been buried by giant multinational companies, to keep their image and stock in control. The average human has tendencies to make mistakes one way or the other, and hence the best way to avoid these mistakes is to study them so that preventive measures can be taken. Same goes for Social Engineering, to develop different preventive measures one must study the past mistakes to avoid the possible future mistakes.

A. RSA SecurID Breach

RSA is one of the first public cryptosystems that is incorporated to ensure the security of sensitive data over a vulnerable network. This asymmetric cryptography algorithm provides the user with two keys, a public key and a private key which are used to encrypt and decrypt the data. According to [10], in 2011 one of the world's best two-factor authentication mechanism known as RSA's SecurID was compromised and fell prey to a social engineering phishing attack. As stated in a blog posted by RSA [10], a small group of employees received two phishing emails over a couple of days with the subject line '2011 Recruitment Plan.' This led to one of the employees retrieving the mail from their spam folder and opening the attached excel file. Blind to the fact that this was a phishing mail, the employee ended up installing a backdoor through an Adobe Flash vulnerability. This resulted in the local network and multiple high-profile accounts being compromised. Due to this security breach, RSA spent about $66 million to recover from the attack and replace all the missing tokens and data [10]. The consequences of the RSA system breach go to

show the power and extent of social engineering as a threat to secure systems and the increased need to become more aware of it.

B. Ubiquiti Networks Breach

Ubiquiti Networks (UBNT) is an American provider of high-performance wireless networking products for businesses. In 2015 it was hit by a cyber-attack which used one of the very common attacks used by social engineering attackers called Phishing. The attacker(s) targeted the finance department of the company and sent out bogus emails to their employees by spoofing the address of a higher-level executive instructing them to make certain fund transfers. No network penetration was carried out until after the initial data phishing phase. This social engineering attack resulted in the transfer of $47 million held by Ubiquiti Networks to a third-party account. Like the RSA breach, a fraudulent email coupled with targeting the more vulnerable employees of multinational companies led to a massive leak of sensitive data as well as money.

C. Watering Hole Attack on Carbon Black (Formerly Bit9, Inc.)

Carbon Black, Inc. (formerly Bit9) is data security company based in the USA that specializes in the protection of computer networks that are bridged to a client device by following a client-server model. [8] Back in 2013, a cybercrime group based out of China named the "Hidden Lynx" used a social engineering technique called Water Holing to infiltrate Carbon Black's security and target their confidential data and customers. Water holing is a more low-key form of security penetration that corrupts a frequently visited legitimate website by injecting malware into it. As stated by [8], Hidden Lynx accessed their infrastructure and injected it with malware which led to multiple Carbon Black customers including various organizations being attacked.

An overview of real-world examples emphasizes on how much of a practical threat Social Engineering is. High profile companies specializing in system security have been scammed for millions of dollars due to incompetence which shows how lethal Social Engineering attacks can be especially when coupled with conventional hacking methods.

IV. Defense Against Social Engineering Attacks

Due to the dual nature of Social Engineering attacks, Psychological and Technical, protection against them requires prioritizing of not just one but two fronts. The increased anonymity that can be achieved over the Internet has added to the risk posed to information systems [9].

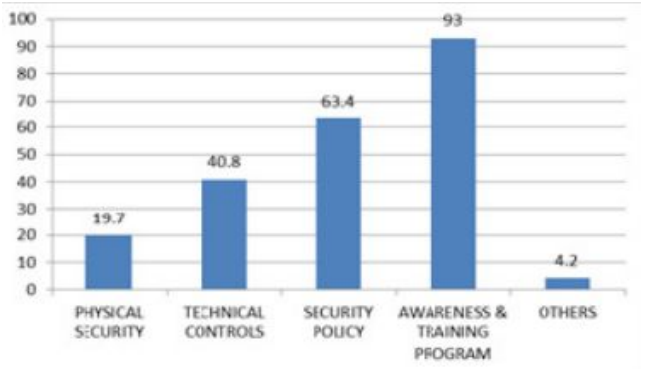

Figure 1. Questionnaire results regarding different safeguards to prevent social engineering attacks [5]

A recently conducted survey at a well renowned IT firm revealed that approximately 93 percent of the employees felt that the prioritization of training programs was essential and about 63 percent believed that a more efficient security policy was necessary [5]. Based on this feedback the following preventive measures were deemed of highest priority for any workplace.

A. *Security Awareness and Training Programs:* With the multifarious threats posed by SE, employee awareness is a crucial tool which enables the user to detect a threat before it might have compromised the system. Another aspect of this is how to rectify or mitigate the damage caused by the detected threat which can be implemented in a work environment by holding timely Training Programs for the employees to equip them with the necessary social and technical tools.

B. *Efficient social and technical penetration tests:* With the constantly evolving nature of vulnerability techniques there is an equal need for cyber security measures to keep growing. Implementing relevant and up to date system network coding languages has never been more important. Hence, constant penetration testing of virtual environments is crucial as it allows an organization to detect network loopholes and fix them accordingly.

C. *Access Control:* Establishing a list of legitimate users with varied privacy settings to prevent any external, unauthorized network attacks. Providing the network users with a two-factor authentication security to ensure confidentiality.

D. *Security Policy:* Introducing workplace security policies to ensure employee activity both online and offline is confidential. The policy should comprise of all measures which are essential to safeguard the company and must be shared with all employees, clients, and partners.

E. *Timely network audits:* Keeping the network malware free by running timely thorough checks and setting up necessary firewalls as suggested by the security officer.

A stable infrastructure incorporating the preventive measures stated above needs to be developed and combined with a technical security module to successfully safeguard a company's assets. Section V. of this paper proposes a multi-layered defense scheme to incorporate measures for prevention, detection and recovery from a Social Engineering attack.

V. Developing A Conceptual Defense Model

The vulnerability of a system against Social Engineering attacks can be reduced significantly by implementing a multi-layered security plan which offers reliable backup and makes up for any weaknesses found in the upper layers of the plan. A good defense scheme merges both the technical and the non-technical aspects to cover multiple areas of threat offered by Social Engineering attacks. These overlapping layers combine measures for prevention, detection, and action to keep the system secure. Based on these facts a multilayered defense plan was formulated to help organizations prioritize their assets and ensure a stable system. A non-technical prevention plan is constructed in Figure 2 based on information from Section IV. Of the paper. Figure 5 shows a technical security plan that can be combined with other modules to draft a solid security plan.

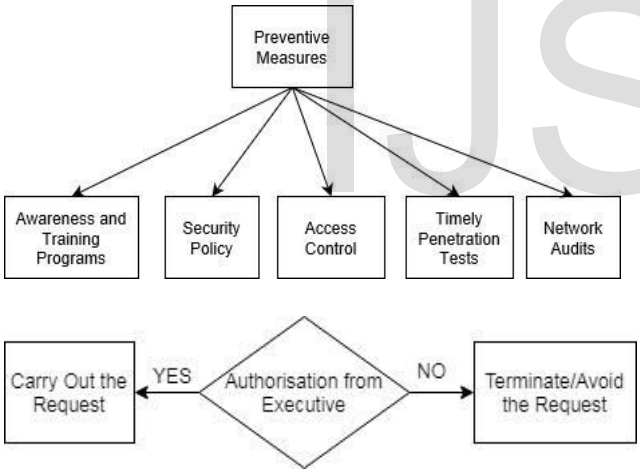

Figure 2. Non-Technical Security Plan

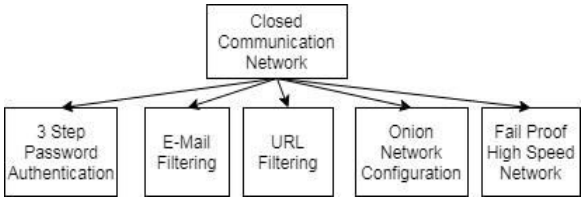

Figure 3. Technical Security Plan

A Closed Communication Network is a necessity in every security module and should include features like:

- 3 step Password Authentication (For when the user forgets the login password) with 128-bit encryption.
- Email filtering to avoid any ill-legitimate emails from bogus ids.
- URL filtering while browsing so that any site does not redirect itself to some other site and takes care of the authenticity of the website.
- The network should be in an Onion configuration (Multiple Server IDs linked together) so that the packet transfer internally can be done securely.
- Lastly, it should be a fail-proof high-speed network so that the security does not compromise the performance.

VI. Conclusion

System users will always be the most vulnerable entity in an organization and therefore system security begins at the user level. Lack of awareness along with inadequate security policies leaves companies defenseless against a potent Social Engineering attack. In this paper, we have provided a detailed overview of Social Engineering, covering the several types of attacks individuals and organizations are susceptible to, real-life occurrences of Social Engineering attacks to show its practicality and relevance in today's age, and listed numerous preventive measures to safeguard oneself from these attacks based on an IT market survey. Derived from the above study and the characteristics of Social Engineering, a basic model was formulated for a multi-layered defense scheme that protects the primary assets of a company from Social Engineering attacks. This scheme prioritizes depth over intensity which is necessary to prevent faults at the employee level as well as the system level. Extensive market research and development is needed in the future to further the advancement of the proposed defense scheme to make it more practical and implementable for companies that are looking to strengthen their security modules. By referring to this multi-layered defense scheme, researchers can get a bigger picture of the threats posed by Social Engineering, and facilitate further research in the subject.

VII. References

[1] Jeff Goldman, "Fully 84 Percent of Hackers Leverage Social Engineering in Cyber Attacks", https://www.esecurityplanet.com/hackers/fully-84-percent-of-hackers-leverage-social-engineering-in-attacks.html, February 2017.

[2] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl "Advanced Social Engineering Attacks", Journal of Information Security and Applications, July 2014.

[3] Abdullah Algarni and Yue Xu "Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models", International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, No. 6, December 2013.

[4] Nabie Y. Conteh and Paul J. Schmick "Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks", International Journal of Advanced

Computer Research, Vol. 6(23) ISSN (Print): 2249-7277 ISSN (Online): 2277-7970.

[5] Anubhav Chitrey, Dharmendra Singh, Monark Bag, Vrijendra Singh "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model," International Journal of Information & Network Security (IJINS), Vol.1, No.2, June 2012, pp. 45~53, ISSN: 2089-3299.

[6] Rohit Dhull , Prof. Sugandha Singh Hooda "Contrast Study of Social Engineering Technique", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 66-68.

[7] Joseph A. Cazier, Christopher M. Botelho "Social Engineering's Threat to Public Privacy", Appalachian State University, April 11-12, 2007, Las Vegas, NV.

[8] Sara Peters, The "7 Best Social Engineering Attacks Ever", Hidden Lynx Watering Hole on Bit9, (https://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=4), March 2015.

[9] Nate Lord "Social Engineering Attacks: Common Techniques & How to Prevent an Attacks", https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack, July 2018.

[10] Lewis Morgan, Real-life examples of social engineering, https://www.itgovernance.co.uk/blog/real-life-examples-of-social-engineering-part-2/, August 2016.