A Taxonomy for Social Engineering Attacks via Personal Devices

Hussain Aldawood
School of Electrical Engineering and Computing
University of Newcastle, Australia
Newcastle, Australia

Geoffrey Skinner
School of Electrical Engineering and Computing
University of Newcastle, Australia
Newcastle, Australia

ABSTRACT

Social engineering attacks are a major threat to organizations and individuals as digitization and connectivity through the internet increase. This study aims to review scholarly research analyzing the topic of social engineering and further chart the evolution of the threat. The review identifies methods of such attacks on various platforms and devices and discusses motivations behind social engineering attacks. Finally, the paper analyzes the nature and impact of social engineering attacks and presents a taxonomy on socially engineered attacks by analyzing their anatomy.

General Terms

Social Engineering Taxonomy

Keywords

Cyber Security, Information Security, Social Engineering, Social Engineering Attacks, Social Engineering Taxonomy, Security Attack Taxonomy.

1. INTRODUCTION

1.1 An Introduction to Social Engineering

Today, organizations are greatly dependent on information systems. This reliance has led to vulnerability to information security threats that put data and people at risk. Furthermore, social engineering fraud has been increasing with advancements in technology. Social engineering is defined in several studies as manipulating and persuading people to disclose sensitive information through online networks or by granting access to restricted areas or systems [1, 2]. Criminals are getting more sophisticated in finding new ways to attack. As a result, organizations have been increasing their investments in cyber security initiatives to safeguard their data. On the other hand, some governments such as Australia have started legislating different laws and regulations against cyber criminals to ensure the protection of citizens and organizations from social engineering attacks and other cyber-related crimes. However, keeping up with perpetrators is challenging. Information security awareness is a crucial step towards having a secure cyber environment in which all types of computer users' (end-users, technical users, employees in different departments, etc.) skill aptitude levels can freely use technology to conduct positive and self-developing activities. In this paper, previous academic papers will be reviewed to broaden the taxonomical understanding of socially engineered attacks. Furthermore, a new framework will be presented to highlight uses of different devices in engineering an attack.

Social engineering attackers use social interaction as a method to conceal their ulterior motives and persuade an employee or an entire organization to correspond to their specific requests. The social interaction leading to a socially engineered attack can range from persuasion to threats devised as ransoms [3]. Recently, there has been a considerable increase in scholarly research analyzing the topic of social engineering. This study will further chart the evolution of social engineering. In addition, this paper will present a taxonomy of social engineering attacks that occur on different devices. Sections 2 and 3 of the paper analyze the nature and impact of social engineering attacks. Section 4 lays the groundwork for the present taxonomy on socially engineered attacks by analyzing their anatomy. Section 5 discusses the proposed taxonomy. It describes different devices used by end-users, which are vulnerable to socially engineered attacks. Section 5 will also explain the types of attack vectors and analyze how social engineering attacks can take place in organizations. Finally, Section 6 concludes this paper by discussing the potential for the taxonomy presented and future research that can be conducted in this direction.

1.2 Emergence of Social Engineering

To better understand the term social engineering, it is important to trace its emergence through history. This term draws its inspiration from the political science field in the early twentieth century. It was then used to represent smart methods of dealing with social problems, drawing its positive connotations from the word 'engineering' [4]. Later, during the Second World War, the term social engineering gained a paradoxical tone of interventions to the natural order that were designed to regulate societal actions and influence people for electoral advantages by politicians [5].

The stereotype of the term during the period still dictates the current negative connotation attached to it with respect to information systems security. It defines cases of organizational or personal attacks that are launched using critical personal information. This information is usually obtained by persuading the humans to reveal sensitive information that otherwise should remain private [6]. For example, an attacker may lead employees to reveal their passwords or access logins to a company's internal network.

The concept gained attention over recent years based on the potency of such attacks. The attack vector may have disastrous consequences, such as organizational hacking, targeted identity thefts, phishing, and malicious links leading to blackmailing [7]. In addition to shedding light on such vulnerabilities, this paper will identify different methods of social engineering attacks, past and present, to create a taxonomy in this knowledge domain.

1.3 Methods of Social Engineering Attacks

Some scholars including Ivaturi and Janczewski [4] have already designed different approaches in suggesting taxonomies of numerous social engineering attacks. These taxonomies include attacks that can either be based on technology, human approach, online perception, or intelligence-based. Additionally, these attacks may further be divided into single or multiple-stage [8]. Ivaturi and Janczewski [4] suggest three major phases in which socially engineered attacks are planned. These include preparation, attack, and post-attack phases. The authors also suggest that attack vectors can be divided into two major categories, which include person-to-person, or person-to-person via media. In person to person, the attacker either impersonates a real or a fake individual to gather intelligence. While, the attack vector via media may encompass text, voice, or video methods.

In addition, Kjaerland [9] highlighted that mere operational viewpoints or process outlooks of social engineering attacks are not always going to provide organizations with a means to an end to counter it. Rather, it is imperative to take the victims of such attacks into consideration. The author suggested classification of the attacks based on source vectors, method of operation of a hacker to carry out an attack, impact or effect of the hacking on the organization, and target sectors or people impacted by the incident.

Furthermore, Krombholz et al. [2, 10] proposed a taxonomy for social engineering attacks involving three main categories of social engineering attacks: channel, operator, and type. As described by the author, the channel comprises the medium of attacks such as email, instant messaging applications, or cloud, among others. Operators can be human or software, and the types of socially engineered attack include physical, technical, social, and socio-technical vectors, such as phishing, dumpster diving, and bailing, among others.

1.4 Research Gap and Need for an Evolved Taxonomy of Social Engineering Attacks

Social engineering employs developmental technologies to launch an attack on an individual, employee or organization as a whole. The literature surveyed and detailed in the following section highlights that social engineering is a dynamic process in which the attackers are motivated to continually perpetrate their actions against the victim(s). As such, existing taxonomies provided by scholars in the field need an updated and more comprehensive framework to protect against evolving social engineering attacks. The gaps pertaining to social engineering attacks include a list of attack vectors, which are not inclusive of all personal devices from which attackers can gain information [4].

Additionally, the distributed collaboration processes of modern organizations and their use of third party channels for their communication needs have not been previously covered in existing taxonomies, nor has the variety of devices available. It also increases the diversity of new attack vectors, thus increasing and the vulnerability of organizations for advanced social engineering attack taxonomies [10]. Any new taxonomy needs to ensure a link between historical and future cases in an effort to assist with the development of early warning signs that could further lead to curbing social engineering cases [9].

2. NATURE OF SOCIAL ENGINEERING ATTACKS

A malicious hacker can use a number of methods to breach information security defenses of organizational information systems. A human-centered approach is one such method. In this section, a review covering attempts to understand the definition and scope of social engineering and to comprehend how the mind of a social engineer functions are provided. The section also sheds light on different methods utilized for social engineering attacks.

2.1 Definitions of Social Engineering

Kumar et al. [2] defined social engineering as “the art of manipulating people into performing actions or divulging confidential information.” Authors highlight that social engineering hackers apply trickery or deception to gather information and accelerate to bigger problems. These include acts such as fraud in accounts of a firm or identity theft, or access to a computer system. These attacks are based on interpersonal information that hackers gain from interacting with an individual, either through direct communication with a person, by phone, or via media communication. Similarly, Schoeman and Irwin [11] defined social engineering as “the science of skillfully maneuvering human beings to take action in some aspect of their lives.” The authors highlighted that social engineering hackers rely on their skills of collecting knowledge on their target enterprises. They target the human element to bypass organizational controls through deception and misinformation. Additionally, Greitzer [12] provided a definition stating that “Social engineering, in the context of information security, is manipulation of people to get them to unwittingly perform actions that cause harm, or increase the probability of causing future harm, to the confidentiality, integrity, or availability of the organization’s resources or assets, including information, information systems, or financial systems.”

The previous three definitions of social engineering highlight that social engineers capitalize on exploiting human psychology. These include exploiting logical flaws in humans and taking advantage of their cognitive biases. Technologies in an organization aim to improve security of information systems. However, social engineers aim to exploit weaknesses linked to human factors [13]. Attackers use the common techniques of phishing, pretexting, baiting, quid pro quo arrangements, and tailgating. Apart from these techniques, this study will further examine and highlight the scope of social engineering attacks to formulate an updated taxonomy.

2.2 Scope of Social Engineering

The scope of social engineering is very wide and gets through organizational information security barriers via insider knowledge, rather than circumventing or breaking them down. The scope of social engineering encompasses everything from trying to gather information about a particular person online to launching specific identity theft attack to dumpster diving efforts to gain access to an organization’s premises [14]. The scope of social engineering attacks is comprised of actions of social engineers to disrupt operation or illicitly acquire information. The scope of social engineers starts from message manipulation to disrupt organizational working structure and extends to the exploitation of firms’ infrastructure [15]. The scope of physical social engineering attacks encompasses retaining first-hand information from a specific user, whereas, the scope of social-based attacks extends to exploitation of emotional and psychological vulnerabilities of a user [16-19].

The scope of social engineering was traditionally limited to email as a primary vector. It was used for spam exploits or phishing. However, with advancement of technologies and network devices, social media enhanced the scope of social engineering further to encompass large volume targets. The attacks use modern devices such as mobile phones, tablets, and other hand-held devices to transport vectors of cyber-attacks. Social gaming available on these devices further provides a platform to deliver phishing payloads by luring individuals [20, 21]. In terms of employees’ security, Wilcox, Bhattacharya, and Islam [22] argue that the scope of social engineering attacks in an organization is dependent upon employees sharing excessively on social media. The authors claim that the increase in employees' exposure to litigation by overuse of communication technologies helps hackers gain access to confidential information. The scope of social engineering attacks is wide and is further increasing with the spread of information technology [23]. Further to the above findings, and in order to fully comprehend the nature of social engineering, one must also understand what motivates social engineering hackers to devise such attacks.

2.3 Understanding the Minds of Social Engineers and their Methods of Attack

A typical social engineering attack includes deceiving a target for purposes including gathering of information, fraud, gaining computer access, or identity theft. However, to understand the intention of social engineers, it is crucial to comprehend the means of interaction used by hackers and the final impact of an attack [2]. Scholarly findings report that social engineers may appear respectable and use this fact as a pretext mask to what they have in mind. Such acts are further intensified by in-person methods of pretending to be a new employee, a person in the role of housekeeping, or even a specialist. Social engineers may use valid credentials to support that identity [24, 25].

Social engineers prefer to take the shortest path to attack an organization. They do not concentrate their efforts in bypassing firewalls; they prefer to ask for information to get around organizational security systems. Methods of attack in the non-technical categories include tailgating, dumpster diving, quid pro quo, and shoulder surfing [16]. While using non-personal techniques such as social networking sites, social engineers are able to see a large user base of information and open grounds for exploiting the vulnerabilities of people. By using a fake account, they may even exploit the weakest link of organizational information security by engaging an employee in small talk on common interests, experiences, or problems. Social engineers may even use reverse attack methods of befriending the victim's friends first and trick them into making a contact [8, 25, 26].

3. IMPACT OF SOCIAL ENGINEERING ATTACKS

The nature of social engineering attacks highlights that hackers have an end goal in mind. The impact on organizations is largely dependent on the attacker's goals that can range from minor issues of gauging the security level of an organization to getting organizational administrative access [27]. Each attack is often different from other attacks. The following section will reflect on the goals of such attacks.

3.1 Goals of Social Engineering Attacks

The primary goal of social engineering attacks is to obtain sensitive information about an organization or gain unauthorized access. Social engineers are manipulative, and their malicious goals may include identity theft of a particular employee. The goals can further be developed into personal property theft or even stealing of organizational assets. Another common goal is network intrusion or system shutdown, leading to disruption of day-to-day operations. Social engineers, through insider knowledge, disturb the financial dealings of a company and even lead to a condition of industrial espionage [28-30].

In addition, social engineers practice various techniques of phishing, such as link manipulation using the common tricks of misspelled URLs, usage of sub-domains, or display links suggestive of a reliable destination. These tricks furnish the goals of sabotaging the information system of an organization, without being detected by the filter evasion techniques [31]. In certain instances, it is the goal of a hacker to constitute an attack in the form of Denial-of-Service. Such attacks are designed to lock users out of their own computing resources, preventing legitimate use of the specified network resources. The goal of such attacks is to sabotage the firm's data. This includes altering the data, stealing it, or even causing its removal, affecting the system performance [15, 32].

Apart from snooping for secrets, a social engineer may have the goal of "Web Defacement." Web defacement is considered graffiti in the digital world, in which the hackers deface websites of an organization. As websites are directly linked to the reputation of the firms and are their commercial public, such an act of defacing the website impacts organizational status adversely [33]. Apart from such ends, social engineers also test the technical information security flaws of an organization. For such goals, they rely on malware applications, which cause maximum damage including financial repercussions. Such malware is software written without any specified goals. The hackers monitor how far it could spread with the information system of an organization. The malware remains dormant in the systems and its exploits can only be witnessed when a technical flaw in the information system is exposed and allows it to spread further [33-35].

3.2 Impact of Social Engineering on Organizations

As the goal of social engineers is to coordinate a deception plan leading employees to reveal information pertaining to their organization, organizational impact of such attacks includes the costs organizations bear for the loss of their reputation. Direct effects of social engineering attacks include disruption of core functions of an organization, exploitation of an end host, infrastructure, or data in transit. The disruptive and exploitive impacts of social engineering have been represented in Figure 1.

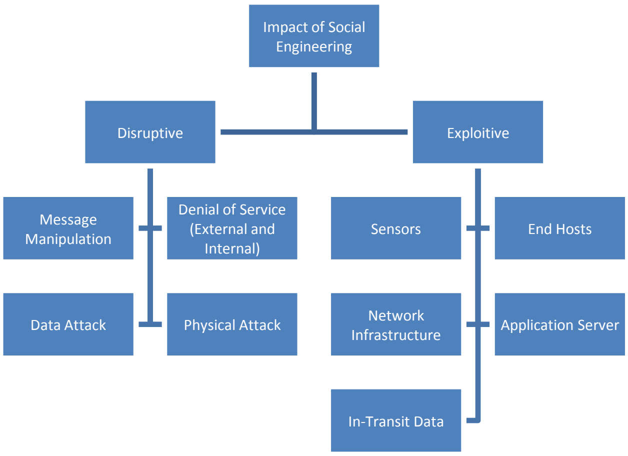

Fig 1: Mechanism of Social Engineering Attacks

Social engineering attacks expose the vulnerability of an organization, which may further lead to a loss of goodwill of the firms. The cost of losing reputation and goodwill has a long run impact on a company's profit line. For example, in the case of an organization losing credit information of its clients, such news discourages other firms from conducting business with the insecure organization [36].

Apart from the impact on the long run profits of the firms, semantic attacks on organizations are characterized by technical enigma. The organizations have to deal with the visible threats at the same time they spend money looking for dormant attacks on their network via user-computer interface [37]. The firms also have to spend money and time on constantly training their employees on new methods of social engineering attacks, as well as devote specific funds to frequently enhance their information security [38].

Additionally, the attacks have an impact on targeted employees. Being a target of such an attack impacts the decision-making capability of the employee directly. Furthermore, such attacks have socio-organizational impacts on the employee for being responsible for a looming threat on the entire organization. The employee may even lose trust and confidence built over the years [39] .

3.3 Defense Mechanisms

The success of social engineering attacks is dependent on manipulating humans to trust their attackers; hence, a defense mechanism is effectively constructed through constant vigilance and education within an organization. It is imperative to recognize social engineering attempts in their early stages with a proactive security and contingency plan. From a management perspective, multifactor authentication security policies strengthen defense mechanisms for the firm [40-42]. A defense mechanism against social engineering attacks is comprised of detection systems in various devices, adjustment of browser settings, and usage of anti-spyware in the network [43]. Technical countermeasures also include firewalls, blacklisting, encryption software, two-factor authentication, and blocking [44].

Firms may choose technologies such as intrusion detection systems, network administrators, and proxy servers to create a perimeter defense against social engineers [38]. Among the defense mechanisms that firms can choose against social engineering attacks is a coordinated defensive deception plan. Mechanisms adopted to form such deception include honeynet centers that mimic the real command-and-control sites of information security. Organizations can also opt for deceptions based on content and object, by luring the attackers with real-looking data or false location of information storage and using non-existent employees in the organization [45, 46].

4. SOCIAL ENGINEERING ATTACK METHODS

Methods of social engineering attacks vary in their scope depending on the creativity and imagination of the attacker. To construct an inclusive taxonomy, social engineering attack methods will be analyzed in the current study based on the types of such attacks and the platforms used in the process.

4.1 Types of Attacks

Although every social engineering attack is unique, to achieve the desired results from an attack, a social engineer follows a four-stage common pattern. These stages include accumulation of data, improvement of the relationship, exploitation, and execution or implementation [4, 9, 37, 47]. Figure 2 shows the common mechanism of social engineering attacks.

In this paper, it is central to provide a taxonomy of social engineering attacks that provides a complete outlook of the nature of such attacks and their impact on an organization. The mechanism of social engineering attacks may combine different methods based on human, technical, computer, social, and physical aspects. Several studies highlight that based on the types of attack, social engineering can be broadly classified into two types: human-based or technology-based approach. Human-based attackers use impersonation, whereas technical attacks are designed to explore online vulnerabilities of the victim. In terms of technical, software-based attacks use various devices including mobile phones and computers to retain information on their targets [15, 16, 18, 19]. Although an attack’s first phase of accumulation of information can be through physical methods of gathering intelligence such as shoulder surfing and dumpster dives, this study concentrates only on the online methods of an attack as a part of our new taxonomy.

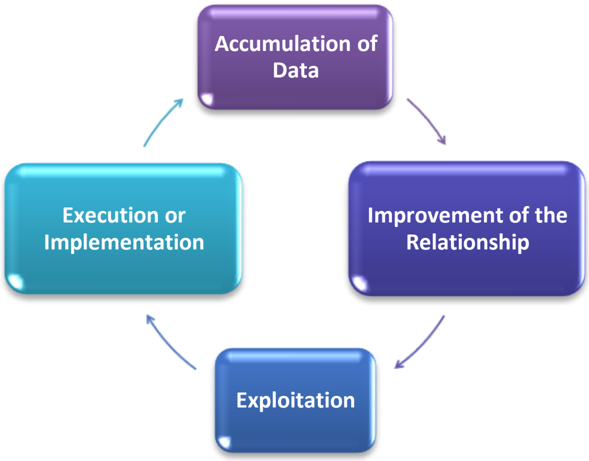

Fig 2: Mechanism of Social Engineering Attacks

In human-based attacks, social engineers use person-to-person methods of attacking the victim. They use methods of guilt, sympathy, ignorance, equivocation, and affiliation to build trust as their ploys to gain access and information. Attack methods include using friendliness, impersonation, conformity, tailgating, pretexting, diffusion of responsibility, and decoys to launch an attack. Also, among the human-based attacks is the method of reverse social engineering in which the attacker presents himself as a person of authority or a friend of a friend to advertise himself. An attacker using a human-based approach provides victims with an incentive to exchange information and persuades them to divulge important information [48, 49].

In attacks using technological methods, the attacker uses media such as texts, search engines, social networks, voice, and video methods. The attacks using texts involve internet media such as browser, email, and even short messaging services. The types of text-based attacks include phishing, cross-site request forgery, malware, email, and popups. The modern methods also include session hijacking attacks, connection-oriented protocol attacks, and SQL injection, inserting malicious code into the user programs from the web giving the attackers a way that they can exploit later. Also, in order to work around different devices, social engineers use the method of search engine poisoning. The method involves usage of unethical techniques of persuasion so an unsuspecting user downloads malware directing them to search engine pages of fake websites. In addition, the attackers may further exploit social networking platforms using fake profiles, message links, malicious URLs and application to launch an attack [37, 44, 49, 50].

Additionally, social engineers using voice methods to devise attacks use cellphones and their networks to exploit the vulnerabilities of their victims. They may use IP-based voice messaging technologies and measures of Vishing. Furthermore, with the progress of new technology, social engineering attacks also extend to include media of videos. Recent attacks also include the use of botnets, rootkits, and superstitious software to impact the devices of the victims [4, 35, 40, 51].

4.2 Platforms of Social Engineering Attacks

Social engineers use various platforms to lure their victims. Some of these platforms are discussed as follows:

4.2.1 Hardware

A hardware platform offers a privileged entry to a social engineer and provides the engineer with access and the ability to manipulate a computing system. In comparison to software, there are no security patches or intrusion detection tools for hardware. Also, there are no anti-virus scanners to detect malicious attacks on periodic intervals. Social engineers exploit these advantages through Trojans such as malicious Integrity Circuits (IC) in the hardware. The attacker exploits on the hacked devices include interference with its computation and bandwidth capability and can impact their performance measures, such as battery power. Social engineering on hardware platforms also takes place through side-channel attacks, opening potential backdoor entry into the organization and allowing for leakage of sensitive information [38, 49, 51].

4.2.2 Software

On software platforms, exploits include cases on incorrect data validation, and social engineers may further use the design flaws and bugs to devise an attack on the user. The attack on software also leads to vulnerabilities such as access privilege, SQL injection, and buffer overflow issues. A buffer overflow attack takes place when there is excessive data in a program’s buffer that further threatens to corrupt adjacent buffers as well [42, 52, 53].

4.2.3 Network Infrastructure

With the expansion of network infrastructure, users are provided with a wide range of protocols that they do not understand. The administrators of official websites may not use efficient encryption, comply with policies of security filters, or apply patches in a timely manner, leaving them vulnerable to social engineering attacks. These attacks include those on the domain names, transmission control protocol, and internet protocol. By attacking any of these network infrastructures, social engineers can impact data transactions and also launch a denial of service attack. Social engineering exploits also include their ability to disguise malicious traffic payloads, making them look legitimate. With a large amount of data flowing through the networks, distinguishing between the traffic payloads becomes difficult [35, 50, 52].

There are many separate proposals and techniques to identify vulnerabilities arising from social engineering attacks in hardware, software and network architecture. To focus on enhancing each layer, this study will present a taxonomy of attacks that are possible on different devices used in the contemporary information system.

5. TAXONOMY FOR SOCIAL ENGINEERING ATTACKS

To focus on each layer of security and look into their bundled security options, it is imperative to look into the taxonomy of social engineering attacks based on the different devices used.

5.1 Mobile

Handheld computing devices are typically mobile devices that have numerous computing services and applications. These devices include smartphones and personal digital assistants (PDAs). Mobile devices are prone to social engineer attacks as they have the capability to connect to a network through SIM and hotspot services. A taxonomy for social engineering attacks via mobile devices is included in Figure 3.

Connectivity on a mobile device includes the mobile network, Wi-Fi, Bluetooth, text or voice, and mobile applications. Phishing attacks expose operating systems and network of browsers on the phone. Phishing attacks can also take place through mobile applications. Social engineering threats include the chance of hackers gaining access to the stored data on phones and stealing users’ related information. The individual is at risk of losing money and sensitive information such as their security logins, passwords, account numbers and contact number. Mobile devices are also vulnerable to phishing attacks through Bluetooth phishing, Instant Messaging Applications, Short Message Service (SMS), and voice overs [54, 55].

Other vectors of attack on mobile devices include luring victims through malicious applications that look like their legitimate version. Malware attacks are designed to download from mobile browsers and include ransomware. Ransomware is used by social engineers to conduct denial of service attacks or even hold important documents as leverage to ensure that the victim is pressured into doing things they otherwise would not [16]. Social engineering attacks using mobile applications are designed to violate application permissions and policies. The attackers sniff information using inter-application exchange and violate the private information security [17, 43].

In some incidents, the mobile platform has also been used by social engineers to spoof the ID of a sender and target individuals on instant messaging applications. To further exploit the information available, attackers hijack user accounts leaving them vulnerable to incidents such as leaking of sensitive information and attack on user privacy [10]. Social engineering attacks in the form of malware that links to the operating system also have the ability to impact the performance of the devices, as in the case of battery draining attacks. Furthermore, attackers through gaming applications on mobile devices also have the capability to conduct traffic flooding attacks in the form of messages and pings or even crashing the system to prevent legitimate users from conducting their work [41].

5.2 Desktop

Desktops have a higher chance of being attacked because of the vulnerability of their hardware. Social engineers can get access to desktops through cloud servers that they are connected to. Through these servers, social engineers can enter the physical servers, switches, routers, power sources, and cooling systems. Since the hardware segment is difficult to comb through for vulnerabilities of attack and lacks the sophistication of software updates to detect any interference with the system, it becomes easy for social engineers. Social engineers through malware attached into communications introduce problems such as worms, virus, Trojan horse, bot attacks, and spywares. Malware can be loaded on to the desktop by offline sources as well. These include USB and flash drives from which the malware propagates to the devices and transfers into the computational logic and embedded systems of the desktops. These attacks enable the social engineers to have control over other network devices in connection using switches and routers. Thus, malwares usually present a higher risk to an entire organizational information system [30, 38, 49, 50].

Furthermore, if the desktop is used by an individual in a large organization to connect with the cloud or any form of internet media such as social networking sites, an attack poses a threat to internal infrastructure. Social engineers have the capability to link to electricity grids through the systems to sabotage internal infrastructure and even initiate information warfare. On the platform level, network connections and web browsers are used by social engineers to launch attacks through malicious scripts and cross-site scripting. These attacks are designed by the social engineers to lure unsuspecting clients into viewing different web pages on their desktop. Attackers hide malicious codes within the platform capable of executing malicious activities on a user's computer [30, 38, 40].

Additionally, the modern technologies enable the social engineers to use standard Internet Relay Chat protocol. These protocols or bots have the capability to link the desktops with a remote connection set up outside the organization. Such command and control server launch attacks through bot masters use the rootkits of the desktop, which prevents the legitimate user from acknowledging that the system is under attack. Certain rootkits also have the capability to avoid detection even when antivirus software is run on the computer. It is capable of modifying boot records of the desktop and beginning to run before the antivirus command is executed [52, 53].

5.3 Tablet

One key feature of tablets is the ease of connectivity. They are now accessible through Wi-Fi and Bluetooth to facilitate communication. Social engineers can use these connections to eavesdrop or even worm-infect the machine by sending files over unprotected networks [38, 56].

Going beyond the simple connectivity services, tablets and handheld devices offer users an increased level of ease to store and edit data. This has led to the increase in sensitive information stored in the tablets. Also, employees use tablets and other personal digital devices to share documents over cloud, email, or other network connection. These documents may contain sensitive information, which can be used by social engineers to launch an attack on the individual or his organization. Social networking sites are also used as a delivery mechanism for social engineering scams. The user logs into these spoofed websites unsuspectingly and is promoted to spread and install malwares [24, 57].

Social engineers can further use vulnerabilities of tablets to exploit devices that are not updated. The attackers are capable of creating issues such as buffer overflow and can access information from the tablet's library to devise an attack against the users. Tablets are also equipped with various application software that poses the same limitation as mobile applications. They expose the user to possible malware, worm, and Trojan attack vectors of social engineering [40, 58-62].

6. DISCUSSION AND CONCLUSION

Social engineering attacks challenge network security and information safety by exploiting the inherent human tendency to trust. These attacks are devised on human intelligence, where the user is led to share sensitive information that can then be used to create financial and emotional damage. Attackers use information from individuals to further gain sensitive information on organizations to cause damage to confidential data. The taxonomy of social engineering attacks based on various devices allows for an understanding of vulnerabilities that exist in the usage of such technologies. Reflection on the academic studies highlights the enhancement in emerging threats with the advancement of telecommunication and information technologies. Threats are also increasingly found on modern devices and network platforms as users do not completely understand security features, and education on all methods of dynamic efforts of social engineering attacks is not easy. Social engineers are able to identify loopholes in security of emerging technologies to expose the vulnerability of the user and use critical infrastructure to devise attacks.

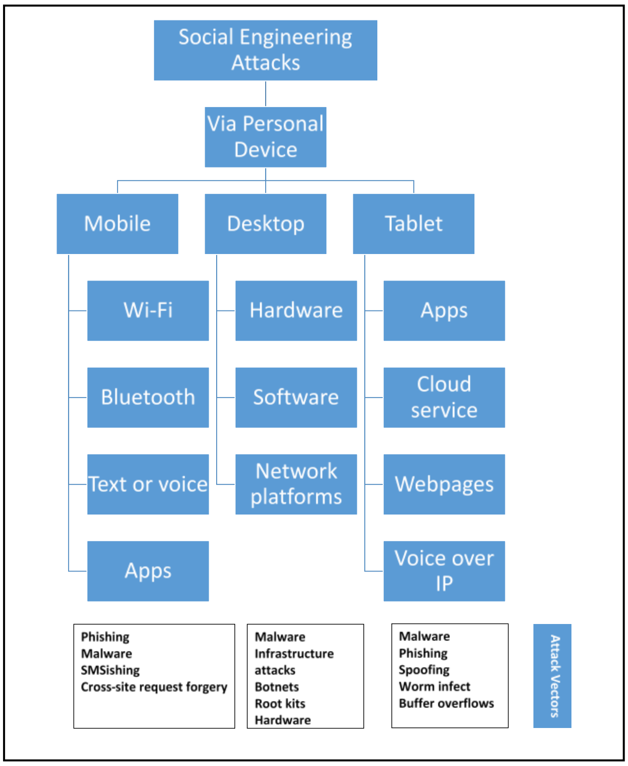

Fig 3: Social Engineering Attacks via Personal Devices

This study highlights the common methods of social engineering attack patterns, outlining a three-phase function social engineers use to lure their users. Attacks may be carried out through a person-to-person method or via media, using techniques of phishing, botnet, and malware to enter user systems through network platforms and social media. The user, however, remains unsuspecting of the attack as the damage spreads into the information system. Social engineers are further capable of using inside knowledge on the firms and its personnel to gain control of the entire command system.

Development of the taxonomy provides a look into the attacks against which security mechanisms are required to preserve user privacy over various platforms. To construct the taxonomy, the current study attempts to understand the mind of social engineers and their attack methods. Our framework in Figure 3 is the formation of a new taxonomy of different social engineering attacks for different types of personal devices.

The current study presents the taxonomy for the social media attack based on the devices of mobile, desktop, and tablets and is based on the impact of social engineering attacks on firms and individuals. Some disruptive attacks of message manipulation take time to impact the entire organizational infrastructure, whereas exploitative attacks impact the sensors and network infrastructure of the organization to adversely impact the organization immediately. The current study presents a review of existing defense mechanisms, such as two-factor authentication methods, firewall, and blacklisting, but recognizes that social engineering is dynamic, and attackers continuously devise new technologies and methods of attack.

Future studies can focus on additional factors that influence users' information security awareness and behavior in order to fill a visible gap in literature. More research including surveys, experiments and case studies will lead to a much better understanding of the flaws in self-reporting as an indicator of users' genuine behavior.

7. REFERENCES

[1] Orgill, G. L., Romney, G. W., Bailey, M. G. and Orgill, P. M. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. ACM, 2004.

[2] Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 2, 11 (2015), 15-19.

[3] Albert, R., Jimenez, A., Keane, S., Mancini, S., Orr, M., Pantazopoulos, R., Reichert, A. and Wentzel, K. The Future of Ransomware and Social Engineering. U.S. Department of Homeland Security (2017).

[4] Ivaturi, K. and Janczewski, L. A taxonomy for social engineering attacks. Centre for Information Technology, Organizations, and People, 2011.

[5] Patel, K. K. and Reichardt, S. The Dark Side of Transnationalism Social Engineering and Nazism, 1930s–40s. Journal of Contemporary History, 51, 1 (2016), 3-21.

[6] Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint arXiv:1606.00887 (2016).

[7] Ablon, L. Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND, 2018.

[8] Algarni, A., Xu, Y., Chan, T. and Tian, Y.-C. Social engineering in social networking sites: Affect-based model. IEEE, 2013.

[9] Kjaerland, M. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security, 25, 7 (2006), 522-538.

[10] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. Advanced social engineering attacks. Journal of Information Security and Applications, 22 (2015), 113-122.

[11] Schoeman, A. and Irwin, B. Social recruiting: a next generation social engineering attack. Journal of Information Warfare, 11, 3 (2012), 17-24.

[12] Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D. and Cowley, J. Analysis of unintentional insider threats deriving from social engineering exploits. IEEE, 2014.

[13] Conteh, N. Y. and Schmick, P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6, 23 (2016), 31.

[14] LeBlanc, J. and Messerschmidt, T. Identity and Data Security for Web Development: Best Practices. " O'Reilly Media, Inc.", 2016.

[15] Harry, C. and Gallagher, N. Classifying Cyber Events: A Proposed Taxonomy. Journal of Information Warfare, 17, 3 (2018), 17.

[16] Salahdine, F. and Kaabouch, N. Social Engineering Attacks: A Survey. Future Internet, 11, 4 (2019), 89.

[17] Koyun, A. and Al Janabi, E. Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST) (2017).

[18] Gupta, S., Singhal, A. and Kapoor, A. A literature survey on social engineering attacks: Phishing attack. IEEE, 2016.

[19] Patil, P. and Devale, P. A literature survey of phishing attack technique. Int. J. Adv. Res. Comput. Commun. Eng, 5 (2016), 198-200.

[20] Ikhalia, E. J. A new social media security model (SMSM). International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae. com (ISSN 2250-2459, ISO 9001: 2008 Certified Journal, Volume 3, Issue 7 (2013).

[21] Arachchilage, N. A. G. and Love, S. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38 (2014).

[22] Wilcox, H., Bhattacharya, M. and Islam, R. Social engineering through social media: an investigation on enterprise security. Springer, 2014.

[23] Narendra, K. and Sreedevi, E. Social Engineering and Defense against Social Engineering (2018).

[24] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. Social engineering attacks on the knowledge worker. ACM, 2013.

[25] Chitrey, A., Singh, D. and Singh, V. A comprehensive study of social engineering based attacks in india to develop a conceptual model. International Journal of Information and Network Security, 1, 2 (2012), 45.

[26] Wilcox, H. and Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise. IEEE, 2016.

[27] Mohebzada, J. G., El Zarka, A., BHojani, A. H. and Darwish, A. Phishing in a university community: Two large scale phishing experiments. IEEE, 2012.

[28] Hadnagy, C. Unmasking the social engineer: The human element of security. John Wiley & Sons, 2014.

[29] Airehrour, D., Vasudevan Nair, N. and Madanian, S. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. Information, 9, 5 (2018).

[30] Gupta, B. B., Arachchilage, N. A. and Psannis, K. E. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67, 2 (2018), 247-267.

[31] Chen, S. Trust Management for a Smart Card Based Private eID Manager. NTNU, 2016.

[32] Van Heerden, R., Irwin, B., Burke, I. D. and Leenen, L. A computer network attack taxonomy and ontology. International Journal of Cyber Warfare and Terrorism (IJCWT), 2, 3 (2012), 12-25.

[33] Nath, H. V. and Mehtre, B. M. Static malware analysis using machine learning methods. Springer, 2014.

[34] Stringhini, G., Kruegel, C. and Vigna, G. Shady paths: Leveraging surfing crowds to detect malicious web pages. ACM, 2013.

[35] Grégio, A. R. A., Afonso, V. M., Filho, D. S. F., Geus, P. L. d. and Jino, M. Toward a taxonomy of malware behaviors. The Computer Journal, 58, 10 (2015).

[36] Laribee, L. Development of methodical social engineering taxonomy project. Naval Postgraduate School Monterey CA, 2006.

[37] Heartfield, R. and Loukas, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48, 3 (2016), 37.

[38] Jang-Jaccard, J. and Nepal, S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80, 5 (2014), 973-993.

[39] Mancuso, V. F., Strang, A. J., Funke, G. J. and Finomore, V. S. Human factors of cyber attacks: a framework for human-centered research. SAGE Publications Sage CA: Los Angeles, CA, 2014.

[40] Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R. and Mas'ud, M. Z. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study, 2011.

[41] Caviglione, L., Coccoli, M. and Merlo, A. A taxonomy-based model of security and privacy in online social networks. IJCSE, 9, 4 (2014), 325-338.

[42] Klaper, D. and Hovy, E. A taxonomy and a knowledge portal for cybersecurity. ACM, 2014.

[43] He, D., Chan, S. and Guizani, M. Mobile application security: malware threats and defenses. IEEE Wireless Communications, 22, 1 (2015), 138-144.

[44] Pienta, D., Thatcher, J. B. and Johnston, A. C. A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries, 2018.

[45] Rowe, N. A taxonomy of deception in cyberspace, 2006.

[46] Pawlick, J. A Systems Science Perspective on Deception for Cybersecurity in the Internet of Things. New York University Tandon School of Engineering, 2018.

[47] Patel, R. S. Kali Linux social engineering. Packt Publishing Ltd, 2013.

[48] Rjaibi, N. and Rabai, L. B. A. Developing a novel holistic taxonomy of security requirements. Procedia Computer Science, 62 (2015), 213-220.

[49] Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R. and Bellekens, X. A taxonomy and survey of intrusion detection system design techniques, network threats and datasets. (2018).

[50] Brar, H. S. and Kumar, G. Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications, 2018 (2018).

[51] Cebula, J. J., Popeck, M. E. and Young, L. R. A taxonomy of operational cyber security risks version 2. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2014.

[52] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S. and Jin, Y. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. Journal of Hardware and Systems Security, 2, 2 (2018), 97-110.

[53] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D. and Wu, Q. AVOIDIT: A cyber attack taxonomy, 2014.

[54] Yeboah-Boateng, E. O. and Amanor, P. M. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5, 4 (2014), 297-307.

[55] Dunham, K. Mobile malware attacks and defense. Syngress, 2008.

[56] Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. and Shabtai, A. Taxonomy of mobile users' security awareness. Computers & Security, 73 (2018), 266-293.

[57] Yoshizawa, H., Ishida, M. and Yoshitsuru, T. Development of and Future Prospects for Tablet Devices. Fujitsu Sci. Tech. J, 49, 2 (2013), 208-212.

[58] Aldawood, H. and Skinner, G. An academic review of current industrial and commercial cyber security social engineering solutions. In Proceedings of the Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (Kuala Lumpur, Malaysia, 2019). ACM, 2019.

[59] Aldawood, H. and Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11, 3 (2019), 73.

[60] Aldawood, H. and Skinner, G. Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. International Journal of Security (IJS), 10, 1 (2019), 1.

[61] Aldawood, H. and Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Sydney, Australia, 2018.

[62] Aldawood, H. A. and Skinner, G. A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. Sydney, Australia, 2018.