INTRODUCTION

Due to the dramatic rise in internet usage, people are now disclosing their personal information online more frequently. Because of this, cybercriminals have access to a lot of confidential information and financial transactions. In a recent study, Huber (2009) defined social engineering as a method of attacking the weakest layer of a data security system; that is the people who use it. Despite the robust security of most infrastructure and networks, they are still vulnerable to attacks from social engineers (Beckers and Pape 2016a). Haunts (2017b) defined Social Engineering as the clever manipulation of the natural human tendency to trust. Social engineering is non-technical, hence it does not require any advanced technical tools, it can be exploited by anyone, and it is cheap (Beckers and Pape 2016b). In order to use this tactic, the attacker, or social engineer, must persuade the target that they are who they say they are or that they are acting in their best interest. Social engineering can be accomplished in many forms, three of which are, phishing, vishing and smishing. In a recent study (Kim et al., 2015) reported that hackers created a fake website and urged users to download free anti-virus software. Many people fell for this scam and lost their credentials to the scammers after downloading antivirus software from these fraudulent websites. One of the most common types of cyberattacks right now is phishing. Phishing is an especially effective form of social engineering that enables cybercriminals to deceive users and steal their credentials. “Phishing is still one of the predominant ways to enter, breach and compromise a company. The reason why it is the major and most effective way to get in is actually the psychology behind it. Psychology plays a large factor in their success rate but also the fact that we as humans are also vulnerable to phishing" (Moltke 2020). Boateng and Amanor (2014) argued that vishing involves a voice phishing attack in which a phone call from the attacker lures the person being targeted into supplying his credentials with the purpose of exploiting that information to cause harm. Smishing, on the other hand, relies on text messages to lure victims into revealing sensitive information. This study examined the psychological method of attack and impact of the Social Engineering attack on Twilio Company. It explains how social engineering works, and how attackers take advantage of human behavior. According to Wikipedia (2019), Twilio is a California-based American company with revenues of US$3.826BILLION and over 8000 employees. Using their web service APIs, they provide programmable communication tools for calling and receiving phone calls, sending as well as receiving text messages, and conducting other forms of communication processes. This study explored the psychological vulnerabilities of Twilio’s staff through individual attitudes and behaviors. It also explored susceptibility to social engineering attacks by deploying the Cyber Kill Chain framework. As such, the paper details how psychological and situational-based security awareness programs can help users and employees reduce cybersecurity attacks. Qualitative and quantitative data was collected from a random sample through an online survey.

ANATOMY OF THE ATTACK

Despite the fact that there are several security software including hardware available on the market, there are several ways of breaching an organization's or an individual's information security defenses. Attackers use social engineering techniques to gain information for purposes such as identity theft, password theft, or other kinds of attacks. To begin their attacks, most attackers follow the Cyber Kill Chain Framework steps, since they provide a path to approach the target safely without being detected. Lockheed Martin (2022b) developed the Cyber Kill Chain framework which illustrates how cyber-criminals go across networks in order to locate and exploit vulnerabilities. Cyber Kill Chain steps are used by attackers to conduct offensive operations in cyberspace. The Cyber Kill Chain consists of seven phases (see Figure 2). This section begins with a study of social engineering attacks on Twilio's network using the Cyber Kill Chain framework adopting some cognitive and psychological bases including data processing, trust, framing, persuasion, deception, acceptance of risks, and situational awareness.

Reconnaissance: Reconnaissance can be carried out online and offline. *"*Shared interest makes success more likely for instance, if you are a fan of Liverpool Football club (LFC) you can spend a lot of time talking about LFC. The attacker will not go straight for the kill rather he takes his time building trust and friendship; good acting helps" (Haunts 2017a). Cyber-criminals use information that does not need verification as well if you say something the person might want to verify. So if the hacker asks the right questions to twilio's employees, they may feel informed by a person with the knowledge. Twilio's employees might be a bit loose with their lips and disclose some Twilio's confidential information to the attackers to make themselves look and feel better. The attacker also deployed elicitation tactics. An elicitation is an act of getting information without asking for it. Most people appreciate politeness and helpfulness. This exploits human nature. People want to appear well-informed so nobody wants to be the guy who doesn't know the answers, it makes you look stupid. "In most cases, this method heavily relies on basic background research, which involves gathering information about a targeted organization. Some of the techniques used to gather this information include shoulder surfing and eavesdropping" (Aldawood H. and Skinner G., 2018).

Weaponisation: At this stage of the attack, cybercriminals developed sophisticated malware to attack Twilio's network. This was based on the information they gathered during the reconnaissance stage. Weaponisation might entail developing payloads or modifying existing malware to use in cyberattacks. For instance, Attackers can modify an existing ransomware variant to develop their Cyber Kill Chain tool (EC-Council 2023a)

Delivery: As illustrated in Figure 2, this stage involves delivering the payload to the target system. The attacker uses a range of techniques to deliver the payload such as email, USB drives, or various web-based exploits. For the case study attack on Twilio, the attacker deployed sophisticated social engineering techniques on Twilio's employees. In addition to having effective communication skills with people, the attacker knows how to adapt communication to fit the situation at hand. The attacker tricked Twilio's employees through phishing text messages. Individuals are likely to fall for this phishing scam which comes in the form of a text message as text messages are personal. As soon as you receive a text message, you read it. We are all biased in some way. Cognitive biases are things in our heads social engineers can break. Cybercriminals can use them against their targets to get their way because ultimately social engineering is using dirty small tricks to get your way. The social engineers used a bias known as doubt avoidance in the Twilio attack. They sent direct phishing sms to the employees' phones that left no room for doubt**.** Attackers increasing their certainty will help them become more convincing and persuasive. If we are unsure about a decision, we make an ill-informed and quick decision to remove any doubt. This will give the attackers high chances of getting their victims to perform the action required of them. Twilio will have firewalls and antiviruses to protect their network and data. However, attackers use phishing emails to make Twilio's employees panic and panic is easy to exploit. We fall for social engineering because of trust bias and help bias (Merrigan 2018).

Exploitation: At this point, the attacker avoids conflict by portraying trust, or the conviction that the other party is acting in a sincere manner. In both the real world and social engineering, trust overcomes suspicion. (Kirmani and Zhu 2007; Deutsch 1958). For example, Twilio employees received phishing messages associated with trust, authority and fear. Incorporating trust into a friendly message encourages compliance. The psychological concepts used here by the attacker are framing, persuasion and deception. Figure 2 defines exploitation stage. According to Kahneman (2011), framing is a means for increasing the persuasiveness of a social engineering text message through manipulating its interpretation by triggering a specific emotion; framing can be utilised in social engineering through personalization and contextualization. The psychology behind this attack is in line with Dr. Robert Cialdini’s principles of persuasion**.** Dr. Robert Cialdini (2006), a popular and esteemed psychologist, proposed the six fundamental principles of persuasion: Authority, Scarcity, Commitment/Consistency, Liking, Reciprocation and Social Proof. In some cases, cybercriminals use the principle of liking to develop trust in their victims or induce specific behaviors by generating fake likes. Similarly, the concept of authority relates to human nature to submit to authority. In their attacks, the attackers posed as the IT department that holds some authority. The concept of scarcity is a form of persuasion that utilizes time-based constraints. For instance, cyber-criminals used time-based constraints to trick Twilio’s employees into believing that their passwords had expired or that their schedules had changed, and that they needed to click on a URL controlled by the cyber-criminals. The attackers deployed limited time tactics to persuade employees to click on the link before time runs out or they face the consequence. Cyber Kill Chain framework premise is human psychology

Installation: At this stage, the attacker starts the attack without alerting the victim. It is imperative to make a victim feel like they have done something good for someone else, enabling potential future interactions. The attacker installs malicious software and other cyber weapons on their network to take control of their system see figure 1.

Command and Control: At this phase of the Cyber Kill Chain, cyber-criminals gained control over Twilio's networks and systems. It is possible for attackers to gain access to privileged accounts, attempt brute force attacks, search for credentials, and change permissions so that they can take over the account **(**Dholakiya 2022). The attackers communicate with the malware they installed on Twilio’s network. The attackers may also use command and control servers to instruct computers to achieve their objectives.

Actions on Objectives: At this phase of cyber-kill framework, the attacker finishes what they started. This is where they reopen that link they got from command and control and pull that information packet by packet; this is so that it is not noticeable and easy to detect (Bitbyte 2020). The Cyber-criminals' objective and final phase of the attack is a carefully designed a perfect escape plan. These attackers gained access to Twilio's customers' data without authorization for a limited time. It is possible that the motive is to steal credit card numbers for financial gain.

IMPACT ANALYSIS

Cybercriminals can exploit the largest vulnerability on earth which is humans. “These people are not just hacking computers they are hacking humans. Because we read, reason and react unlike computers, we actually respond to propaganda” (Huffman 2019). Twilio is one of many successful social engineering attacks. These attacks have serious consequences which are outlined as follows: Cyberattacks can be a traumatic experience that has real and lasting consequences for victims, their families and organisations. Twilio's customers who are also victims of these attacks may also suffer a wide range of emotional responses including long-term mental, physical trauma, shame, embarrassment, distress, sadness and anger (FCA 2022). Once an organization gets attacked by a cyber-criminal, the organization's credibility and reliability are continually questioned. Due to their breach, their customers lose trust in them and their ability to secure their information as their private information, such as names, email addresses, credit card numbers, behavioral metrics, and health information, may be compromised. An organisation that suffers from cyberattacks will suffer reputational damage over the course of several years. For example, other companies like Okta customers, Facebook whom Twilio provides services for were directly affected by this attack. This has badly damaged Twilio's reputation (MS 2021a). “Beyond the obvious ways social engineers steal money is the less commonly recognized implications for instance: In the event of an attack, downtime for your organization can have a negative impact on the bottom line. Then there are the court and legal costs of privacy violations lawsuits" (MS 2021b). When data is stolen from a social engineering attack, aggrieved clients, shareholders, or others may file lawsuits.

REFERENCES

Aldawood, H. and Skinner, G., 2018. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) [online]. Available from: https://ieeexplore.ieee.org/document/8615162 [Accessed 30th March 2023].

Beckers, k. and Pape, S., 2016a. International Requirements Engineering Conference: A Serious Game for Eliciting Social Engineering Security Requirements [online]. Germany. 16-25.

Beckers, k. and Pape S., 2016b. International Requirements Engineering Conference: A Serious Game for Eliciting Social Engineering Security Requirements [online]. Germany. 16-25.

Bitbyte, (2020). The cyber kill chain how / Hackers do what they do [online]. Youtube. Available from: https://www.youtube.com/watch?v=mMkonxKnqHI [Accessed 1st April 2023]

Boateng, Y. and Amanor, P., 2014. "Phishing SMiShing & Vishing: An Assessment of Threats against Mobile Devices", *J. Emerg. Trends Comput. Inf. Sci*, vol. 5,4. 297-307. Available from: https://scholar.google.com/scholar?as_q=Phishing%2C+SMiShing+%26+Vishing%3A+An+Assessment+of+Threats+against+Mobile+Devices&as_occt=title&hl=en&as_sdt=0%2C31 [Accessed 30th March 2023].

Christopher, H., 2010. *Social Engineering: The Art of Human Hacking.* Available from: https://books.google.co.uk/books?hl=en&lr=&id=9LpawpklYogC&oi=fnd&pg=PT7&dq=research+on+social+engineering&ots=vclzIPe7QM&sig=68DzMDfF5a1-ISIhtgzGN9AuThk&redir_esc=y#v=onepage&q=research%20on%20social%20engineering&f=false [Accessed 30th March 2023

Cialdini, B., 2006. *Influence: The Psychology of Persuasion*, revised ed.; Harper Business: New York USA,1–12. Available from: https://cltr.nl/wp-content/uploads/2020/04/Robert-P-Cialdini-Influence-The-Psychology-of-Persuasion.pdf

Deutsch, M., 1958. Trust and suspicion. Journal of conflict resolution. 2(4), 265–279.

Dholakiya, P., 2022. What Is the Cyber Kill Chain and How It Can Protect Against Attacks | IEEE Computer Society [online]. Available from: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks [Accessed 4th April 2023]

EC-Council, 2023a. The Cyber Kill Chain: The Seven Steps of a Cyberattack [online]. Available from: https://eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/ [Accessed 20th March 2023]

EC-Council, 2023b. The Cyber Kill Chain: The Seven Steps of a Cyberattack [online]. Available from: https://eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/ [Accessed 20th March 2023]

Financial Crime Academy, 2022. Impact Of Fraud [online]. Available from: https://financialcrimeacademy.org/impact-of-fraud/ [Accessed 3rd April 2023]

Hube, M. and Kowalski, S., Nohlberg, M. and Tjoa, S., (2009). *Towards automating social engineering using social networking sites,* Proceedings - *12th IEEE International Conference on Computational Science and Engineering CSE*

2009, vol. 3, pp. 117-124, 2009[online]. Available from: https://ieeexplore.ieee.org/document/5283344 [Accessed 5th March 2023]

Huffman E., 2019. Human Hacking. The Psychology behind cyber security [online]. Youtube. Available from: https://www.youtube.com/watch?v=FrNLE1Ixgak [Accessed 3rd March 2023]

Hutchins, E., Cloppert, M. and Amin, R., 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* [online]. Available from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed on 5th March 2023]

Kim D., Yan P., Zhang J., 2015. *Detecting fake anti-virus software distribution webpages. Computer and Security* [online]. 49, 95-106. Available from: http://dx.doi.org/10.1016/j.cose.2014.11.008 [Accessed 5th March 2023]

Mitnick Security, 2021. How Social Engineering Can Affect an Organization [online]. Available from: https://www.mitnicksecurity.com/blog/how-social-engineering-can-affect-an-organization [Accessed 3rd March 2023]

Moltke, M., 2020*. NCC Global Group A Hacker's Confessions - The Psychology of Phishing* [Online Youtube] Available from: https://www.youtube.com/watch?v=AQLxyjuDTwQ] [Accessed 2nd March 2023]

Haunts, S., 2017a. Hacking Humans: Social Engineering Techniques and How to Protect Against Them. NDC Conference. Sydney. [online]. Available from: https://www.youtube.com/watch?v=YVqurfWzB-Q [Accessed on 18th March 2023]

Haunts, S., 2017b. Hacking Humans: Social Engineering Techniques and How to Protect Against Them. NDC Conference. Sydney. [online]. Available from: https://www.youtube.com/watch?v=YVqurfWzB-Q [Accessed on 18th March 2023]

Kahneman, D., 2011. Thinking, fast and slow. Macmillan. 18th West Street Newyork United states.

Kirmani, A. and Zhu, R., 2007. Vigilant against manipulation: The effect of regulatory focus on the use of persuasion knowledge. Journal of Marketing Research 44(4). 688–701.

LockheedMartin, 2011a, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [online]. Available from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed on 20th March 2023]

LockheedMartin, 2011b, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [online]. Available from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed on 20th March 2023]

Merrigan, S., 2018. The Pyschology of Social Engineering. NDC Conferences[online]. Oslo. Available from: https://www.youtube.com/watch?v=wDY_SPfed7c
[Accessed on 18th March 2023]

Mouton, F., Malan, M., Leenen, L. and Venter, S., 2014. Social engineering attack framework. Information Security [online]. South Africa. pp. 1-9. Available from: https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework [Accessed on 20th March 2023]

TwilloBlog, 2022. Incident Report: Employee and Customer Account Compromise [online]. USA: Twillo Inc. Available from: https://www.twilio.com/blog/august-2022-social-engineering-attack [Accessed 23/03/2023].

WikipediaContributors, 2019. Twilio [online]. Available from: https://en.wikipedia.org/wiki/Twilio [Accessed 1st April 2023].

APPENDIX

Social Engineering

The Social Engineering Attack Framework

Goal	The attackers are motivated by money and the challenge of successfully hacking into a high security system, meaning in other words the goal of the attack is financial gain. Engaging in cybercrime can be both thrilling and lucrative.
Target	They target Twilio through the employees of the company to steal their financial and personal information.
Social Engineer	The cybercriminal / attacker are social engineers.
Communication	During this stage, the attacker builds relationships and trust using the information he gathered.
Medium	Using direct text messages to impersonate authority figures within the IT department
Technique	The technique used in this attack is phishing sms
Compliance Principles	Psychology authority bias confirmation

Figure 1: Table showing The Social Engineering Attack Framework

THE CYBER KILL CHAIN FRAMEWORK

Reconnaissance	This is the first step in the Cyber Kill Chain and involves searching for potential targets before a cyber-attack. The reconnaissance stage includes the attacker identifying Twilio, and uncovering their vulnerabilities with the weakest link employee.
Weaponisation	As part of the weaponisation stage, the attacker creates malware designed to attack Twilio as an identified target. Weaponisation could involve creating new types of payload or modifying existing tools to penetrate Twilio's networks.
Delivery	Cyber weapons and other Cyber Kill Chain tools are used in the delivery phase to penetrate Twilio's network and reach their employees. Sending phishing emails with malicious attachments and using elicitation techniques to get Twilio's employees to click on them is a particular form of delivery.
Exploitation	The exploitation phase follows the delivery and weaponisation of a cyberattack. Attackers exploit vulnerabilities identified in previous attacks to further penetrate Twilio's network and achieve their objectives.
Installation	When the attackers accessed Twilio's network through social engineering, they started the installation phase of the cyber kill chain. This is done by installing malicious software and other cyber weapons on their network to take control of their system. This is done to steal customers' data. Attackers may use Trojan horses, back doors, or command line interfaces to install cyber weapons and malicious software at this stage.
Command and Control	Cybercriminals use this phase of the Cyber Kill Chain to interact with malware they have installed on Twilio's network to achieve their objectives. The attackers exploited stolen personal information to gain access to Twilio's network and some of their internal databases. This enabled them to access confidential client data.
Action on Objectives	After gaining control of Twilio's network, The attackers initiated the final phase of the Cyber Kill Chain:they were able to access certain customer date.

Figure 2: Table showing Cyber Kill Chain Framework

(Lockheed Martin 2011a; EC-Council 2023b; Twilio Blog 2022)