# Efficacious Tactics, Mechanics and Heuristics for Progressive Social Engineering

Ujas Dhami

*Department of Computer Engineering, Silver Oak University, India*

**Abstract**
With increasing digitalization and company infrastructure over the years, the attack vectors in computer security have been enormously metastasizing. In scope, several breaches and intrusions have been dominantly carried out by one common tactic, Social Engineering. The domain has gained momentum over the years in successful compromisation of assets[1]. Metrically, Social Engineering proportionately, has been considered one of the most dangerous weapons of any threat actor and consecutively, one of the most dangerous threats to any company's human resources[2]. As per *Cobalt's Cybersecurity Statistics of 2021*[3], 61% of organizations globally, have faced breaches carried out by Social Engineering attacks. Moreover, *proofproint 2021 State of the Phish Report*[4] recognizes Social Engineering attacks as emerging attacks with devastating potential. These type of attacks are often undervalued by employees and the IT staff for majority of the companies. This paper will brief about the new tactics I used, as a threat actor, endeavouring to make the most out of a persuasive conversation, involving *(i)* physical hooking, *(ii)* telephonic attacks, and *(iii)* neuro-anatomical deductions briefing how the existing Social Engineering attacks can emulate the neurochemical processes inside the brain.
*Keywords:* Social Engineering, Cyber Security, Company Culture, Crime, Enterprise Security, Cyber Threats

*Corresponding Author
*Email Address:* ujasdhami@gmail.com (Ujas Dhami)

## I. Introduction

*1.1* **On Context of Work:** Most Social Engineering attacks are architected by using simpler neural tools, to alter the thoughts of the target and to deceptively provoke him into triggering an event of mental instability, causing a *neural buffer breach*[5] and unintentionally leaking out requisite information without his prior knowledge. Today's Social Engineering is far more perplexed than the available human and technical tools used primitively. Enterprises have already implemented rigorous topologies of tackling with attacks depicting Social Engineering[6]. Still, the attacks maintain their position at the peak in weaponization and conducting breaches [1]. There are various newly-born attacks for Social Engineering, professionally known as *0days*, which have been experimented socially, by tampering with the primitive tactics and deriving new techniques for doing so. Mechanics of these attacks vary from the attack surface to the culture of the target company. And the same will be framed in this work.

*1.2* **On the Objective:** This work aims at demonstrating the various new tactics and methodologies of successful Social Engineering compromisations, involving human behaviour, verbal tools, honeypots, and neural outreaches.
Note: The attacks performed on the targets are then acknowledged to them, as to being a part of the experimentation execution.

*1.3* **On Benefits:** Through this work, the reader will acknowledge the various tools for conducting enterprise-level Social Engineering and also the cultural prerequisite for companies to adapt in order to challenge these multi-procedural repercussions. Moreover, the work reflects the idea of envisaging a neuro-anatomic postulation towards the process of Social Engineering and heuristics of various other successful attempts I have conducted for this particular research.

[1]Most of the compromisations involve Spear-Phishing, Pretexting, Homographs and Honeypots which are studied and referenced to other advanced attacks covered in the paper.

[2]Methodologies of effective planning and scale in regards to preventing Social Engineering are scarce. Thus, company cultures and small-scale start-ups do not have well-defined models for the same.

[3]https://cobalt.io/blog/cybersecurity-statistics-2021

[4]https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[5]Neural Buffers are temporary containers storing encoded information in the Hippocampus of the brain. This can very much contribute towards Social Engineering paradigm.

[6]https://www.esecurityplanet.com/trends/best-defenses-against-social-engineering-attacks/

## II. Review of Literature

*2.1* **Social Engineering: Hacking into Humans [2]**

In this paper, the author demonstrated the various types of individual and aggregated attacks performed by hackers and other social engineers, which, on the organizational scale, involves:

1. Phishing
2. Spear-Phishing
3. Baiting
4. Watering-Hole
5. Pretexting, and
6. Quid Pro Quo

These customary attacks provide a sceptical representation of how employees are targeted by specific actors and are encouraged into propagating information, which in return, impacts the integrity of the company and arises extremely circumstantial questions among its consumers about the data-sharing policy of the company.

*2.2* **Social Engineering Guide [3]**

Jason Tribby has exemplified phishing and other *P2P* and *P2B* attacks by a cognitive approach, illustrating how the act of Social Engineering can be possible through interactions. The work covers the methods of preventing these attacks with a substantial proposition on how companies have started implementing steps to counteract basic Social Engineering attacks and online frauds in order to keep their employees shielded from conferring out confidential and policy-protected information to external entities.

*2.3* **Cyber Crime through Social Engineering [4]**

This work escalates the surface of Social Engineering and leverages the use of malwares to infect the target entity with technological tools for encapsulating the malware and propagating the same. The author has proposed efficient approaches towards entities through the particular malwares:

1. Trojan Horses
2. Dumpster Diving through Cache Poisoning
3. Spywares/MITM

These techniques/malwares can be an efficient tool in compromisations and from the statistics of the Social Engineering surface, the maximum SE has been done through imitating Google T1 Cloud applications, followed by Facebook and Twitter. The work briefs methodologies of the same by using existing tools to craft the payloads and transmit the same by synchronous channels.

## III. Research Methods

Prerequisites of this work include tools, scripts and statistics to develop a multi-synchronous cluster to examine and execute required contrivances to the target. For the demonstration, the entities are assigned $E_x$, the threat actors are assigned $TA_x$, and other variables are self-assigned during the demonstration. The research pivots from a P2P interaction to a *P2G* compromise, involving intel gained from all the entities present in a group/sub-group. TAs can vary from one person to a sub-group, depending upon the targeted surface and the level of the compromise[7]. The tools used are verbal, technical and potentially coercive. During attempts, I act as a TA with an intel about the target I am approaching to, for preventing any kind of counteractions and if so, stay composed and predictive about the same. The research involves entity-specific gimmick actions and attacks used to alter the target's neurochemical balances, governed by the Prosencephalon inside the brain. Some attacks are used as a daisy-chain to escalate the attack surface to other elements, whereas others are constructed to target a specific role/entity inside the company infrastructure.

*3.1 Counterfeit Provocation Attack*

Derived from human psychology, behavioural sciences and the report from the *BetterHealth channel*[8], anger and rage affect the neural complexes of the brain, encouraging bodies to go in a state of scrimmage and this can affect the Parietal Lobe of the brain, outputting a confused state of mind. Circumstances involve emanating crucial information to adversaries, if carried out the attack effectively.

$TA_1$ plans a Counterfeit Provocation Attack *(CPA)* on $E_1$, working in a company C. $TA_1$ wants to know the location of $E_1$ and where he is sitting at the moment, so he can acknowledge whether to barge in his office being a rogue employee, or not. For this thing, he would call $E_1$ and the conversation pivots as follows:

$E_1$: "Hello?"
$TA_1$: "Is this Jeremy Flinch?"
$E_1$: "Yes?"
$TA_1$: "I recently examined your work reports and am disappointed of what an unprolific output you have given to the company lately."
$E_1$: "Excuse me? Who is this?"
$TA_1$: *(enraged)* "I need to talk to you personally regarding your neoteric project and hope you do not bring your unproductive visionary ideas this time. See you in your office at 2."
$E_1$: *(vexed)* "I'm sorry, but I need to know who's this. And for your kind information, sir, I've been working at C since the past 3 years and I have contributed decent to the company. If you want to know more, you can approach Mr. Thomas about my contributions in the SAARS project which was the recent one."
$TA_1$: *(bluntly)* "Oh, I personally am acquainted to Mr. Thomas and he also undercover got disappointment in your contributions. This is why we are arriving at your office."
$E_1$: "Oh, is Mr. Thomas arriving either? That's strange, and over the spot, I'm not in my office. I am on a vacation to Spain for 2 weeks, sir. Please check my register kept in my top drawer at my desk. You'll be acknowledged to the META project documents, if you want to discuss about the recent project details. Also, do I know you?"
$TA_1$: "Certainly. We'll talk along with Mr. Thomas over a cup of coffee once you return. Let's see what you've got."
*(hangs up)*

From the above illustration, a TA can effectively purloin information about an employee or an authority by constituting specially crafted sentences which can directly impact the critical parameters to which the entity is dependent on. In this case, $E_1$ was dependent on the job and if someone raises questions regarding the same, the chemical processes inside the brain get tampered and hormonal changes take place, with Cortisol decrement and increased arterial tension, which makes $E_1$ vulnerable to giving out the TA's intended information, being susceptible of a successful CFA.

[7]The more the surface, the more Social Engineers get involved in the exploitation process. This can either be P2G or G2P.

[8]https://www.betterhealth.vic.gov.au/health/healthyliving/anger-how-it-affects-people

### *3.2 Oppressive Rejoinder Attack*

This attack targets the entity's mental state and oppresses him to carry out operations by simulating an environment depicting intense urgency and coercion of acquiring the desired result. One way of doing so, is to call an ISP and make the spokesperson reveal sensitive information about the victim through implementing a state of hastiness.

For this experimentation, as modus operandi, I played the role as a TA, calling an ISP *X*, trying to unsheathe information about an entity E, through Oppressive Rejoinder Attack *(ORA)*. The operation was carried out by the consent of E and the entity was then notified about the same. The attack expedites as follows:

X: "Thanks for calling X, how may I help you?"
TA: *(playing audio of loud car horns in the background)*
"Hello? Ah yes, I'm E's husband and I'm trying to log- oh god what the heck?!"
X: "Hello? Sir?"
TA: "Get aside man! *(audio of people arguing starts playing)*
Hello? *(with a loud pitch)* Ah yes I'm E's husband and we are trying to log into her account but it isn't working despite trying with the right *(noise of horns)* credentials, so can you just verify her email to be `E@email.com` or not? We operate this account jointly. *(people arguing)* Oh get off the road!"
*(plays a female voice saying "Yes, please.")*
X: *(briskly)* "Oh um, okay sir, please wait a moment."
TA: *(car horns intensify) (enraged)* "Make it quick, sir! We are short of time!"
X: "No, sir, the email address you specified-"
*(TA interrupts)*
TA: *(enraged) (arguing in the BG)* "Can't you see we've been holding it since an hour! Get off and clear the damn traffic! Oh, I'm sorry, what were you saying? *(loud pitch)*"
X: *(high pitch) (briskly)* "Sir the email address is `E@email.net` and not the one you specified."
TA: "Ah okay! Wait a moment. E, try the email `E@email.net` now and check it out."
*(horns repeat)*
TA: "Huh! Hello?! The passcode is still incorrect! *(a person arguing noisily)* Dude I'm waiting here since an hour because of this mess! *(high pitch)* Clear this out! Hey, what a dross system you built for your company! I'm not buying this and log us in! *(horns continue)*"
X: *(pestered)* "O-Okay sir! Will it be good if I change the passcode for you? You may change it later on."
TA: "Make it quick! *(BG arguments escalate)*"
X: *(briskly)* "Okay sir, what you want your passcode-"
*(TA interrupts)*
TA: *(arguing in the BG)* "You're damn responsible for this!"
X: "Um, sir? What would you like the passcode to be?"
TA: *(high pitch)* "Hello?! Yes, E, what do you want your passcode to be? *(after 4 seconds)* Ok, make it `E#1234`."
X: "Ok. Your passcode is set, sir."
TA: *(horns continue)* "Alright, thank you."
*(phone hangs up)*

Through the above experiment, TAs can make use of the basic psychological advantage of mental oppression to extract plausibly a very decent amount of information out of any particular employee who is not aware of the company policies and customarily sharable information. TAs have to find ways to exploit X's mental contemplation and make him run down operations through coercion and haste, as any job toped-off under hounding can have an 85% possibility to yield down imperfections. In this case, X, as an ISP's customer care spokesperson, was not authorized to change the passcode of E's account. But under pressure and accessibilty, he quickly changed the passcode under the TA's request, intending to not leave him off with negative feedback about the ISP.

According to the stress analysis report by *The Lincoln College, UK*[9], under pressure, the brain stops functioning due to the flooding of Cortisol in the body, causing the heart rate to increase, and so does the breath, making ORA an extremely fruitful attempt of information gathering.

### *3.3 Corporeal Syndication Attack*

This tactic, potentially, is performed on on-premise groups or individuals by a TA, and is an extension to the traditional Elicitation. The methodology involves physical contact of both, the threat actor and the entity. Corporeal Syndication Attack *(CSA)* involves a topology of a successful execution. The attack can be performed by both Grouped Threat Actors *(GTAs)* and TAs. The topology comprises of three phases, required for the TA to follow in order to gain the intended information from E. The steps include:

i. Fellow Feeling

The first step towards CSA is comforting the target(s). The victim(s) should feel safe around the TA(s) and shouldn't mind being acquainted to them. The body posture and gestures of the TA(s) shall be highly welcoming.

E: "Humidity's ruining up the fun."
TA: "An air-conditioned lounge with an electrolyte-infused drink is what I peg."
E: *(smiles)* "Sounds righteous."
TA: "Taylor Morgan, nice to meet you over sharing same sentiments about humidity."
E: "E, nice to meet you either."

ii. Support and Agreements

Being supportive and concurring can significantly build trust among parties [5]. It takes a matter of minutes for the entity(s) to get friendly if the TA(s) goes on supporting his/their opinions and shares his same which are oriented to the succour of the victim(s). This can highly impact trust relationships and only takes minutes to form.

iii. The Attack

Once enough trust is established and the victim starts divaricating his personal/professional anecdotes, the TA can then plan to stage the attack. Again, he will require specialized sentences to alter the consciousness of the entity. This can be done either by convincing the entity from crafted statements, or intoxicating him through alcohol or hypnotics. Once the target is eligible for being executed the attack on, the TA can extract information as follows:

TA: "I agree. The developers we hired in recent days are near the knuckle. I mean, how can you expect someone working on an outdated version of the most important framework in our application to be of any use? The devs use .NET 3.5, what a waste."
E: "3.5? That's pathetic. At least my people know how to play a fair game. They're at 4.30319. Making an app for them is pretty easy these days, as F# is moving itself on the inner side with

[9] `https://alumni.lincolncollege.ac.uk/news/mind-goes-blank/`

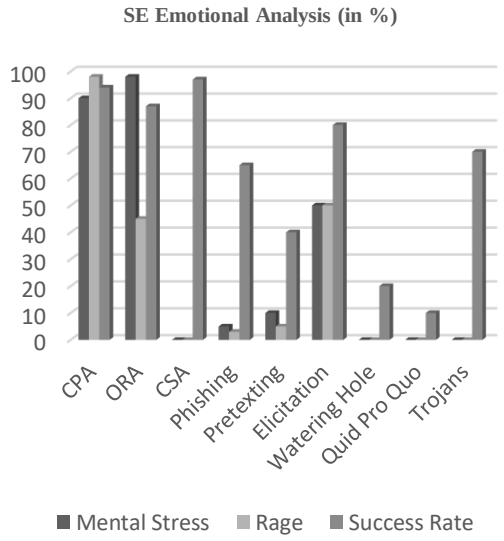
CIL these days. That's decent of the Microsoft code monkeys. What'd you say about this?"
TA: "Absolutely."

Through this methodology, the attacker can extract information out of any individual or group in a matter of minutes. All that is required, is the perfection in dialogue architecture. In the above experiment, the entity provides information about his company application's infrastructure and which version it is using. Since his .NET version is comparatively old in regards with the newly released versions, the TA can effortlessly conduct a breach into the application, using exploits released for .NET v4.30319. CSA can significantly be efficient in information gathering inside physical environments.

### *3.4 A Mental Approach to Traditional Social Engineering*

Phishing is undoubtedly one of the most primitive forms of Social Engineering attacks. Over the years, Social Engineering has gained an aggregated form of several elements combining into one. With Social Engineering, millions of people and companies are hooked as victims by these attacks because of the advanced tools and methodologies for doing so [6]. With this acknowledgement, several other Social Engineering attacks have been developed which can drop upon the victims a mental stress or impact them in some way or the other. Traditional Social Engineering, on the other hand, is stealthy and smartly forged.

Based on the experimentation statistics, I have cobbled a graph representing the Emotional Analysis of several Social Engineering attacks developed till date, plus the attacks I carried out for the research. All the attacks have been carried out for the research and all the entities have been apprised about the same.




Social Engineering is carried out mostly on the internet in the present days [7], and all of the tactics graphed above can be used to target specific individuals, groups or companies technically. However, they are not so efficient as awareness and modus operandi is already equipped by people on how to prevent the common Social Engineering attacks. Thus, non-technical approach towards these attacks make them exceptional.

## IV. Findings and Analysis

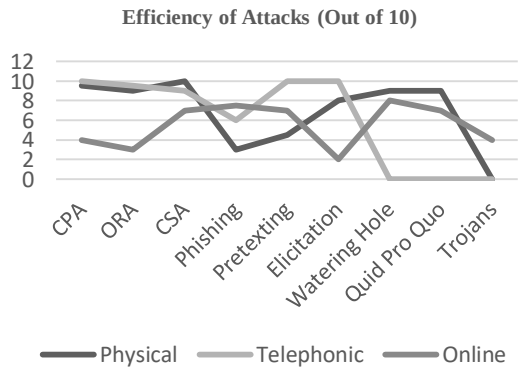
Through the research, a few deductions were made on the implementation of these attacks on entities. Each of these attacks have been carried out numerously, with inscribing the mental output and the topology of the attack's succession with each entity. Collectively, after finalizing the experiment, an average deduction out of all documented particulars was calculated. The output was then put down into tabular forms, as follows:

*$T_1$: Prerequisites and Plausibility of the Experiments*

| Attack | Technical tools as a prerequisite | Can be performed over a telephonic connection | Possibility of counterattacks |
|---|---|---|---|
| CPA | No | Yes, and also can be performed physically. | Yes. Recommended to research about the entity first. |
| ORA | No | Yes, and is highly effective through this method. | Yes. Specialized sentences required for bypassing doubt. |
| CSA | No | Yes, but is less efficient comparatively, from physical execution. | Yes. Make sure the entity has gained enough trust. |

From this table, the prerequisites and the possibilities of the experiments can be determined. However, the attacks are not limited to non-technical surfaces, but rather are recommended to originate from the same.

Traditional Social Engineering attacks have gained enough popularity to get detected easily. Employees can detect a fake email, or a hyperlink [8]. Modern solutions involve architecting automated systems which can auto-detect a mail to be malicious or legit, by comparing the Digital Certificates and the Certificate Authority (CA) of the receiving and the sending party. Programs can now auto-visit a link through automated scripts (called bots) to check if the hyperlink is really safe for the receiver to visit to. If they find a port-forwarded tunnel, they immediately can raise alerts to the user, about the link being a phishing link. In these scenarios, technical approaches to SE are less effective than physical or telephonic. Below is the observation chart of the commonly-used SE attacks and the three attacks demonstrated in the work.




Through the above compiled statistics, it is clearly observable that the experiments covered in the work are comparatively

more efficient to carry out than the common attacks Social Engineers use in their assessments. The attacks do have a weak technical stronghold, but they are extremely fruitful to execute in situations where telephony or physical meetings are viable. However, these attacks can be performed using technical tools in fusion with the existing Social Engineering attacks which are technologically more effective. As per the statistics above, Pretexting and Elicitation can be fused with either of the three experiments and can be conducted online. The effectiveness will gradually increase, depending upon the scrutiny of the threat actor and the victim.

## V. Prevention Strategies

For majority of the attacks, there are various countermeasures present in order to acknowledge individuals and companies on how to prevent being social-engineered [9] [10] [11]. There are numerous methodologies derived from the existing security parameters companies are holding to mitigate these attacks. This section will list all those techniques, along with some additions derived from the attacks covered in the paper.

Prevention algorithms for these attacks are extremely important at the Enterprise scale, as it can substantially affect the company's reputation, consumer trust for data privacy and existing projects. Thus, these prevention strategies will cover everything you need to know for mitigating such Social Engineering attacks.

i. Stay Aware about Company's Data-Sharing Policies

Policies keep changing with time, so does the data collection and sharing algorithms. Every employee has to precisely go through the data-sharing policies as they are the most vital source any threat actor will go for. As a whole, the company shall determine steps for acknowledging its employees the importance of the new policy, also the changelogs. It reserves the responsibility of ensuring every employee has construed the changes.

ii. Entertain No Special Cases

Many companies fail to acknowledge its employees about potential Social Engineering scenarios covered in the ORA and CSA. The employees should be made prepared to tackle such situations with uttermost patience and presence of mind, especially the ones sitting in the customer care department.

iii. Improvise Company Culture

A good company culture is one of the most important parts of any firm. For improvising company culture, the companies have to take required steps; organize events, arrange public presentations, have competitions and other challenging tools which can improve individual skills, grow more awareness inside the campus and discuss challenges together, involving Social Engineering.

iv. Implement TACACS+

Terminal Access Controller Access Control System+ (TACACS+) provides detailed information on logons, accounts and *Access Controls (ACs)*. It is a flexible system responsible for perpetuating and providing administrative controls over authentication and authorization. TACACS+ is a very important instalment for any middle-scale or large-scale company for maintaining accountable access to all the employees within and outside the company perimeter [12]. TACACS+ can be used to mitigate Social Engineering, as employees will have limited access to every element inside the company's network *(intranet)* and can only access directories and instances required for their roles. With this strategy, even if an employee becomes a victim of a Social Engineering attack, because of the limited controls, he would not be able to give out or tamper sensitive information.

v. Use Multi-Factor Authentication

For the online attacks being carried out, the usage of Multi-Factor Authentication *(MFA)* is the first prerequisite for any employee to attain, whether working in the campus or a secure facility. If, by any case, he is exploited by Social Engineering, the threat actor will not be able to pivot down to his machine because of MFA.

vi. Use VMs for Opening Links

Links from unknown/impersonated sources are abominable and should be opened in a *sand-boxed environment*[10]. If the link contains a malware, the malware will not be able to propagate to the host, if executed in a *Virtual Machine (VM)*[11], as the VM creates its own network and shares the internet connection with the host through *NAT*[12]. However, *Bridged connections* are susceptible to propagating extremely unstable malwares to the host.

vii. Prevent Keeping Workstations Unattended

Hackers or Social Engineers can simply plug-in a *USB Rubber Ducky*[13] to the unattended workstation, fetching out all the saved passwords, NTLMv2 hashes and other critical information while the employee is away. And this takes no more than 3 seconds to accomplish. Thus, always log off the account before leaving the desk.

viii. Appoint Social Engineers to Test Employees

An assessment once every year or half is required to test the company's employees for their vigilance and cautiousness in exchanging information to outside parties. Ethical Social Engineers can create a similar environment, simulating a threat actor and testing employees about how aware they are and this can determine the company culture and how much more awareness is needed to be delineated to them.

ix. Always Verify a Software's Checksum

*Checksums* are blocks of data used to verify the integrity of the software [13]. Checksums can usually contain a MD5 hash and can be verified by running *certutil* inside a PowerShell window, and *md5sum* or *sha1sum* inside a linux terminal, or can be installed using a package manager for the same. If any file has an invalid checksum, the file either is tampered, or replaced by a rogue file and should be deleted immediately.

x. Change Passwords Once 3 Months

Changing passwords is a crucial step towards Enterprise Security. Variable passwords often prevent threat actors to maintain persistent connections on infected machines.

[10]A sandbox environment isolates the host machine with a VM for testing untrusted code or programs.
[11]A virtual machine virtualizes computer architecture, providing all the benefits of a physical computer virtually.
[12]NAT is a method of mapping an IP address as a single address representing a network to the internet.
[13]Rubber Ducky is used for plug-n-play credential stealing and other attacks based on automation scripts.

## VI. Conclusion

Throughout the paper, several Social Engineering experimentations were (i) demonstrated, (ii) acknowledged, (iii) compared and (iv) foreseen. The neuroanatomical statements were given in order to support the success rate of the experiments and how they can be leveraged. The existing Social Engineering attacks were compared with the ones experimented by using a different attack topology, or which were derived from them, having a success rate more than the currently available SE methodologies. Moreover, analysis of human emotions and efficiency of the attacks were presented and compared, with all the three experiments manifesting to be the most efficient out of all. With demonstrating the process of exploitation using those tools, the strategies of mitigating them were also listed down. Individuals/Enterprises can successfully mitigate a decent number of the Social Engineering attacks by implementing the same in their campuses and daily operations. However, Social Engineering is an emerging domain and attacks will continue to transpire. Actively arising awareness and educating people about the same can dwindle SE attacks to a miniscule extent.

## VII. References


[1] C. Hadnagy, Social engineering: The art of human hacking, Wiley, 2010.

[2] Lohani, Shivam, Social Engineering: Hacking into Humans (February 5, 2019). International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 2019, Available at SSRN: https://ssrn.com/abstract=3329391.

[3] Tribby, Jason, Social Engineering Guide (April 20, 2021). Available at SSRN: https://ssrn.com/abstract=3830143 or http://dx.doi.org/10.2139/ssrn.3830143.

[4] Panwar, Ayush, Cyber Crime Through Social Engineering (January 28, 2014). Available at SSRN: https://ssrn.com/abstract=2386521 or http://dx.doi.org/10.2139/ssrn.2386521.

[5] K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security, Wiley, 2001.

[6] Alharthi, Dalal and Regan, Amelia, A Literature Survey and Analysis on Social Engineering Defense Mechanisms and INFOSEC Policies (2021). International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.2, March 2021, Available at SSRN: https://ssrn.com/abstract=3830208.

[7] B. Blunden, "Manufactured Consent and Cyberwar," in Proc. LockDown Conference, 2010.

[8] JOURAU, Chizari Hassan, Zulkurnain Ahmad, Hamidy Ahmad, Husain Affandi, 2015/01/01, 188, 198, Social Engineering Attack Mitigation, VL – 1, JO. International Journal of Mathematics and Computational Science.

[9] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," *2015 International Conference on Cyberspace (CYBER-Abuja)*, 2015, pp. 91-100, doi: 10.1109/CYBER-Abuja.2015.7360515.

[10] Spinapolice, Matthew, "Mitigating the risk of social engineering attacks" (2011). Thesis. Rochester Institute of Technology. Accessed from https://scholarworks.rit.edu/theses/394.

[11] T. Mataracioglu and S. Ozkan, "User Awareness Measurement Through Social Engineering,"arXiv preprint arXiv:1108.2149, 2011.

[12] V. Ravi, N. R. Sunitha, R. Pradeep and S. Verma, "Formal methods to verify authentication in TACACS+ protocol," *2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT)*, 2017, pp. 1-4, doi: 10.1109/ICECIT.2017.8453431.

[13] David Basin (Ed.). 2021. ACM Trans. Priv. Secur. 24, 1 (January 2021).