Asian Journal of Research in Computer Science

Volume 17, Issue 12, Page 234-251, 2024; Article no.AJRCOS.128138
ISSN: 2581-8260

Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures

Ntogwa Ng'habi Bundala [a*]

[a] *Tanzania Police Force, Police Headquarters -Dodoma, Criminal Intelligence Bureau, Tanzania.*

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Article Information

DOI: https://doi.org/10.9734/ajrcos/2024/v17i12541

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/128138

Original Research Article

Received: 17/10/2024
Accepted: 21/12/2024
Published: 27/12/2024

ABSTRACT

Cyber professionals and general users are still challenged on how to secure cyberspace and their related activities. The primary challenge remained difficulty in identifying the perpetrators of cybercrimes due to the anonymous nature of the internet and the use of sophisticated and stealthy techniques by attackers to hide their identities. The emergence of advanced crime in cyberspace such as Advanced Persistent Threats (APTs) unlike traditional cyberattacks, APTs are characterized by the use of stealthy tactics, including advanced evasion techniques and zero-day vulnerabilities, making them challenging to detect using conventional security measures. Therefore, this study aimed to explore the techniques, psychological tricks, technical tricks, and countermeasures using the two models of cyberattacking: cyber kill chain and cyberattacking process phase's models. The study applied the Systematic Literature Review (SLR) and Autoethnography methods. The sample of 305 sent (replied) emails from the Yahoo account of the Author from 2012 to 2024. The OSINT techniques are used to verify the empirical validity of the 10 spammed message contents. The study found that in traditional phishing, the attack uses a

**Corresponding author: E-mail: bundalantogwa@gmail.com;*

Cite as: *Bundala, Ntogwa Ng'habi. 2024. "Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures". Asian Journal of Research in Computer Science 17 (12):234-51. https://doi.org/10.9734/ajrcos/2024/v17i12541.*

combination of tricks such as false identity and financial lures, emotional manipulation and trust through divinity and love psychological tricks, involvement of the trusted figure usually the religious leaders, direct solicitation of personal information, urgency and action. In general, we conclude that phishers usually a combination of blended psychological and technical tricks to manipulate the recipient into providing personal information and facilitating the scam. Notably, phishing attacks start with psychological tricks to induce or deceive the target to accept the technical tricks such as clicking the link or downloading. Therefore, we recommend that cyber professionals and general users engage in cognitive training to raise cybersecurity awareness.

Keywords: Cybercrime; modus operandi; phishing attack; psychological tricks; technical tricks.

1. INTRODUCTION

The rapidly evolving threat landscape increases the challenge for cyber professionals and general users (Soares, 2023; Bhadani, 2024). Cyber threats are constantly changing, with new vulnerabilities, malware, and attack techniques emerging regularly (Soares, 2023). These changes challenging to stay ahead of potential threats and design effective security solutions (Junaid and Schaffer, 2024). Organizations must continuously update their defense strategies, which can strain resources and require ongoing training (Bhadani, 2024). Some studies describe the complexity of IT Environments, insufficient resources, data privacy regulations and lack of skilled personnel are common challenges (Kausar, Leghari, and Iftikhar, 2023; Nyre-Yu, 2021). Moreover, many organizations struggle with limited budgets, personnel, and tools for implementing robust cybersecurity measures and conducting thorough investigations (Kausar et al., 2023). The resource constraints can lead to inadequate security controls and slower response times during incidents (Dhondwad, Sakhare, and Bukshete, 2024). On the other hand, compliance with varying data protection laws (e.g., GDPR, HIPAA) can complicate security planning and investigations (Dhondwad *et al.,* 2024). The investigators must balance the need for access to data with legal and ethical considerations, which can hinder the investigation process (Kausar et al., 2023; Ware, 1979). Some studies evidenced that there is a shortage of qualified cybersecurity professionals, making it difficult for organizations to find and retain skilled staff (Gnanasekaran et al., 2024; Junaid and Schaffer, 2024). This talent gap can lead to inadequate security planning and delayed incident response (Gnanasekaran et al., 2024).

In addition, coordination and communication, incident detection and response, attribution challenges, integration of security solutions, and user awareness and training are common challenges in cybersecurity solutions (Gnanasekaran et al., 2024; Nyre-Yu, 2021). The delayed detection can result in more severe damage and longer recovery times. Moreover, *identifying the perpetrators of cybercrimes can be difficult due to the anonymous nature of the internet and the use of sophisticated techniques by attackers to hide their identities (*Gnanasekaran et al., 2024; Junaid and Schaffer, 2024). For example, the emergency of Zero Trust and Advanced Persistent Threats (APTs) are among the most sophisticated cyber-attacks, often orchestrated by highly skilled adversaries with considerable resources (Bhadani, 2024). Unlike traditional cyber-attacks, APTs are characterized by the use of stealthy tactics, including advanced evasion techniques and zero-day vulnerabilities, making them challenging to detect using conventional security measures. APTs typically target government agencies, defense organizations, critical infrastructure, and large corporations (Karabacak and Whittaker, 2022).

Traditional security measures are often insufficient in detecting and mitigating APTs, necessitating the adoption of advanced detection strategies and multi-layered defense mechanisms (Karabacak and Whittaker, 2022). Behavioral analysis, threat intelligence, and machine learning play pivotal roles in detecting APTs, while multi-layered defense strategies, proactive threat hunting, and incident response are essential for mitigating these threats (Karabacak and Whittaker, 2022). As the cyber threat landscape continues to evolve, organizations must remain vigilant and proactive in their efforts to counter APTs effectively. The complexity and stealth of these cybercrime increases the challenge for investigators and cybersecurity professionals to deal with. It *complicates investigations and can hinder legal actions against cyber criminals (*Junaid and Schaffer, 2024*). On the other hand,*

*organizations often use multiple security tools and technologies, which may not integrate well with each other (*Junaid and Schaffer, 2024). Furthermore, human factors are often the weakest link in cybersecurity, employees may be unaware of security policies or best practices (Gnanasekaran et al., 2024). Insufficient training can lead to increased susceptibility to phishing attacks and other social engineering tactics (Junaid and Schaffer, 2024; Soares, 2023).

Therefore, we notice that the fundamental or primary challenge for cyber professionals and general users such as investigators and service providers is the *difficulty in identifying and confining perpetrators of cybercrimes due to the anonymous nature of the internet and the use of sophisticated and stealth techniques by attackers to hide their identities; also they lack a compressive understanding on technologies, techniques, tools that cybercriminal uses (*Junaid and Schaffer, 2024; Dhondwad et al., 2024; Karabacak and Whittaker, 2022*).* In other words, cybersecurity professionals and investigators lack understanding of the *cybercrime modus operandi;* hence, became a challenge. In this study, we aimed to introduce the modus operandi in the two important attacking plans (models) which are the cycle of cyber attacking (Cyber Kill Chain) and the Cyberattacking Process Phases models. Jaikanth and Madisetti (2024) conclude that understanding the structural differences between the attack cycle and phases aids organizations in developing more robust incident response plans by recognizing that tactics may evolve throughout the attack.

Moreover, the findings of Martin (2022) emphasize that while phases represent tactical execution, the cycle encompasses a broader understanding of attacker motivations and adaptation, indicating that defenses should be both phase-specific and cycle-oriented. Therefore, the objective of this study is to explore the modus operandi of the cycle of cyberattacking (cyber kill chain) and the cyberattacking process phases. The study benefits cybersecurity professionals and investigators to establish robust cybersecurity solution plans in their organizations. Specifically, the study established the definition and interpretation of the term cybercrime modus operandi to establish all *entry*, *executing, exiting,* and *escaping* techniques, tricks, and tools. This is because cyber attackers plan how to enter, execute, exit, and escape (Bhusal, 2021). This broad definition and interpretation of cybercrime modus operandi helps cybersecurity professionals and investigators to be familiar with techniques, tools, and tricks in the overall planning process of the cyberattack. Hence, they can prevent and combat cybercrimes.

2. LITERATURE REVIEW

Modus operandi (MO) is a Latin term that means a method of operating (Turvey, 2013). It is comprised of acts and decisions that are necessary to commit a crime and any related choices made by an offender. In other words, the term modus operandi refers to the specific offender behaviors at crime scenes (Sundberg, 2020). Law enforcement has long held to the belief that understanding the methods and techniques criminals use to commit crimes is the best way to investigate, identify, and ultimately apprehend them (Turvey, 2013; Sundberg, 2020). An offender's MO behaviors are learned, and by extension, they are dynamic and malleable (Turvey, 2013). This is because MO is affected by time and can change as the offender learns or deteriorates (Turvey, 2013). MO is best used to help guide investigators to more certain evidence and keep their efforts on course (Turvey, 2013).

Recently, the emergency of the modern crimes that are committed by computer and information technologies such as cybercrimes, poses a challenge for traditional investigators on how to identify and map for modus operandi of those crimes, particularly, the cybercrimes. This is because cybercriminals hide their behavior or techniques of committing crimes. Understanding the modus operandi of cybercriminals is a vital concern in developing effective cybersecurity solution strategies (Pospisil, 2020). Cybercriminals employ a variety of techniques to compromise systems, steal sensitive information, and exploit vulnerabilities (Pospisil, 2020). The Modus operand of cybercrime is still a challenge because they quickly adapt to the new technology and use the new technology to modify or improve their modus operandi. For example, the emergence of Advanced Persistence Threats (APTs) and Zero-Day Vulnerabilities pose a great challenge (Karabacak and Whittaker, 2022). These crimes are persistent, sophisticated, and stealthy (Bhadani, 2024). Therefore, we need to learn its modus operandi.

On the other hand, several studies have been done to explain cybercrime techniques.

ProofPoint (2024) classified cybercrime into four (4) categories, namely cybercrimes against individuals (CAI) such as E-mail spoofing, spamming, phishing, social engineering, cyber defamation, cyber harassment, and cyberstalking (ProofPoint, 2024). The second class is cybercrime against property (CAP) which includes credit card fraud, internet time theft, and intellectual property crimes (TTU, 2024; ProofPoint, 2024). The third class is the cybercrime against organizations (CAO) which includes unauthorized accessing of computers, denial of service, computer contamination/virus attacks, e-mail bombings, Man –in- Middle (MITM), salami attacks, logic bombs, trojan horse and data diddling (ProofPoint, 2024). The fourth class is cybercrime against society (CAS) which includes forgery, cyber terrorism, web jacking, and cyberwarfare (TTU, 2024).

3. METHODOLOGY

The study applied the Systematic Literature Review (SLR) and Autoethnography methods. SLR is a research methodology to collect, identify, and critically analyze the available research studies, such as articles, conference proceedings, books, and dissertations, through a systematic procedure (Carrera-Riveraa et al., 2022; Pati and Lorusso, 2018). An SLR updates the reader with current literature about a subject-cybercrime modus operandi (Carrera-Riveraa et al., 2022; Kitchenham and Charters, 2007). On the other hand, Autoethnography is a qualitative research method that combines autobiographical writing with ethnographic analysis (Mengista, Soromessa, and Legese, 2020). It allows researchers to explore their personal experiences while contextualizing them within broader cultural, social, or political frameworks (Yang et al., 2021). This method emphasizes the interplay between the individual's narrative and the collective experiences of a particular community or culture (Mengista et al., 2020). It is a powerful research method that bridges personal experience with cultural analysis (Carrera-Riveraa et al., 2022). Therefore, we collected 305 sent (replied) emails from the Yahoo account of the author and sorted the conversation of spammed messages. Of 305 messages, 10 were spammed messages which the author replied to at the different stages of phishing from 2012 to 2024. Hence, the author became familiar with empirical psychological tricks and technical tricks by phishing attackers. This experience is used as the self-testimony empirical validation of the cyber-tricks in this study. The Open Source Intelligence (OSINT) technique was used to verify the content of the spammed messages from the phishers.

4. RESULTS

This study aimed to introduce a new concept of interpreting and determining the modus operandi of the cyber kill chain and cyber-attack phases. Therefore, the introduced new definition of the cybercrime modus operandi includes techniques, tools, tricks, objectives, and determinants of the cybercriminals. Moreover, this study described the cybercrime countermeasures for each cybercrime modus operandi in the cyber kill chain and cyber attacking phases.

4.1 Definition and Interpretation of MO of Cybercrime

According to Turvey (2013), an offender's MO behaviors are learned, and by extension, dynamic and malleable. It is affected by time and can change as the offender learns or deteriorates. It is comprised of acts and decisions that are necessary to commit a crime. Moreover, MO is related to the means and techniques used by the criminal to enter and leave the crime scene (Sundberg, 2020). These studies overlooked the nature of cybercriminals who apply both psychological and technical tricks to deceive their targets. They describe the traditional crimes such as rape and burglary. Therefore, this paper fills the theoretical gap in the definition and interpretation of cybercrime modus operandi in cyberspace. In that sense, we extract the fact that what the criminals do at the crime scene is the modus operandi determined by their prior and after (post) plans. The prior and after (post) plans are part of the modus operandi (Bhusal, 2021). Therefore, *we define the modus operandi in cyberspace as the dynamic learned (acquired) specific or unique means, characteristics, actions, or behavior possessed or shown by the cyber attacker in entering, executing, exiting, and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before (prior), during and after(post) the cyber-attack.* This is mostly influenced by time and technological changes.

4.2 The cycle of Cyber Attacking and Cyber Attacking Phases

The terms "cycle of cyber attacking" and "cyber attacking phases" can often be used interchangeably, but they can imply slightly

different focuses. The Cycle of Cyber Attacking its focus emphasizes the *iterative nature* of cyber-attacks (Jaikanth and Madisetti, 2024; Martin, 2022). It refers to the complete process from initial reconnaissance to the final objectives and potentially back to reconnaissance for future attacks (Yadav and Rao, 2015). In summary, while both concepts describe stages of cyber-attacks, the "cycle" emphasizes the ongoing nature and potential for iteration, whereas "phases" highlight the specific steps taken during a single attack.

4.2.1 Cyberattack cycle (Cyber kill chain) modus operandi

Cyber kill chain in simple terms is an attack chain, the path that an intruder takes to penetrate information systems over time to execute an attack on the target (Martin, 2022; Yadav and Rao, 2015). It breaks down a cyber-attack into a series of sequential steps, hence helping organizations understand and analyze the different phases attackers go through, enabling them to improve their defenses and incident response strategies (Jaikanth and Madisetti, 2024; Martin, 2022). The stages are summarized (Fig. 1).

Fig. 1 shows the cyber kill chain or the cyber attacking cycle, which is the intruder takes to penetrate information systems over time to execute an attack on the target (Yadav and Rao, 2015). The cycle or chain contains eight stages. The first stage is reconnaissance. This is the initial phase where attackers gather as much information as possible about the target (Jaikanth and Madisetti, 2024). Attackers may also conduct network scans to identify active devices, open ports, and potential vulnerabilities (Yadav and Rao, 2015). The goal is to build a comprehensive profile of the target to identify the best points of entry (Yadav and Rao, 2015).

The second stage is the weaponization. In this stage, attackers create a malicious payload that can be delivered to the target. Weaponizing involves the design and development of two components which are remote access tool (RAT) and Exploit (Yadav and Rao, 2015). RAT is a piece of software that executes on the target's system and gives remote, hidden, and undetected access to the attacker, usually called payload, this can be client or server (Yadav and Rao, 2015). On the other hand, an exploit is the part of a weapon that facilitates the RAT to execute. Exploit acts as a carrier for the RAT and uses system/software vulnerabilities to drop and execute the RAT (Yadav and Rao, 2015). The major objective in using exploits is to evade user attention while establishing silent backdoor access using the RAT.

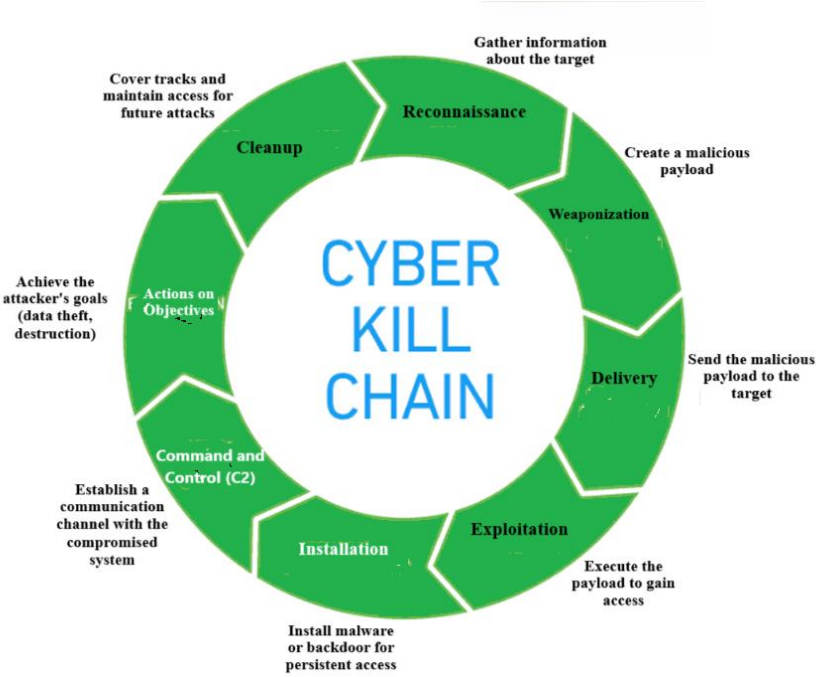

Fig. 1. The Cyber Kill Chain Model
Source: Developed from Martin (2022)

The third stage is the delivery. This stage involves the transmission of the weaponized payload to the target. Delivery is the critical part of the cyber kill chain which is responsible for an efficient and effective cyber-attack (Yadav and Rao, 2015). Common delivery methods include phishing emails with malicious attachments, links to compromised websites, or physical methods like USB drives left in public places. The effectiveness of this phase relies heavily on the attacker's ability to bypass security measures and convince the target to interact with the payload (Yadav and Rao, 2015).

The Exploitation is the fourth stage. Once the payload is delivered, the attacker aims to exploit a vulnerability in the target system to execute the malicious code (Jaikanth and Madisetti, 2024). This may involve executing a script or triggering a vulnerability in software. Successful exploitation allows the attacker to gain control over the system or application, paving the way for further actions (Yadav and Rao, 2015). To trigger the exploit certain conditions need to be matched to be successful. First, the user must be using the software or Operating System for which the exploit has been created. Second, the software or Operating System should not be updated or upgraded to the versions wherein an exploit does not work, and third Anti-Viruses or any other security mechanism should not detect the exploit or payload neither statically nor dynamically scan during run time (Jaikanth and Madisetti, 2024). If all these conditions are fulfilled then the exploit is triggered and will successfully install/execute the payload in the target's system.

The fifth stage is the installation. After the exploitation, the attacker installs malware on the target system to establish a persistent presence. This can include installing backdoors, rootkits, or other forms of malware that ensure continued access even if the initial vulnerability is patched (Yadav and Rao, 2015). The installation phase is crucial for maintaining control over the compromised system. Malware nowadays is multi-staged and they heavily rely on droppers and downloaders to deliver the malware modules in a much more sophisticated manner (Jaikanth and Madisetti, 2024). Dropper is a program that will install and run the malware to a target system. Before executing the malware code, dropper nowadays tries disabling host-based security controls at the target and hides the installed malware (Yadav and Rao, 2015). Downloaders were designed to perform the same actions as Droppers disabling the victim's security and monitoring software, hiding core components and obfuscating the infection vector, etc. but tended to be smaller than Droppers because they did not contain the core malicious library components (Jaikanth and Madisetti, 2024).

Command and control (C2) is the sixth stage. The C2 system is used to give remote covert instructions to compromised machines (Jaikanth and Madisetti, 2024). It also acts as the place where all data can be extracted. In this phase, the attacker establishes a command and control channel to communicate with the compromised system. This allows the attacker to send instructions, execute commands, and exfiltrate data. C2 channels can use various methods, including HTTP, DNS tunneling, or direct socket connections, to avoid detection by security measures (Yadav and Rao, 2015). There are mainly three types of C2 communication structures, namely the traditional centralized structure, the newer peer-to-peer decentralized architecture, and the latest Social Networks structure (Yadav and Rao, 2015).

The seventh stage is the Actions on Objectives. With control of the compromised system established, the attacker proceeds to take actions aligned with their goals (Martin, 2022). This might include data exfiltration, deploying ransomware, or disrupting services. The specific actions depend on the attacker's objectives, such as monetary gain, information theft, or sabotage. Moreover, the Cleanup lasts eight stages. In the final phase, the attacker may attempt to cover their tracks (Jaikanth and Madisetti, 2024). This can involve deleting logs, removing malware, or using techniques to obfuscate their activities to avoid detection by security teams. The cleanup phase is critical for ensuring that the attacker can maintain access or avoid attribution for the attack (Yadav and Rao, 2015).

Furthermore, the study explored the common techniques, and psychological and technical tricks that are clearly present in this study (Table 1).

Table 1 shows the cycle of cyber-attacking techniques, tricks, tools, and countermeasures. In the first column, the Table 1 describes the 8 stages of the cycle of cyberattack, which are reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), actions on Objectives, and Cleanup. The

Table 1. Cycle of Cyber Attacking Techniques, Tricks, Tools and Countermeasures

Stage	Objective	Targets	Techniques	Psychological Tricks	Technical Tricks	Tools	Counter Measures
1. Reconnaissance	Gather information about the target	Employees, company websites, social media	Social engineering, network scanning	Building trust through impersonation	Using search engines and social media	Nmap, Maltego, Shodan	Regular security audits, employee training
2. Weaponization	Create a malicious payload	Software applications, file formats	Crafting malware or exploits	Leveraging current events or fears	Combining exploits with delivery methods	Metasploit, Cobalt Strike	Regular software patching, endpoint protection
3. Delivery	Send the malicious payload to the target	Email accounts, websites, social media	Phishing emails, malicious links	Creating urgency or fear (e.g., account suspension)	Using URL shorteners or obfuscation techniques	Email spoofing tools	Email filtering, user awareness training
4. Exploitation	Execute the payload to gain access	User devices, servers, web applications	Exploiting software vulnerabilities	Manipulating users to enable macros	Buffer overflow exploits, SQL injection	Exploit kits, custom scripts	Application whitelisting, IDS
5. Installation	Install malware or a backdoor for persistent access	Compromised systems, networks	Using rootkits, trojans, or ransomware	Making installation appear legitimate	Hiding malware in legitimate processes	Remote access tools (RATs)	EDR, regular malware scans
6. Command and Control (C2)	Establish a communication channel with the compromised system	Compromised systems, internal networks	Using web servers, peer-to-peer networks	Creating fake services to divert attention	DNS tunneling or HTTP/S for communication	Cobalt Strike, custom C2 frameworks	Network segmentation, monitoring outbound traffic
7. Actions on Objectives	Achieve the attacker's goals (data theft, destruction)	Sensitive data repositories, databases	Data exfiltration, lateral movement	Manipulating users to bypass security	Using legitimate credentials	Data exfiltration tools, scripts	DLP systems, robust access controls
8. Cleanup	Cover tracks and maintain access for future attacks	Compromised systems, logs	Deleting logs, using anti-forensic methods	Creating distractions to divert attention	Modifying timestamps, using steganography	Log cleaners, rootkit detectors	Regular log audits, forensic analysis

Source: Lockheed Martin (2022)

Table 2. Cyber Attacking Phases Techniques, Tricks, Tools and Countermeasures

Phase	Objective	Targets	Techniques	Psychological Tricks	Technical Tricks	Tools	Counter Measures
Intention/ Contemplation	Determine the target and plan the attack	Organizations, individuals	Researching potential targets	Assessing weaknesses and potential gains	Analyzing public profiles and online presence	None	Threat intelligence, security awareness training
Reconnaissance	Gather information about the target	Employees, company websites, social media	Social engineering, open-source intelligence (OSINT)	Building trust, impersonation	Using search engines, social media analysis	Nmap, Maltego, Shodan	Regular security audits, employee training
Scanning the Target	Identify vulnerabilities and weaknesses	Network devices, applications	Network scanning, vulnerability scanning	Creating a false sense of security	Port scanning, service enumeration	Nessus, OpenVAS, Nmap	Vulnerability management, network segmentation
Gaining Access	Exploit vulnerabilities to gain unauthorized access	User devices, servers, applications	Phishing, exploiting software vulnerabilities	Creating urgency or fear (e.g., account issues)	Buffer overflow, SQL injection	Metasploit, Cobalt Strike	Application whitelisting, IDS
Maintaining Access	Ensure persistent access to the compromised system	Compromised systems, networks	Installing backdoors, using rootkits	Making installation appear legitimate	Hiding malware in legitimate processes	Remote access tools (RATs)	EDR, regular malware scans
Clearing Tracks	Remove evidence of the attack	Compromised systems, logs	Deleting logs, using anti-forensic methods	Creating distractions to divert attention	Modifying timestamps, log manipulation	Log cleaners, rootkit detectors	Regular log audits, forensic analysis
Exfiltration	Steal sensitive data	Sensitive databases, file repositories	Data exfiltration techniques	Manipulating users to pass the security	Using encryption, steganography	Data exfiltration tools, scripts	DLP systems, robust access controls
Impact	Achieve the attacker's goals (data theft, disruption)	Critical infrastructure, sensitive data	Data destruction, service disruption	Threatening or coercing victims	Ransomware deployment, altering data integrity	Ransomware, wiper malware	Incident response plans, backups

Source: Jaikanth and Madisetti (2024)

specific objective is described in column two in their respective stages which are gathering information about the target, creating a malicious payload, sending the malicious payload to the target, executing the payload to gain access, installing malware or a backdoor for persistent access, establishing a communication channel with the compromised system, achieving the attacker's goals (data theft, destruction) and covering tracks and maintain access for future attacks.

On the other hand, the Table 1 described the common psychological tricks including building trust through impersonation, leveraging current events or fears, creating urgency or fear (e.g., account suspension), manipulating users to enable macros, making installation appear legitimate, creating fake services to divert attention, and others. The common technical tricks are using search engines and social media, combining exploits with delivery methods, using URL shorteners or obfuscation techniques, and others as indicated in the Table 1. The Table 1 provides the countermeasures in their respective stages, which are conducting regular security audits, employee training, regular software patching, endpoint protection, and others as indicated in the Table 1.

4.2.2 Cyber Attacking Phases Modus Operandi

Cyber-attacking phases refer to the distinct stages that attackers follow when executing a cyberattack. By analyzing these phases, cybersecurity professionals can better anticipate attacker behavior and strengthen their defenses against potential threats. Moreover, it helps the cybersecurity decision-makers to establish effective **defensive measures,** and improving the i**ncident response and** training **and awareness** by educating employees about these phases can help reduce the risk of successful attacks, especially in the reconnaissance and gaining access stages. This study explored the techniques, tricks, tools, and countermeasures in each phase (Table 2).

Table 2 shows the Cyber Attacking Phases Techniques, Tricks, Tools, and Countermeasures. The first column shows the phases of attacking. These include the intention/contemplation which is the initial phase that involves attackers identifying potential targets and planning their approach. Attackers evaluate the benefits and risks associated with various targets to decide where to focus their efforts. The key activities at this stage are researching organizations or individuals, assessing vulnerabilities and potential rewards, and determining the best attack methods based on the target's profile. The common technique is researching potential targets. Moreover, the common psychological tricks are assessing weaknesses and potential gains and the technical tricks are analyzing public profiles and online presence. The countermeasures are conducting threat intelligence and security awareness training. The second phase is reconnaissance. This is when attackers gather information about the target to identify weaknesses. This phase can be passive (observing without interaction) or active (engaging with the target to gather information). The common activities include conducting open-source intelligence (OSINT) gathering, using social engineering techniques (e.g., phishing or pretexting), mapping the target's network, and identifying key personnel. The common techniques are social engineering, and open-source intelligence (OSINT). Also, the common psychological tricks are building trust and impersonation, and technical tricks are using search engines, social media analysis, and tools such as Nmap, Maltego, and Shodan. The countermeasures are conducting regular security audits and employee training.

The third stage is Scanning the Target. In this phase, attackers actively probe the target's systems to identify specific vulnerabilities. This involves using various scanning techniques to assess the security posture of the target. The key activities are performing port scans to identify open services, conducting vulnerability assessments to find weaknesses, and enumerating services and versions running on the target systems. The common techniques are Network scanning and vulnerability scanning. On the other hand, the psychological tricks create a false sense of security, and the technical tricks are Port scanning, service enumeration, and tools such as Nessus, OpenVAS, and Nmap. In this stage, the countermeasures are vulnerability management and network segmentation. The Gaining Access is the fourth phase. In this phase, the attackers exploit identified vulnerabilities to gain unauthorized access to the target's systems or networks. This phase often involves executing the initial attack vector. The key activities include deploying malware or exploits to compromise systems, using social engineering tactics to trick users into revealing

credentials, and leveraging stolen credentials to access sensitive areas of the network. The common techniques include phishing and exploiting software vulnerabilities. Moreover, psychological tricks include creating urgency or fear (e.g., account issues), and technical tricks include buffer overflow and SQL injection. Also, the tools are Metasploit and Cobalt Strike, and the countermeasures are application whitelisting and IDS.

The fifth phase is the Maintaining Access. After gaining access, attackers work to ensure they can return to the compromised system at a later time. This often involves installing persistent malware or backdoors. The common activities are installing rootkits or other forms of malware that provide remote access, creating new user accounts with administrative privileges, and modifying system configurations to avoid detection. The techniques include installing backdoors and using rootkits. The psychological trick includes making the installation appear legitimate, and the technical trick includes hiding malware in legitimate processes. Also, the tools are remote access tools (RATs) and the countermeasures are EDR and regular malware scans. The sixth phase is Clearing Tracks. In this phase the cyber attackers avoid detection and cover their activities, attackers erase evidence of their presence. This phase is crucial for maintaining ongoing access without alerting defenders. The common activities are deleting or altering log files to remove traces of the attack, modifying timestamps to disguise the attack timeline, and using anti-forensic tools to hide malicious activities. The techniques include deleting logs and using anti-forensic methods. Moreover, the psychological trick is creating distractions to divert attention and technical tricks are modifying timestamps and log manipulation. The common tools are log cleaners and rootkit detectors, and the countermeasures are regular log audits and forensic analysis.

The Exfiltration is the seventh phase. In this phase, the attackers steal sensitive data from the compromised system and transfer it to an external location. This phase is often the primary objective of the attack. The common activities are this phase include compressing and encrypting data to facilitate transfer, using various channels (e.g., email, cloud storage, FTP) to exfiltrate data, and employing steganography to hide data within legitimate files. The common techniques are data exfiltration techniques. The psychological tricks are manipulating users to bypass security and technical tricks are using encryption, steganography, and tools are data exfiltration tools and scripts. The countermeasures are DLP systems and robust access controls. On the other hand, the impact is the eighth and the last phase. In this phase, the attackers achieve their intended goals, which may include data theft, destruction, or disruption of services. The impact can vary based on the attacker's motivations (e.g., financial gain, espionage, or sabotage). The key activities include deploying ransomware to encrypt data and demand payment, destroying or altering critical data, and disrupting services to cause operational downtime.

5. EMPIRICAL ANALYSIS OF CYBERCRIMINAL TRICKS

The study used one spam message out of the 10 phishing messages identified from 305 sampled messages from the author's Yahoo account from 2012 to 2024. The aim is to explore and extract the empirical (real) psychological and technical tricks from the conversion of the author and cyber attacker (phisher). Hereby are the exhibits of the conversations (Exhibits 1&2).

From: Rita Leonard <ritaleonard@outlook.com>
To: Author author@yahoo.com
Sent: Monday, August 26, 2013 8:34 PM
Subject: **Darling Please I Need Your Assistant with Love and Trust**

Dearest one,
How are you today together with your business and your family? I guess that everything is okay with you? Please bear with me as I would like us to have a good and trusting relationship despite anything because I have this feeling that you are the right person I have fasted and prayed for. I am more than happy to read your interesting mail reply to me today from the dating site and I believe this relationship will be built on love and trust as I have noticed that you are the kind of man I have fasted and prayed for since all this while, I believe that you are a trustworthy and caring person, that's what makes me disclose my identity to you. My name is (Miss Rita Leonard), 25 years old, but like I said, age does not matter in a real relationship, but love and

care matter most, am from Liberia in Monrovia West Africa, and presently I am residing here in the refugee camp Dakar Senegal as a result of the killing of my family by the rebels last year. I am from the family of the late (Dr. Leonard Armah). My father was chairman and managing director of (LEONARDO INDUSTRIAL COMPANY LTD LIBERIA), in Monrovia the economic capital of my country, and he was also the personal adviser to the former head of state before the rebels attacked our house one early morning and killed my mother and father in a cold blood. My stepmother was a very wicked woman and she intended to kill me since my father and my real biological mother were dead. I managed to escape with the documents which cover my father's deposited money of $3.5M. USD (Three million five hundred thousand US dollars). He used my name as the next of kin. Meanwhile, I am still residing here as a refugee under the UNITED NATIONS COUNCIL FOR REFUGEES, I am saddled with the problem of securing a trustworthy foreign personality to help me transfer the money from the bank pending my arrival in your country. I will like to see you face-to-face soon.

Furthermore, on your wish, you can contact the bank for confirmation and you can communicate directly with them regarding this fund of my late father which was deposited in their custody. I am giving you this offer as mentioned with every confidence in your acceptance to assist me retrieve the money from the bank and transfer it to your nominated account. You can reach me through this number (+221-775-872-582) It is a Reverend Fathers phone number, by name Reverend Father Steven Peter When you call, tell him that you want to speak with Rita Leonard, i am staying in the female hostel. I have already informed him that someone will call me through his phone, so he will send for me from the hostel to come and speak with you. So please do not fail to call me, because I need to hear your voice too. So on your which to help me out, i would like to have your data such as (1) Your Full name (2) Your address (3) Your Country & city (4) Telephone & Fax numbers
Immediately i receive this i will put things in action and give you the contact of the bank where my late father deposited the money for you to contact them on how to transfer the money to your nomination account. I attached my photo here for you to know my face and i hope you like me.
Yours sincerely
With love Rita

***Replied Message*:**
Re: **Darling Please I Need Your Assistant With Love And Trust**
Form Author to ritaleonard@outlook.com Tue, Aug 27, 2013 at 7:28 AM
Message Body: yes! I will do. I have ever and never loved a woman! Thanks

Exhibit 1. The conversation between the author and the phisher (cyber attacker) in August 2013

From: Rita Leonard <ritaleonard@outlook.com>
To: Author <Author@yahoo.com>
Sent: Tuesday, August 27, 2013 3:12 PM
Subject: **Darling Please Contact This Bank Now For More Information about the Transfer***,*

Hello Sweetheart,

How are you feeling today over there in your country together with your day? I believe that you are doing well over there as regards your health, and your business. If so thanks be to God. Mine is a little good today as i have seen today, it's just that i miss you, but i believes by the grace of God who has made it possible for us to have contact this way will surly bring us together very soon. Please i kept about this money as secret from everybody here the only person who knows about it is Reverend Stephen because he has been like a father to me since i arrived into this Refugee camp, and i will like you to also keep it to yourself alone until i am there with you because i am afraid of loosing my life and the money if wicked people gets to know about it. You know i had fasted and pray to GOD before i made contact to you and that is what made me to disclosed all my identity to you believing that you will not try to betray me when the money get to your position. I am more than happy to read from your interesting mail reply in my box today and of most your

acceptance hand to assist me transfer the 3.5 million American dollars deposited by my late father in a leading Bank in England which i am the next of kin to the money. Please remember to send some money for me from the money after it has been transferred for me to prepare my traveling documents to join you over there in your country. As you know i send and receive mails from Rev. Steven Peter's office computer. I will like you to call me with his Tel. **(+221-775-872-582**), you can call the Reverend and ask him the good time to call me OK. Regrading the transfer of my father's deposit to your account, i will like you to contact this Bank with this information's below for confirmation and to know the possibilities of transferring the money to your nomination account. As you know i can not stand for myself on the transfer due to my refugee status, and because i don't have passport, even the resident permit which i can use to stand for myself, so that is why i want you to contact the Bank for me, As i said, i have my father death certificate and statements of account here with me which i will send to you later, meanwhile, i have already informed the Bank about you that you are my trustee / partner who will standing for me on the transfer, so do not be afraid to contact them by phone and E-mail immediately you finish reading this mail.

THE BANK CONTACT INFORMATION ARE AS FOLLOWS: LLOYDS TSB BANK PLC LONDON: E-mail address: lloydstbk@london.com
lloydstsbnklondon@accountant.com: Telephone Number. +447-024-068-338; hp to Winfred David...+447-031-859-717; Fax number. +448-701-351-970; The name of the transfer officer is. Sir Winfred David / WAJ01041.

NOW I WANT YOU TO SEND THIS MAIL TO THE BANK EMAIL FOR CONFIRMATION AND THE POSSIBLE TRANSFER
Good day, Sir David.
My name is Author
I am a foreign partner/trustee to Miss Rita Leonard whom i believe she has already told you about me regarding some fund of Dr Leonard Armah who is her late father, So Please i want to know the possibility of transferring her late fathers money deposited in your bank to my account in my country of which she is the next of kin but due to her refugee statue she wants me to stand for her through the transfer.
I am awaiting for your response.
Regards Author.

MY FATHER'S ACCOUNT INFORMATION'S ARE AS FOLLOWS. My father A/c Name. DR. LEONARD ARMAH; A/c No. 142552003
IBAN. GB63LLOYDS TSB209561142552003; SWIFTBIC... LLOYDS TSBGB20. Next of kin. RITA LEONARD.

Darling, contact the Bank immediately on how to transfer the 3.5 million dollars deposited by my late father DR. LEONARD ARMAH of which i am the next of kin. You will have 15% of the total money for your assistance after the transfer and i have also mapped out 5% for expenses so that after the transfer you will take the total of 20% and if you don't intend staying with me as your wife then we know how to do the remaining money. Remember i will also need your assistance to managing the money since i am still too young to handle that amount and as my most concern now is to complete my university studies. Be sure you send mail to both emails for proper confirmation. God bless you and awaiting to hear from you soonest
Yours in love
Rita.

Replying from Author
Re: DARLING PLEASE CONTACT THIS BANK NOW FOR MORE INFORMATIONS OF THE TRANSFER,
From: Author to ritaleonard@outlook.com Wed, Aug 28, 2013 at 10:43 AM
Message Body: *Thanks, I will do! I am always love the woman under 18 years. How old are you?*

Exhibit 2. The conversation between the author and the phisher (cyber attacker) in August 2013

Table 3. Psychological Tricks Analysis

Psychological Trick	Example	Analysis
Emotional Manipulation	"I have this feeling that you are the right person I have fasted and prayed for."	Creates a strong emotional connection, making the recipient feel special and chosen, increasing their investment in the interaction.
Trust-Building Language	"I believe that you are a trustworthy and caring person, that's what makes me disclose my identity to you."	Establishes a bond of trust, encouraging the recipient to feel a sense of responsibility towards the sender.
Vulnerability	"I am from the family of late (Dr. Leonard Armah)... I managed to escape with the documents."	Presenting herself as vulnerable elicits sympathy and makes the recipient more likely to want to help.
Fear and Urgency	"My stepmother was a very wicked woman and she intends to kill me."	Instills urgency and fear, prompting immediate action from the recipient without careful consideration.
Personal Connection	"I am more than happy to read your interesting mail reply to me today from the dating site."	Creates a sense of familiarity and connection, making the recipient feel more engaged and invested in the relationship.
Flattery	"I believe this relationship will be built on love and trust."	This flattery reinforces the recipient's self-esteem, encouraging them to respond positively to the sender's requests.
Hope for Future Relationship	"I would like to see you face to face soon."	This statement fosters a sense of anticipation and commitment to the relationship, making the recipient more likely to comply with requests.
Financial Incentive	"You will have 15% of the total money for your assistance."	Offering a financial reward encourages the recipient to act, making the scam more appealing.

Source: Author (2024)

Table 4. Technical Tricks

Technical Trick	Example	Analysis
Fictitious Identity	"My name is (Miss Rita Leonard), 25 years old... I am from Liberia in Monrovia."	Establishes a detailed identity that lends credibility to the message, making it more believable.
False Financial Claims	"I managed to escape with the documents which cover my father's deposited money of $3.5M USD."	Mentioning a large sum of money serves as a lure to entice the recipient into engaging further.
Involvement of a Third Party	"You can reach me through this number (+221-775-872-582) It is a Reverend Father's phone number."	Including a trusted figure (the Reverend) adds a layer of legitimacy and makes the recipient feel safer in the proceeding.
Request for Personal Information	"I will like to have your data such as: (1) Your Full name (2) Your address (3) Your Country & city (4) Telephone & Fax numbers."	Directly asking for sensitive personal information is a classic tactic in phishing scams, leading to potential identity theft.
Contacting a Bank	"You can contact the bank for confirmation and... communicate directly with them regarding this fund."	Encourages the recipient to engage with a fake bank, furthering the scam and creating a false sense of legitimacy.
Bank Details and Contact Information	"THE BANK CONTACT INFORMATION IS AS FOLLOWS: LLOYDS TSB BANK PLC LONDON."	Providing fake bank details and contact information is a common tactic to further the scam and create a false sense of legitimacy.
Urgent Action	"Contact the Bank immediately on how	Encourages quick action, which can

Technical Trick	Example	Analysis
Request	to transfer the 3.5 million dollars."	prevent the recipient from thinking critically about the situation.
Attachment of a Photo	"I attached my photo here for you to know my face."	Including a photo humanizes the sender, making the recipient feel more connected and less suspicious.
Promise of Action	"Immediately I receive this I will put things in action."	Suggests that the recipient's compliance will lead to quick results, increasing the likelihood of them acting without hesitation.

Source: Author (2024)

Exhibit 1 shows the conversion between the author and phisher on Monday, August 26, 2013, at 8:34 PM. The conversation started with an e-mail from Rita Leonard ritaleonard@outlook.com (the phisher) to Author author@yahoo.com. Rita claimed that she would like us to have a good and trusting relationship despite anything because she had that *feeling that the author* was *the right person* and that *she had fasted and prayed for* him. In this statement, we detected the psychological tricks phrases such as "*feeling that author he is the right person that she had fasted and prayed for him".* These phrases limit the mind of the author to judge why Rita (phisher) selected him, it is due to Godly power because Rita fasted and played for him. Moreover, Rita (phisher) encourages the communication through Reverend Father Steven Peter, to deceive the author into believing that the mission or offer is safe. These are impersonation ticks. This is a *divinity* psychological trick. Moreover, the love psychology tricks phrases are detected in Exhibit 2.

The Exhibit 2 shows the continuation of the conversation between the author and the Phisher (Rita) on *Tuesday, August 27, 2013, at 3:12 PM and* Wed, Aug 28, 2013, at 10:43 AM. The study evidenced that traditional phishing commonly uses a combination of psychological tricks including divinity and love psychological tricks. A summary of the empirical analysis of these conversations is provided (Tables 3 & 4).

Tables 3&4 summarizes the analysis of the conversation between the Author and the phishing in Aught 2013. Close examination of this type is a traditional phishing which uses the multiple of email to send to unknowns. The classification of psychological and technical tricks is based on the assumption that psychological Tricks focus on emotional manipulation and relationship building to influence the recipient's feelings and decisions, and technical Tricks involve deceptive practices that create a false narrative or scenario, often centered on financial gain or identity theft.

5.1 Technical verification of the E-mail contents

We used the OSINT technique to verify the content information of the email, particularly, the Bank details: name of the bank (LLOYDS TSB BANK PLC LONDON), IBAN (GB63LLOYDS TSB20956114 2552003) and SWIFTBIC (LLOYDS TSBGB20). We revealed the true name of the Bank LLOYDS TSB BANK PLC, but Rita (phisher) added the word LONDON to trick the recipient. Also, SWIFTBIC (LLOYDS TSBGB20) and IBAN (GB63LLOYDS TSB20956114 2552003) are fakes (Exhibits 3 &4).

5.2 Empirical Findings

From this empirical analysis, we find some of the facts and issues that are necessary to be highlighted. We evidenced the false identity and financial lures applied by the phisher by using the fictitious identity and promising a large sum of money to trick the target (author). This is a tacky component of the scam message designed to attract the reception's interest and provoke a response. Also, the study found that they use emotional manipulation and trust tricks to create a sense of trust and agency. The phisher (Rita) expresses their vulnerability to emphasize the elicited sympathy making the receiver (author) feel compelled to assist her. Moreover, the study evidenced that the phisher uses the technique of involvement of the trusted figure, the third party (the Reverend), the phisher does this to enhance credibility, making the receiver (author) feel safe in engaging with the request or mission. The study, also found that the solicitation of personal information trick was used by the phisher. The phisher (Rita) requests personal data which is the indicator of the phishing intent, which is to

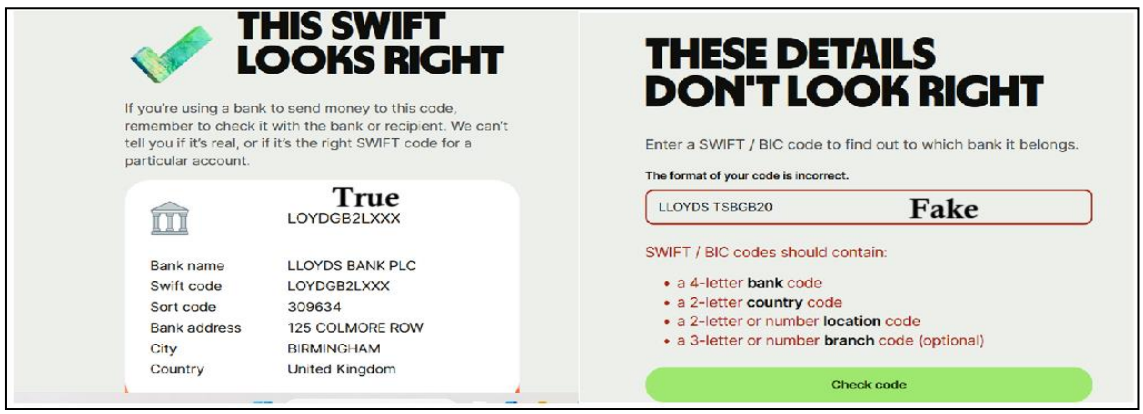

Exhibit 3. The OSINT verification of SWIFTBIC sent by a phisher (Rita)
Source: Author (2024):

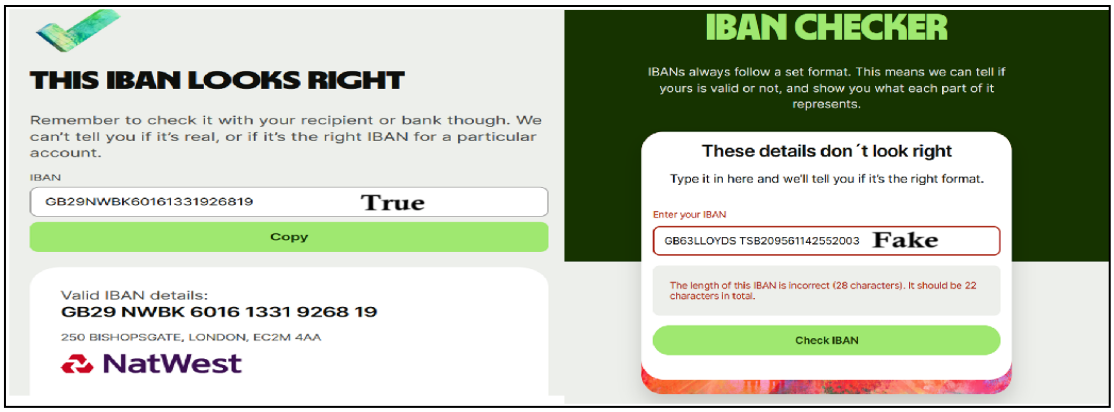

Exhibit 4. The OSINT verification of IBAN sent by phisher (Rita)
Source: Author (2024):

acquire sensitive information for intense theft or future scams. On the other hand, the study evidences that urgency and action tricks were exercised in these conversations. The phisher demanded the call for immediate action. This is a common trick in the scam, aimed to pressure the receiver into making hasty decisions that could have a negative consensus. In general, the conversation employed a blend of psychological and technical tricks to manipulate the recipient into providing personal information and facilitating the scam, highlighting the importance of caution in such interactions.

6. DISCUSSION

This study aimed to explore the cybercrime modus operandi. The study extracted and analyzed several theoretical and empirical academic and professional studies and researched articles, journals, and policy papers. The study extended the definition of the cybercrime modus to include the techniques, tools, psychological tricks, and technical tricks. The study defined the cybercrime modus operandi *as the dynamic learned specific or unique means, characteristic, action or behavior possessed or shown by the cyber attacker in entering, executing, exiting, and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before, during and after the cyber-attack*. The term "learned" means that cybercriminals can learn through informal and formal systems. The informal system includes the socialization with the criminal society or groups. That is, the criminal gaining criminality behavior or experiences through socialization with the criminal society (Turvey, 2013; Sundberg, 2020). On the other hand, formal learning includes procedural learning through official systems such as classroom learning in schools and colleges. This definition filled the gap in the traditional definition of the modus operand that was based only on the actions done at the scenes, that is during the commission of a

crime. The traditional definition overlooked the two important aspects, that is, facts before the crime commission (planning scene), and facts after the crime commission (exiting and escaping scene). In modern or emerging crimes such as cybercrimes and other organized crimes, we must extend the meaning of the modus operand to understand the overall behavior, technical ability, and skills of criminals. Therefore, we need a new definition of the modus operand that incorporates multiple features of the criminal's skills and knowledge in the use of the techniques, tools, and psychological and technical tricks as the main components of the modus operand in cybercrime. Thus, this definition incorporated the actions and behavior of the criminal done before, during, and after the crime commission. This definition provided a significant contribution for both law enforcement and policymakers as it provides comprehensive knowledgeable information on how cybercriminals plan, organize, execute, exit, and escape from the crime scene.

On the other hand, the study provided the stages and targets of the cybercriminal attack and cyber kill chain. This helps law enforcement and other security professional to be aware of the cyber-attacks in each stage and then be able to set appropriate prevention and combating strategies or plans at early stages. This is useful because the target, that is, individuals or organizations targeted by the cyber attackers will be able to understand the aim or goals of the attacker and, hence able to provide the mitigation strategies in their respective organizations.

The study closely examined both the psychological and technical tricks. The study found that the common psychological tricks are fear, urgency, trust, familiarity, authority, social proof and curiosity, and emotional appeal. That is, the cybercriminals use these psychological tricks to deceive the end users into providing their personal or confidential information or data to the cyber attacker, usually the phisher unknowingly. They are miming the good men. The common means technique of cyber attackers is phishing. The criminal creates psychological phrases that trick the individual into fear or make a sense of urgency or familiarity with the deceived issue or fact. These psychological trick phrases are created according to the target. Furthermore, the study explored the common technical skills that cybercriminals are using to phish or enter the cybercrime commission. In reality, the technical trick is usually targeted to trick or deceive cybersecurity professionals, because they are created to provide technical fake information. This deceived technical information is intended to trick or trap those who are knowledgeable of cyberspace. This study highlighted some common technical tricks. Cybercriminals use tricks such as automated email generation for hacking software or tools, alteration of email headers, spoofing of URLs, and others. Henceforth, the study provided the stage-based countermeasures in the cyberattacking phases and cyber kill chain. This is very useful because it provides a sense of awareness of the cybersecurity issue for the targets. Notably, the phisher uses the psychological trick to deceive the recipient by entering a technical trap /trick such as clicking the link, downloading, or sending some credential information. In that sense, the *entry trick* of the cyber attacker is a psychological trick that conquers the mind of the receiver (target) and accepts the cyber attacker's technical command or request easily.

7. CONCLUSION AND RECOMMENDATIONS

The study aimed to introduce a new concept of interpreting and determining the modus operandi of cybercriminals. That is, the modus operandi should be reflected in the whole or overall behavioral, technical, and skills attributes of the cyber criminals. Moreover, the concept of modus operandi should involve all actions or behavior shown by the criminal in the whole process of the crime commission from the preparatory stage to the escaping stage, that is, at the entry, exit, and exits and escaping In other words, the modus operandi in the cybercrime study should involve the actions and behavior before, during and after the crime incident. Therefore, we define modus operandi as:-

"The dynamic learned (acquired) specific or unique means, characteristic, action or behavior possessed or shown by the cyber attacker in entering, executing, exiting, and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before, during and after the cyber-attack".

Therefore, the study suggested the investigations of the four crime scenes in cybercrime; *planning crime scene, execution crime scene, exit crime scene, and escaping scene*. This means, that the cybercriminals most of them are well-educated

and skilled in ICT, and they use their knowledge and skills to commit crimes. In that sense, before committing a crime, they make decisions or research on how (select methods, e.g. phishing) to enter the target, execute (selection of techniques and tools), exit (vulnerability), and escape from the risk identified. Hence, the cybercrime investigator must understand the methods, techniques, tools, and tricks those are used by cybercriminals to enter, execute, exit, and escape.

On the other hand, the study highlighted the techniques, psychological tricks, technical tricks, and countermeasures. The study found that in traditional phishing, the attack uses a combination of tricks such as false identity and financial lures, emotional manipulation and trust through divinity and love psychological tricks, involvement of the trusted figure usually the religious leaders, direct solicitation of personal information, urgency and action. In general, we conclude that phishers usually a combination of blended psychological and technical tricks to manipulate the recipient into providing personal information and facilitating the scam. Notably, phishing attacks start with psychological tricks to induce or deceive the target to accept the technical tricks such as clicking the link or downloading. Therefore, the effective recommended countermeasures are psychological base strategies such as cognitive training on cybersecurity awareness.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

Bhadani, U. (2024a). *Advanced persistent threats (APTs): Detection strategies and mitigation techniques*. Silver Oak College of Engineering & Technology, Gujarat Technological University, Gujarat, India.

Bhadani, U. (2024b). *The evolving landscape of cybersecurity: Exploring threats, vulnerabilities, and defense mechanisms*. Silver Oak College of Engineering & Technology, Gujarat Technological University, Gujarat, India.

Bhusal, C. S. (2021). Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security, 12*, 104-114. https://doi.org/10.4236/jis.2021.121005

Carrera-Rivera, A., Larrinaga, F., & Lasa, G. (2022). Context-awareness for the design of smart-product service systems: A literature review. *Computers in Industry, 142*, 103730. https://doi.org/10.1016/j.compind.2022.103730

Dhondwad, G., Sakhare, A., & Bukshete, S. (2024). The study on legal and ethical issues in cybersecurity: In India. *International Journal of Research and Analytical Reviews (IJRAR), 11*(2), 581-584.

Gnanasekaran, V., Bartnes, M., Grøtan, T. O., & Heegaard, P. E. (2024). Cyber-incident response in industrial control systems: Practices and challenges in the petroleum industry. *2024 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems and 2024 IEEE/ACM Second International Workshop on Software Vulnerability (EnCyCriS/SVM)*.

Jaikanth, M., & Madisetti, V. K. (2024). A comparative analysis of cybersecurity threat taxonomies for healthcare organizations. *Journal of Software Engineering and Applications, 17*, 359-377. https://doi.org/10.4236/jsea.2024.175020

Junaid, N., & Schaffer, A. (2024). Legal compliance and ethical challenges in cybersecurity for human resources management. *ResearchGate*.

Karabacak, B., & Whittaker, T. (2022). Zero trust and advanced persistent threats: Who will win the war? *Proceedings of the 17th International Conference on Cyber Warfare and Security, USA, 17*(1), 92-101. https://doi.org/10.34190/iccws.17.1.10

Kausar, S., Leghari, A. R., & Iftikhar, E. (2023). Analysis of the cybersecurity challenges and solutions. *Journal of Positive School Psychology, 7*(1), 163-171.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical Report, EBSE Technical Report EBSE-2007-01*.

Martin, L. (2022). *Cyber kill chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mengista, W., Soromessa, T., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. *7*, 100777. https://doi.org/10.1016/j.mex.2019.100777

Nyre-Yu, M. (2021). Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development. *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Pati, D., & Lorusso, L. N. (2018). How to write a systematic review of the literature. *HERD, 11*(1), 15-30.

Pospisil, B. (2020). Modus operandi in cybercrime. In E. Huber, G. Quirchmayr, & W. Seboeck (Eds.), *Pages 17* (pp. 17). https://doi.org/10.4018/978-1-5225-9715-5.ch013

Proofpoint. (2024). *What is email spoofing?* Proofpoint, Inc. 925 W Maude Avenue. Sunnyvale, CA 94085.

Soares, L. H. (2023). The evolution of cyber threats and its future landscape. North Whales Management School, Wrexham Glyndwr University, Wrexham, United Kingdom.

Sundberg, J. (2020). Linking crime through modus operandi: On linking series of crime into single offenders through structured collection of crime scene information. *Degree project in criminology* (15 credits). Malmö University: Faculty of Health and Society, Department of Criminology.

Texas Tech University (TTU). (2024). *Scams – Spam, phishing, spoofing, and pharming*. Cybersecurity Awareness Program: Lubbock. TTU Office of the CIO, Lubbock, TX 79409.

Turvey, B. E. (2013). Modus operandi. In *Encyclopedia of forensic sciences* (pp. 150-153). https://doi.org/10.1016/B978-0-12-382165-2.00026-X

Ware, W. H. (1979). *Security controls for computer systems: Report of Defense Science Board Task Force on Computer Security*. Santa Monica, CA: RAND Corporation.

Yadav, T., & Rao, A. M. (2015). Technical aspects of the cyber kill chain. In J. H. Abawajy et al. (Eds.), *Springer International Publishing Switzerland 2015, CCIS 536* (pp. 438-452). https://doi.org/10.1007/978-3-319-22915-7_40

Yang, L., Zhang, H., Shen, H., Huang, X., Zhou, X., Rong, G., & Shao, D. (2021). Quality assessment in systematic literature reviews: A software engineering perspective. *Information and Software Technology, 130*, 106397. https://doi.org/10.1016/j.infsof.2021.106397

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/128138