Int. j. adv. multidisc. res. stud. 2025; 5(1):77-86

Received: 14-11-2024
Accepted: 24-12-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Detecting and Mitigating Cyber-Psychological Tricks and Cyber-Technical Tricks in Cyberattacks

Ntogwa N Bundala
Tanzania Police Force, Morogoro Police Regional, Tanzania

Corresponding Author: **Ntogwa N Bundala**

Abstract
The detecting and mitigating of cyber-psychological tricks and cyber-technical tricks is still an active challenge in cyberspace security. The advancement and convergence of technologies are going parallel with the emergence of new challenging cyber attacks such as advanced persistent threats (APTs), zero-day attacks, and others that are sophisticated and stealthy. In that sense, the study of cyber-psychological and cyber-technical tricks is inevitable in cybersecurity solution planning. This study aimed to explore the cyber-psychological tricks, cyber-technical tricks, indicators, and their mitigation strategies. The study applied the metadata analysis research approach to compile, compare, and analyze the different theoretical and empirical findings. The study found that the common cyber-psychological tricks are Fear, Authority, Social Proof, Exclusivity, Scarcity, Emotional Appeals, Reciprocity, Urgency, Familiarity, and Curiosity, and the effective mitigating strategy of psychological ticks is the training of the users. On the other hand, the study evidenced that common cyber-technical tricks are Spoofing, Malware Delivery, Phishing Kits, Domain Spoofing, DNS Spoofing, Man-in-the-Middle (MitM), Credential Harvesting, SSL Stripping, Card Skimming, URL Manipulation, Data Breach through Phishing, Exploit Vulnerabilities, Credential Stuffing, Phishing via SMS (Smishing), Fake Academic Portals, Network Sniffing, Fake Donation Links, Social Media Phishing, SCADA Exploits and Network Scanning. The mitigation of these cyber-technical tricks requires the end users to be trained on how to get rid of the cyber-attacks. Therefore, we concluded that cyber-psychological tricks are the first runners for cyber-technical tricks, and the effective mitigation strategy is the training for users. Thus, we recommend that cybersecurity stakeholders (targets of cyber-attacks) such as health, education, government agencies, and business enterprises establish both psychological awareness and technical know-how; off and on-the-job training programs for their staff and customers to increase the organizational reputation.

Keywords: Cyber-Psychological Tricks, Cyber-Attacks, Cyber-technical Tricks, Mitigation Strategies

1. Introduction and Literature Review

The detection and mitigating of cyber-psychological tricks and cyber-technical tricks is still an active challenge in the cybersecurity arena. Therefore the study of cyber-psychological and cyber-technical tricks is inevitable as it is relevant to the cybersecurity stakeholders. Several studies describe the common cyber-psychological tricks and cyber-technology tricks with their respective theoretical and methodological limitations. For example, Kuzior *et al.* (2024) [21] addressed the concept of cyber-psychological and cyber-technical tricks by using the concept of social engineering attacks which is too general to describe specific tricks. The term signifies the techniques such as phishing, spoofing, spamming, pharming, and others (Kuzior *et al*. 2024; APWG, 2023**;** Schulze, 2021) [21, 4, 33]. Another study by Miller *et al.* (2020) [23] contented that overconfidence is the one psychological factor that reduces the phishing awareness of the individual, hence becoming more vulnerable to cyber-attacks. The study overlooked the cyber-technical tricks such as spoofing of its categories and others. Miller *et al.* (2020) [23] concluded that experience and training are the most effective tools for mitigating the cyber-attack. Although, Miller *et al.* (2020) [23] did not specify the kind of training and skills required they recommended that is relevant as it will change the user's education on the specific issues.

On the other hand, Desetty, Jangampet, and Pulyala (2020) [11] explained that phishing attacks remain a significant cyber threat to individuals and organizations globally. Over time, phishing attacks have become more sophisticated and harder to detect (Kuzior *et al*. 2024; Desetty, *et al*. 2020) [21, 11]. Several studies identified common cyber-attack techniques to include spoofing, social engineering, malware, targeted or spear phishing, deceptive phishing, clone phishing, whaling, link manipulation, mobile phishing, which uses SMS text messages (smishing), mobile apps, and mobile websites to steal the personal or credential data such as password, user names, credit numbers, and others (APWG, 2024; FBI, 2023; Zywave; 2020; Sathish, Kumar, and Vayansky, 2018) [5, 12, 39, 31]. These studies failed to describe the cyber-psychological trick and cyber-technical trick instead, they are describing only the techniques. This is the weakness that was filled by this study.

Furthermore, Desetty, *et al*. (2020) [11] identified that common smishing attack tricks include, scaremongering, links to fake websites, and Deepfakes. There are three types: Audio Deepfakes, Video Deepfakes, and Image Deepfakes (Desetty, *et al*. 2020; Sathish, *et al*. 2018) [11, 31]. Cyber attackers use Deepfakes to spread misinformation and propaganda, that is, they use Deepfake to create fake news stories or content that could be rapidly spread and significantly impact public opinion (Desetty, *et al*. 2020; Jones, n.d) [11, 20]. Moreover, Deepfakes can be used by cyber attackers to cause financial fraud. That is, they can use Deepfakes to impersonate executives or manipulate financial transactions leading to losses for individuals and organizations. Also, some scholars described voice phishing using cyber-psychological tricks such as impersonation, urgency and scaring, social engineering tricks, and requesting sensitive information (APWG, 2024; FBI, 2023; Bhavsar, Kadlak and Sharma, 2018) [5, 12, 7]. These studies were also limited to cyber-psychological ticks, they overlooked the cyber-technical tricks.

Some scholars explained the concept of bait and hook as cyber-tricks, baits represent cyber-psychological tricks and hooks represent cyber-technical tricks. The bait is achieved through email phishing and hooks represented by manipulated websites (APWG, 2024; APWG, 2023; FBI, 2023) [5, 4, 12]. Notably, many cyberattacks start with phishing (Bundala, 2024) [9]. The bait is represented or done by email is classified into two characteristics, social engineering which involves psychologically manipulated tricks such as urgency, impact, familiarity, trust, and others, meanwhile, technical characteristics which contend the technical tricks such as links to websites that gather information, reply address differ from the claimed sender, hiding the host information, redirecting the URL and switching ports. On the other hand, characteristics of the hook (phishing websites) include the website contents includes Spoofed Content, Spoofed Layout, Forms to Submit Information, Pup-Up Windows, Information Processing, Account Access Restrictions, Images Mimicking Windows, and Windows Masking Underlying Windows. Moreover, the technical characteristics of the website include SSL Certificates, Browser Discrimination, Fake Address Bars, Disabling Right-Click, Visually Deceptive URLs, and Images Masking Underlying Text (Kuzior *et al*., 2024 [21]; FBI, 2023 [12]; Zywave, 2020 [39]; HICP, n.d).

Several studies are suggesting the mitigating strategies for cyber attackers to include user education, spam filters, anti-malware, use of monitoring tools and web application firewalls that can significantly reduce the exposure to cyber-attacks, and the use of tools like email security gateways and network intrusion detection system (Kuzior *et al*. 2024 [21]; Zywave, 2020 [39]; HICP, n.d). Moreover, some studies recommended the use of multi-factor authentication, regular security updates, spam guards, communication via phone or secure websites, not clicking on links, downloading files, or opening attachments in emails from unknown senders, setting sound security policies in the organization and provide the security awareness training (APWG, 2023; Sathish, *et al*, 2018; Bhavsar *et al*, 2018) [4, 31, 7]. These findings overlooked addressing the mitigation strategies for cyber-psychological tricks and cyber-technical treks and instead provided the general mitigation strategies for techniques that are not effectively achieved. On the other hand, some studies addressed the detection strategies of cyberattacks. Bhavsar *et al* (2018) [7] suggested that some measures such as the use of custom DNS services, using your browser's phishing list, using sites to check links, using your own Ninja skills, looking for secure connections, looking at the domain of URL (if the change or modifies), and look at the site itself is it is familiar to you.

This paper addresses the general question left from the previous studies, that is how to detect or what are indicators of cyber-psychology tricks and cyber-technical tricks, and how they can be mitigated. Therefore, this paper aims to provide the cyber-psychological tricks and cyber-technical tricks, indicators, and their respective target countermeasures. This finding will enhance the investigation of cybercrime issues and enhance the security solution of cyberspace. The next part of the paper covers the methodology of the study, findings, discussion conclusion, and recommendations.

2. Methodology of the Study

This study applied the Meta-data-analysis which is the analyses of the analyzed or previous findings on the research problem. This method is very relevant in the study of cyber-attacks because cybercriminals are highly dependent on time and technological changes. Hence, using metadata analysis enables the researcher to compile and extract different observations and findings from previous theoretical, methodological, empirical, and professional studies (Zhao, 1991) [37]. In other words, the results of data analysis are findings obtained through the analysis of raw materials, i.e., data that are collected in the field. Balkibayeva (2024) [6] emphasized that while data analysis processes "raw data," meta-data analysis processes the "processed data." Metadata analysis is not the same as data reanalysis which seeks to analyze the same set of raw data over again using different procedures or for different purposes. Instead, meta-data-analysis is the analysis of the results of previous analyses or the analysis of analyses (Balkibayeva, 2024 [6]; Glass 1976). In that sense, the study applied Meta-data-analysis able to compile and explore (examine) the study of the underlying assumptions of various data-analytic procedures in the cyber-attack or cybercrimes and compare different forms of data in terms of their quality and utility based on the cybercrime or cyber-attacks. Moreover, the study also synthesizes the findings of a range of research studies that are related to the same phenomenon.

3. Findings

The study aimed to explore the cyber-psychological tricks, cyber-technical tricks, indicators, and their mitigation strategies. The following sub-section describes the findings of this study.

3.1 Common Cybercriminal Psychological Tricks

Cyber-psychological tricks are tactics used by cybercriminals to manipulate human behavior and exploit psychological principles to achieve their goals, such as stealing personal information, spreading malware, or conducting scams (Hooks, *et al*., 2022; Zende, 2022) [16, 36]. These tricks often play on emotions, social dynamics, and cognitive biases to induce fear, urgency, trust, or compliance (Geer, Jardine, and Leverett, 2020) [13]. Understanding these cyber-psychological tricks is essential for individuals and organizations to recognize manipulative tactics and develop effective strategies for cybersecurity (Zwilling *et al*., 2022; Liu *et al*., 2022) [38, 22]. Therefore, the study presented the common cyber-psychological tricks in the next paragraphs.

Fear is among the most common cyber-psychological tricks of cybercriminal attacks. This tactic leverages fear to compel individuals to take immediate action, often by highlighting potential negative consequences (Siddiqi, Pak, and Siddiqi, 2021). The objective is to create urgency and prompt quick compliance or decision-making (Abroshan, *et al*. 2021) [1]. Cybercriminals can use common cyber-psychological trick phrases such as "*Your account will be suspended unless you verify your information immediately!" or Click here to remove it!"* These messages may threaten the users to comply with the instructions, hence making them vulnerable to cyber-attacks (Abroshan, *et al*. 2021) [1]. The common indicators are receiving threatening messages and security warnings. Another cyber-psychological trick is Authority which involves impersonating authority figures to gain trust and compliance (Inkster, Knibbs, and Bada, 2023) [19]. The objective is to exploit the natural tendency to obey authority and make individuals more susceptible to requests (Hooks, *et al*., 2022) [16]. For example, the cyber attackers may send you the message "*This is Officer Smith from the Cybercrime Division. We need your cooperation to investigate fraudulent activity.* The common indicators are receiving messages from supposed authoritative figures.

Social proof is another cyber-psychological trick. This trick uses the influence of others' actions or endorsements to persuade individuals (Alghamdi, 2020; Rizk and Elragal, 2020) [3, 29]. The objective is to create a sense of safety in numbers, encouraging compliance based on perceived popularity. The common examples of cybercriminal cyber-psychological tricks phrases are statements like "*Join the thousands of satisfied customers who have already upgraded ".* The common indicator is references to others' actions or endorsements. Moreover, the study described the exclusivity trick which creates a sense of privilege or special access to encourage immediate action (Zwilling *et al*., 2022; Liu *et al*., 2022) [38, 22]. The objective is to make individuals feel special and prompt them to act quickly to secure their exclusive offer (Zende, 2022) [36]. For example, a phisher can send you emails with the phrase "*You've been selected for a limited-time offer just for our loyal customers!".* The common indicator is receiving limited-time offers or membership invitations.

On the other hand, scarcity and emotional appeals are identified as the common cyber-psychological tricks. Scarcity is the tactic that emphasizes limited availability to create urgency (Purwaningsih, Sholikhah, and Wardani, 2018) [26]. The objective is to prompt quick decision-making due to fear of missing out. Common examples of cyber-psychological trick phrases include statements such as "*Only 5 items left in stock! Order now before they're gone!* The common indicator is claiming limited availability or time-sensitive offers. The emotional appeal is another cyber-psychological trick. This tactic uses emotional language to provoke feelings such as sympathy, guilt, or urgency (Liu *et al*., 2022) [22]. The objective of this trick is to manipulate emotional responses to drive compliance (Liu *et al*., 2022) [22]. For example, the cyber attacker may use psychological phrases such as "*help us support children in need—every donation makes a difference!" or "Act now—your quick response could save someone's life*!" The common indicator is message content designed to provoke emotional responses.

Furthermore, the study explored other cyber-psychological tricks such as reciprocity, urgency, familiarity, and curiosity. Reciprocity is a tactic that involves offering something of value to create an obligation for the recipient to reciprocate. The objective is to leverage the social norm of reciprocity to prompt compliance. For instance, cyber attackers can craft messages such as *"Enjoy this free trial—if you like it, consider subscribing*!". The common indicator is receiving offers of free gifts or services. The urgency is the tactic that creates a sense of immediate action required, often linked to time constraints (Inkster, Knibbs, and Bada, 2023) [19]. The objective is to prompt quick actions that may not be thoroughly considered. The common cyber-psychological trick phrases are like this *"Hurry! This deal ends at midnight!".* The common indicator is receiving messages that call to action and create a sense of urgency.

On the other hand, the familiarity trick exploits the comfort derived from familiarity, often using recognizable logos or language. The objective is to build trust and reduce skepticism. The common cyber-psychological trick phrases include "*As a valued customer, we're reaching out to share this important update.".* The common indicator is receiving messages that evoke a sense of recognition or comfort. In addition, curiosity is another cyber-psychological trick that provokes curiosity to elicit a response or action, often through ambiguous or enticing messages. The objective is to encourage individuals to click on links or engage with content without careful consideration. For example, cyber attackers can craft messages such as "*You won't believe what we discovered about your account—click here to find out!".* The common indicator is intriguing or mysterious messages. Moreover, detailed further examples of cyber-psychological tricks with their respective targets, indicators, objectives, and tools are provided in Table 1 in Appendix A.

3.2 Common Cybercriminal Technical Tricks

Cyber-technical tricks refer to a range of tactics and techniques used by cybercriminals to exploit vulnerabilities in technology and human behavior for malicious purposes (Newaz *et al*., 2021) [24]. These tricks often involve manipulating technical systems, software, or human interactions to gain unauthorized access, steal data, or disrupt services (Riggs *et al*., 2023) [28]. Understanding these technical tricks, their descriptions, and examples helps individuals and organizations recognize and defend against cyber-psychological manipulation more effectively. Awareness is crucial in fostering a secure digital

environment (Gunduz and Das, 2020; Sakthivel *et al*., 2020) [15, 30].

Therefore, this study explored several cyber-technical tricks such as spoofing, malware delivery, and phishing kits (Rapid, 2024) [27]. The spoofing trick involves disguising a communication from an unknown source as being from a known, trusted source (Riggs *et al*., 2023) [28]. The objective is to deceive the recipient into believing the message is legitimate, often to gain sensitive information or access (Ahsan *et al*., 2022) [2]. The common cyber-technical trick phrase includes statements like "*Your bank has detected suspicious activity. Please verify your account details immediately."* The common indicator is receiving unexpected emails and mismatched sender addresses. Malware delivery is another tactic that involves sending malicious software to a target device through various means, such as email attachments or infected websites (Ahsan *et al*., 2022; Newaz *et al*., 2021) [2, 24]. The objective is to compromise the target's system for data theft, espionage, or control (Ahsan *et al*., 2022) [2]. For example, the cyber attacker may craft a message such as *"Please review the attached document for our meeting. It contains important updates.* The common indicator is slow performance or unexpected pop-ups. On the other hand, phishing kits are pre-packaged tools that allow attackers to create phishing sites easily and launch email campaigns (Hu, 2021; Buchanan *et al*., 2020) [17, 8]. The objective is to automate and simplify the process of executing phishing attacks. For example, the cyber attacker may craft messages such as "*Click here to log in to your account and claim your reward!"* The common indicator is urgent requests for credentials and suspicious URLs.

Also, the study explored further cyber-technical tricks including Domain Spoofing, DNS Spoofing, and Man-in-the-Middle (MitM). Domain Spoofing involves registering a domain name similar to a legitimate one to deceive users into thinking they are communicating with the real entity (Buchanan *et al*., 2020) [8]. The objective is to trick individuals into providing sensitive information. An example of a cyber-technical trick phrase is *"Your subscription is about to expire, renew now at www.example-subscription.com!"*. The common indicator is detecting the look-alike domains in email addresses or/ typos. Moreover, DNS Spoofing is the technique that redirects traffic from a legitimate website to a malicious one by corrupting the DNS cache (Ahsan *et al*., 2022; Newaz *et al*., 2021) [2, 24]. The objective is to redirect users to fraudulent sites without their awareness. One example of a cyber-technical trick phrase is like this "*due to maintenance, please login through this alternative link."*. The common indicator is detecting unexpected DNS changes and redirected web traffic. On the other hand, the Man-in-the-Middle (MitM) is an attack where the attacker secretly intercepts and relays messages between two parties. The objective is to eavesdrop on communications or manipulate data being transmitted (Sakthivel *et al*., 2020) [30]. The common examples of cyber-technical trick phrases include statements like "*to ensure your data is secure, please re-enter your login information*." The common indicators are SSL warnings and insecure connections.

Other common cyber-technical tricks are Credential Harvesting, SSL Stripping, and Card Skimming. Credential Harvesting is a trick that involves collecting user credentials through deceptive means, often through phishing (Hu, 2021) [17]. The objective is to gain unauthorized access to accounts or systems. The common cyber-technical tricks phrase is *"Your login attempt was unsuccessful, please enter your username and password to try again.".* The common indicator is detecting fake login pages and prompts for credentials. Another trick is SSL Stripping that attack downgrades a secure HTTPS connection to an unsecured HTTP connection without the user's knowledge (Sakthivel *et al*., 2020) [30]. The objective is to intercept sensitive data that would otherwise be encrypted. For example, the cyber attacker may craft a message such as "*Your session has expired, please log in again using the link below."*. The common indicator is missing HTTPS and warnings of insecure sites. Moreover, the Card Skimming trick involves the use of devices to capture card information from unsuspecting users at ATMs or point-of-sale terminals (Riggs *et al*., 2023) [28]. The objective is to steal credit or debit card information for fraudulent transactions (Buchanan *et al*., 2020) [8]. An example of a common cyber-technical trick phrase is *"Please enter your PIN for verification."*. The common indicator is detecting unusual charges and tampered card readers. Another common cyber-technical trick is URL Manipulation which is a tactic that involves altering the URL to mislead users into visiting malicious sites (Newaz *et al*., 2021) [24]. The objective is to trick users into clicking links that lead to phishing sites or malware downloads (Oz *et al*., 2022) [25]. For example, the attacker may use fake links such as "*Visit our official site: www.yourbank.com.login-update.com to verify your account"*. The common indicator is noticing the Suspicious URLs and misleading links.

Furthermore, the study described the common cyber-technical tricks such as Data Breach through Phishing, Exploit Vulnerabilities, and Credential Stuffing (Sakthivel *et al*., 2020) [30]. Data Breach through Phishing is the tactic that uses phishing emails to gain access to sensitive data, often leading to significant data breaches (Cobb, 2024) [10]. The objective is to compromise databases and steal large amounts of personal information (Riggs *et al*., 2023) [28]. The common cyber-technical trick phrase of this trick is "*Urgent: Your account information needs updating."*. The common indicator is detecting compromised accounts and receiving notifications of unauthorized access. Exploit Vulnerabilities is another trick that involves taking advantage of weaknesses in software or hardware to gain unauthorized access. The objective is to infiltrate systems for data theft or disruption. An example of the cyber-technical trick phrase is like that "*Your software is outdated. Click here to download the latest version."* The common indicator is detecting unpatched software and unexpected behavior of the system.

Moreover, Credential Stuffing is a trick that uses stolen username and password pairs from one breach to gain access to accounts on other services (Ahsan *et al*., 2022) [2]. The objective is to exploit users' tendency to reuse passwords across different platforms. The cyber-attacker may craft a tricky message such as "*Your login attempt has failed. Please verify your credentials."* The common indicator is noticing the multiple failed login attempts and account lockouts. On the other hand, Phishing via SMS (Smishing) is among the common cyber-technical tricks that involve sending fraudulent SMS messages to deceive individuals into revealing personal information (Buchanan *et al*., 2020; Sakthivel *et al*., 2020) [8, 30]. The objective is to exploit

mobile users who may not be as cautious as with email (Hu, 2021) [17]. One example of the cyber-technical trick phrase is "*Your package has been delayed, click this link to reschedule delivery."* The common indicator is receiving unexpected SMS with links or requests. Other common cyber-technical tricks are Fake Academic Portals, Network Sniffing, and Fake Donation Links. The Fake Academic Portals are fraudulent websites designed to mimic legitimate academic institutions to collect personal information from students. The objective is to obtain sensitive data, including financial information and identities. The cyber attackers may craft cyber-technical trick phrases to trick users such as *"Welcome to the new student portal. Please log in to access your courses", or "Your scholarship application requires additional information—click here to submit."* The common indicator is receiving links look-alike websites, and requests for personal data.

Network Sniffing is another technique that involves monitoring and capturing data packets traveling over a network. The objective is to collect sensitive information, such as passwords or unencrypted data. For example, the cyber-technical trick can be phrased as *"We need to check your network settings—please provide your login details".* The common indicator is detecting unusual network traffic and data leakage. Moreover, Fake Donation Links are fraudulent websites set up to solicit donations under false pretenses, often for fake charities. The objective is to exploit the goodwill of individuals for financial gain. An example of a cyber-technical trick phrase can be presented as ". *Click here to donate to our cause!"* The common indicator is requests for donations via unfamiliar channels.

In addition, the study described other common cyber-technical tricks such as Social Media Phishing, SCADA Exploits, and Network Scanning. Social Media Phishing is a trickle tactic that uses fake profiles or messages on social media platforms to deceive users into revealing personal information (Hu, 2021; Sakthivel *et al*., 2020) [17, 30]. The objective is to gain access to accounts or steal personal data. The common cyber-technical trick phrase may crafted as *"Congratulations! You've won a prize! Click here to claim it."* The common indicator is receiving unusual messages from friends, and suspicious links. Moreover, the SCADA Exploit is a trick that attacks target Supervisory Control and Data Acquisition (SCADA) systems to disrupt critical infrastructure (Buchanan *et al*., 2020) [8]. The objective is to manipulate or disable essential services, creating operational havoc (Ahsan *et al*., 2022; Newaz *et al*., 2021) [2, 24]. One of the examples of the cyber-technical trick phrase is likely that *"important update needed for the control system—click here to install the patch."* The common indicator is detecting unauthorized access to control systems. oreover, Network Scanning is another trick that involves probing a network for open ports and services to identify vulnerabilities. The objective is to gather information that can be used for further attacks. One example of the cyber-technical trick phrase is crafted as "*to enhance security, please log in to confirm your network configurations."* The common indicator is noticing unusual port activity and increased traffic. More examples are described in Table 2 in Appendix B, with detailed information on objectives, tools, and indicators each tricks on their respective targets.

3.3 Mitigation Strategies of Cyber-Psychological Tricks

Cyber-psychological tricks refer to tactics that exploit human psychology to manipulate individuals into taking actions that compromise their security or reveal sensitive information (Liu *et al*., 2022) [22]. These tricks are often employed in various cyber-attack methods, including phishing, social engineering, and scams (Geer, Jardine, and Leverett, 2020) [13]. Here are some common psychological tricks used in cyber contexts including urgency and scarcity when attackers create a sense of urgency or scarcity to prompt quick action without careful consideration. For example, they may claim that an account will be locked or that a limited-time offer is about to expire. This causes the psychological impulse or pressure that leads individuals to act impulsively, bypassing their usual caution (Rizk and Elragal, 2020) [29]. Authority when cybercriminals may impersonate figures of authority, such as company executives or law enforcement officials, to instill trust and compel victims to comply with their requests. In this case, the individual may be at the risk of a phisher attacker, because psychologically, people are more likely to comply with requests from perceived authority figures, reducing their skepticism (Hughes-Larteya, *et al*., 2021) [18].

Moreover, the common psychological tricks include trust exploitation, emotional manipulation, and reciprocity. Trust exploitation is when attackers often use familiar branding or names to appear legitimate. For example, they may create emails or messages that mimic trusted organizations. Trust exploitation creates a familiarity that can lead victims to let their guard down and engage with malicious content. On the other hand, **e**motional manipulation tricks are when cyber attackers invoke strong emotions such as fear, excitement, or sympathy. For example, cybercriminals might send messages claiming that a loved one is in danger and needs immediate financial help (Zwilling *et al*., 2022) [38]. In that sense, emotional responses can cloud judgment, making individuals more susceptible to manipulation. The reciprocity is done by the attacker by offering something of perceived value (like free software or gifts) to create a sense of obligation in the target, leading them to provide personal information in return. This principle of reciprocity can compel victims to comply with requests they might otherwise refuse. In addition, social proof is a trick when cybercriminals may leverage testimonials or claims that "many people" have taken advantage of an offer or have fallen for a scam, suggesting that the action is safe or common. This can encourage individuals to follow suit, believing that if others are doing it, it must be legitimate (Alghamdi, 2020) [3]. Understanding these cyber-psychological tricks is essential for individuals and organizations to enhance their cybersecurity awareness. By recognizing the tactics that attackers use, people can develop better defenses against manipulation and make more informed decisions when faced with potential threats. Therefore, the study established the mitigation strategies fin respectively to their target (Table 1) in Appendix A. The detailed explanations of Table 1 are provided hereby.

Mitigating strategies of cyber-psychological tricks refer to the techniques and approaches used to reduce or eliminate the impact of psychological manipulation tactics employed by cybercriminals (Inkster, Knibbs, and Bada, 2023) [19]. These strategies aim to enhance awareness and resilience among individuals and organizations to protect against various forms of cyber threats that exploit human psychology (Zende, 2022) [36]. This study explored several mitigation strategies including Fear, Authority, and social

proof (Zwilling *et al*., 2022) [38]. The fear can be mitigated by providing user education by training the users to recognize fear-based tactics in communications and encourage them to verify claims before acting, practicing calm communication by providing clear, calm, and factual responses to concerns rather than amplifying fear (Liu *et al*., 2022) [22]. We recommend using reassurance techniques such as clear communication, providing context, positive framing, and reinforcing procedures. Moreover, we can mitigate these fear tricks by establishing the incident response plan by developing a robust incident response plan to address potential threats, minimizing unnecessary fear (Hughes-Larteya, *et al*., 2021; Alghamdi, 2020) [18, 3]. The authority trick can be mitigated by improving the verification protocols by encouraging the users to independently verify the authority of the sender, such as checking official websites or contacting organizations directly, training the users about common tactics used by scammers to impersonate authority figures, including the use of fake email addresses, and follows the chain of command by establishing clear protocols for escalating concerns or verifying requests from authoritative figures (Inkster *et al*., 2023; Geer, Jardine and Leverett, 2020) [19, 13]. The social proof can be mitigated by teaching the users to critically evaluate claims of popularity or social endorsement, questioning the authenticity of testimonials, helping the users to understand that social proof can be manipulated and encouraging them to seek independent reviews or verification and increasing the awareness campaigns by run campaigns to inform users about the potential for fake endorsements and the importance of independent research (Alghamdi, 2020; Rizk and Elragal, 2020) [3, 29].

The study explored the mitigation strategies for psychological tricks such as exclusivity, scarcity, and emotional appeals. To mitigate the exclusivity tricks we can **e**ncourage skepticism by promoting a culture of skepticism regarding offers that sound too good to be true or claim exclusivity (Rizk and Elragal, 2020) [29]. Also, we can train the users to research offers that create a sense of exclusivity and check for legitimacy before engaging. This training increases the behavior of the users to verify offers (Abroshan, *et al*. 2021 [1]; Siddiqi, Pak, and Siddiqi, 2021). And, improve access control by implementing policies that require verification for exclusive offers within organizations to prevent unauthorized access (Inkster, Knibbs, and Bada, 2023; Hooks, *et al*., 2022) [19, 16]. The scarcity tricks can be mitigated by educating the tactics by informing users about the scarcity principle and how it can be used to manipulate decision-making (Alghamdi, 2020) [3]. Also, we can mitigate the trick by encouraging patience by reminding the users that legitimate offers will not disappear overnight and encouraging them to take their time before making decisions (Purwaningsih, Sholikhah, and Wardani, 2018) [26]. And, encouraging by teaching the users to research opportunities before acting on perceived scarcity to determine if the offer is genuine (Hughes-Larteya, *et al*., 2021) [18]. Moreover, the emotional appeals tricks can be mitigated by practices the Balanced Communication in ensuring that communications are factual and balanced, avoiding overly emotional language that can cloud judgment. Also, increase the awareness of Manipulation by educating the users about how emotions can be exploited in marketing and phishing attempts, fostering a critical mindset. And, **s**upporting the resources by providing the resources for emotional support that help users process emotional appeals without feeling pressured to act (Wang, Zhu, and Sun, 2021) [35].

Also, the study identified psychological tricks such as reciprocity, urgency, and familiarity. The reciprocity tricks can be mitigated by training the users to be cautious of unsolicited gifts or offers, understanding that these may come with strings attached, and making clear policies by establishing clear organizational policies regarding gifts and reciprocity to guide user behavior (Rizk and Elragal, 2020) [29]. The urgency trick can be mitigated by promoting due diligence by encouraging the users to take their time and conduct due diligence before responding to urgent requests or offers. Train the users to train users to verify the legitimacy of urgent communications by checking with trusted sources before acting. And, creating or raising awareness about the urgency tactic and its potential for manipulation, reinforcing the idea that legitimate requests allow time for consideration (Rizk and Elragal, 2020; Geer, Jardine, and Leverett, 2020) [29, 13]. The familiarity trick can be mitigated by conducting regular audits by conducting regular audits of communications to ensure they are secure and authentic, helping to prevent impersonation, and educating the users on phishing by training them to recognize phishing attempts that use familiar logos or language to deceive. And, applying the Multi-Factor Authentication adds an extra layer of security, reducing the impact of familiarity-based tricks (Abroshan, *et al*. 2021) [1]. Another common cyber-psychological trick is curiosity (Hooks, *et al*., 2022; Zende, 2022; Zwilling *et al*., 2022) [16, 36, 38]. Curiosity trick can be mitigated when taking caution with clicks, that is we advise the users to be cautious when clicking on links or opening attachments, especially from unknown sources, conducting the critical evaluation by teaching the users to evaluate the source and context of curious content before engaging with it. And, encourage users to verify URLs and search for reviews or information about unfamiliar links or offers (Liu *et al*., 2022) [22].

3.4 Mitigation Strategies of Cyber-Technical Tricks

According to Rapid (2024) [27], mitigation strategies for cyber-technical tricks involve a combination of proactive measures, user education, and technical controls to reduce the risk of cyberattacks. The study explored several technical tricks with their mitigation strategies (Table 2) in Appendix B. From Table 2 we discussed in detail the technical tricks to include Spoofing which is mitigated by implementing the SPF, DKIM, and DMARC which are used for email authentication protocols and verification of sender identities (Cobb, 2024; Rapid, 2024) [10, 27]. Other mitigation strategies in the trick are user education and regular audits (Riggs *et al*., 2023) [28]. The user education aimed to train the users to recognize suspicious emails and verify sender domains before taking action. And, regular Audits are done by conducting regular audits of domain registrations to identify look-alike domains (Cobb, 2024) [10]. On the other, hand, the Malware delivery technical tricks can be mitigated by the application of user antivirus and anti-malware software which they security software updated to detect and block malware. Moreover, the regular software is updated to ensure all systems and applications are patched to close vulnerabilities. And, also, train or educate the users on the safe browsing habits and risks of downloading unknown files (Newaz, *et al*. 2021; Hu *et al*., 2021) [24, 17].

On the other hand, the study explored the mitigation strategies for phishing kits, domain spoofing, and DNS Spoofing. The phishing kits are the mitigation strategies which include email filtering, user training, and report mechanism (Rapid, 2024; Hu *et al*., 2021) [27, 17]. Email filtering is done by implementing advanced email filtering solutions to detect and block phishing attempts (Cobb, 2024; Government of Canada, 2021) [10, 14]. The user training is conducted in regular sessions on recognizing attempts and suspicion links. The common training strategies include seminars and on-the-job training. Domain spoofing is a trick that is mitigated by domain monitoring, user verification, and HTTPS implementation (Newaz *et al*. 2021) [24]. The domain monitoring service is done to watch for a watch for similar domain registrations that could be used for spoofing. Moreover, the users are encouraged to verify URLs before entering sensitive information, and HTTPS implementations are done to ensure that all legitimate sites use HTTPS to secure communications (Oz *et al*. 2022, Gunduz and Das, 2020) [25, 15]. Notably, the single "S" letter in HTTPS, stands for security domain.

DNS spoofing is another cybercriminals technical trick. This tick is mitigated by implementing DNSSEC which is the use of DNS security Extension to protect against DNS spoofing attacks, monitoring DNS Traffic which is done by regularly analyses DNS traffic for unusual patterns or anomalies, and secure configuration to ensure DNS servers are securely configured and regularly updated (Government of Canada, 2021; Gunduz and Das, 2020) [14, 15]. Other technical tricks Man–in–the–Middle (MitM), Credential Harvesting, and SSL Stripping. The mitigation strategies of MitM include the use of Encryption usually SSL/TLS for secure communication and transfers, educating the users on their self-awareness to look for secure connection indicators in their browsers, to improving the network security by implementing strong network security measures such as firewall and intrusion detection systems (Oz *et al*. 2022, Gunduz and Das, 2020) [25, 15]. The credential Harvesting is mitigated by implementing the implement Multi-Factor Authentication (MFA) which adds an extra layer of security beyond just passwords (Rapid, 2024; Cobb, 2024; Newaz, *et al*. 2021) [27, 10, 24]. Also, the user training for educating users about the importance of using unique passwords and recognizing phishing attempts. And, password management is done by encouraging the users to use password managers to facilitate strong, unique passwords (Gunduz and Das, 2020) [15]. Moreover, common mitigating strategies of SSL Stripping are enforced HSTS for implementing the HTTP Strict Transport Security to ensure browsers only connect over HTTPS, improve the user's education by training them to recognize signs of security warnings in browsers, and ensure the regular audits for conduct security audits to identify and mitigate vulnerabilities (Government of Canada, 2021; Newaz *et al*. 2021; Oz *et al*. 2022) [14, 24, 25].

Another technical trick for cyber-attacks is Card Skimming. These tricks can be mitigated by improving the use of anti-skimming technology which will able to detect and prevent card skimming in point-of-sale systems (Riggs *et al*. 2023; Oz *et al*. 2022, Gunduz and Das, 2020) [28, 25, 15]. Also, it is recommended to ensure regular monitoring by conducting routine checks of card readers and ATMs for tampering and improving the users' awareness by educating customers on recognizing signs of skimming devices (Oz *et al*. 2022) [25].

On the other hand, URL Manipulation mitigation strategies include URL Filtering as the security solutions that filter and block access to known malicious URLs, improving users' education by training them to hover over links to check URLs before clicking and implementing secure coding practices to prevent URL manipulation vulnerabilities. In addition, Data Breach through Phishing is a technical trick that can be mitigated by implementing Advanced Threat Protection which detects and blocks advanced phishing threats, and conducting incident Response Planning by developing and maintaining an incident response plan for data breaches. And, do regular Security Awareness Training to keep users informed about new phishing tactics (Oz *et al*. 2022, Gunduz and Das, 2020) [25, 15].

Other technical tricks explored by this study are exploiting vulnerabilities, Credential Stuffing, and Phishing via SMS (Smishing). Exploit Vulnerabilities can be mitigated by Patch Management, which regularly updates and patches all software and systems to close known vulnerabilities, and scan vulnerabilities by conducting regular vulnerability assessments to identify and remediate weaknesses. And, practices the best security plan by following the security best practices for configuration and deployment of software (Riggs *et al*. 2023; Ahsan *et al*., 2022) [28, 2]. The Credential Stuffing mitigating strategies include the implanting of MFA by **e**ncouraging or requiring the users to use multi-factor authentication to protect accounts, applying the rate limiting on login attempts to deter automated attacks, and improving the user's education by educating them on the importance of using unique passwords for different accounts (Newaz *et al*. 2021) [24]. Moreover, the Phishing via SMS (Smishing) mitigating strategies include the conduct of user awareness campaigns to educate users about smishing and how to recognize it, applying the blocking measures by implementing technologies to block known smishing numbers, and improving the reporting mechanism by providing users with a way to report smishing attempts (Rapid, 2024; Riggs *et al*. 2023; Government of Canada, 2021) [27, 28, 14].

Other cyber technical tricks are Fake Academic Portals, Network Sniffing, and Fake Donation Links. This trick can be mitigated by encouraging the users to verify the legitimacy of educational institutions providing personal information, encouraging users to verify the legitimacy of educational institutions before providing personal information and Monitor the web for counterfeit educational websites (Oz *et al*. 2022, Gunduz and Das, 2020) [25, 15]. Network Sniffing can be mitigated by the use of Encryption to ensure that all sensitive data transmitted over the network is encrypted and, the use of network security tools such as intrusion detection systems to monitor for suspicious network activity (Oz *et al*. 2022) [25]. And, improving user awareness by educating users about secure network practices, especially on public Wi-Fi (Riggs *et al*. 2023) [28]. On the other hand, Fake donation Links can be mitigated by improving the verification of charities by encouraging the users to verify the legitimacy of charities before donating, improving user education by training them to recognize legitimate donation requests and URLs, and practices actively monitoring for fraudulent donation campaigns and report them, which is monitoring for scam.

The study also explored social media phishing, SCADA Exploits, and network scanning are common cyber technical tricks. Social media phishing can be mitigated by improving the profile privacy settings by encouraging users to adjust

privacy settings to limit exposure to potential scammers, improving the user's education by conducting training on how to recognize phishing attempts on social media platforms (Rapid, 2024; Riggs *et al.*, 2023) [27, 28]. And, improving the monitoring activity procedure by regularly monitoring social media channels for suspicious activity (Rapid, 2024; Cobb, 2024) [27, 10]. SCADA Exploits can be mitigated by implementing network segmentation by isolating the SCADA networks from corporate IT networks to reduce exposure (Cobb, 2024; Oz *et al.* 2022) [10, 25]. Also, practices regular security audits by **c**onducting security assessments to identify vulnerabilities in SCADA systems, and conducting employee training on the specific risks associated with SCADA systems and security best practices (Gunduz and Das, 2020; Sakthivel *et al*., 2020; Buchanan *et al*.,2020) [15, 30, 8]. Furthermore, the network scanning can be mitigated by improving the Intrusion Detection Systems by **i**mplementing the IDS to monitor network traffic for unauthorized scanning attempts, limiting exposure by restricting external access to sensitive network segments, and improving the user's education by educating them about the risks of unauthorized scanning and how to report suspicious activity (Ahsan *et al*., 2022; Sakthivel *et al*., 2020) [2, 30].

4. Discussion

The study described the common cyber-psychological tricks are Fear, Authority, Social Proof, Exclusivity, Scarcity, Emotional Appeals, Reciprocity, Urgency, Familiarity, and Curiosity. The common targets of cyber-attacks are Individuals, Organizations, Employees, Consumers, and Non-Profits. From this, we learned that the cyber-psychological trick mitigation strategies are weighted toward the end users of the technology. For example, in the mitigation for the fear trick, the individual should be trained about common scams, promote awareness of real threats, verify sender authenticity, and implement training on recognizing authority scams. In that sense, the effectiveness of the cyber-psychological trick mitigation strategies depends on the both *psychological and physiological capability of learning*. The psychological capability signifies the cognitive or mental ability and experiences in cybersecurity. That is the ability to learn. On the other hand, physiological capability includes the physical ability of an individual to learn such as audibility, visional, health, and other learning features. In other words, the responsibility of getting rid of cyberattacks is shifted to the end users. In that sense, preventing and combating cyber-attacks become challenging because the victims of cyber-attacks become the enablers or take part in the crime commission process. Unfortunately, some of the studies addressed the mitigating strategies to be applied on one side of the end users, overlooking the other side of the technology vendor or providers. This is a challenge that is required to be addressed by researchers and policymakers. Therefore, to overcome the cyber-psychological tricks we need a fundamental strategy: Training.

On the other hand, the common tools for cyber-psychological tricks are phishing emails, malware alerts (fake notifications), spoofed emails, fake notifications, fake reviews, social media posts, targeted marketing campaigns, promotional campaigns, manipulative ads, fundraising campaigns, fake donations, marketing campaigns, giveaways, promotional emails, ads, social media posts, newsletters, clickbait, and misleading content. From these tools we learn *two fundamental facts*; *cyber-attacks are done if there is communication between the attacker and victim*, and that communication is enabled through cyberspace. The communication messages (text, audio, image, video) can be channeled through email (enabled by website) or mobile phone enabled through mobile networks. In that sense, the messages are a *carrier* of both cyber-psychological and cyber-technical tricks. Therefore, we notice the important components where the cybercrime is committed (crime scene) that are mobile and website. That is, we can find deceived or illegal messages on websites/email and mobile phones. Because we cannot cease to communicate, therefore, we need to secure our communication through websites and mobile phones to reduce cyber-attacks.

Furthermore, the study described several cyber-technical tricks such as Spoofing, Malware Delivery, Phishing Kits, Domain Spoofing, DNS Spoofing, Man-in-the-Middle (MitM), Credential Harvesting, SSL Stripping, Card Skimming, URL Manipulation, Data Breach through Phishing, Exploit Vulnerabilities, Credential Stuffing, Phishing via SMS (Smishing), Fake Academic Portals, Network Sniffing, Fake Donation Links, Social Media Phishing, SCADA Exploits and Network Scanning. The mitigation strategies that are recommended include implementing the SPF, DKIM, and DMARC and educating the end-user on email verification, use of antivirus software and regular updates, training users to recognize phishing and Email filtering, monitoring domain registrations and User education on URL verification, implementing DNSSEC and Use secure DNS services, use HTTPS everywhere and implement VPNs, use MFA and educate users on recognizing fake sites, implement HSTS and Educate users on secure connections, and other. These strategies are technically drafted. They need know-how and skills in cybersecurity. Hence, becomes most applicable or relevant to cybersecurity professionals. On the other hand, the common indicators that can help the end users to detect easily cyber-attack attempts also are created technically. For example, the individual detects unexpected emails, mismatched sender addresses, slow performance, and unexpected pop-ups, urgent requests for credentials, suspicious URLs, look-alike domains in email addresses, typos and unexpected DNS changes, redirected web traffic. The logical question that results from these indicators is "*unexpected situation or condition of the services*", which is how the individual with little knowledge of how to use the technology can detect the "*unusual or unexpected condition* of the service. This also requires experience or technical know-how. In that, sense we learn that both the cyber-psychological and cyber-technical tricks can be mitigated by training.

5. Conclusion and Recommendation

The study aimed to provide or detect and mitigate the cyber-psychological and cyber-technical tricks. The study found that the common cyber-psychological tricks are Fear, Authority, Social Proof, Exclusivity, Scarcity, Emotional Appeals, Reciprocity, Urgency, Familiarity, and Curiosity. The study found that the effective mitigating strategy is training the users. On other hand, the common cyber-technical tricks are Spoofing, Malware Delivery, Phishing Kits, Domain Spoofing, DNS Spoofing, Man-in-the-Middle

(MitM), Credential Harvesting, SSL Stripping, Card Skimming, URL Manipulation, Data Breach through Phishing, Exploit Vulnerabilities, Credential Stuffing, Phishing via SMS (Smishing), Fake Academic Portals, Network Sniffing, Fake Donation Links, Social Media Phishing, SCADA Exploits and Network Scanning. Most cyber-technical trick mitigation strategies are technically crafted and require the technical know-how skill to be applied. They are related to advanced or experienced users or cybersecurity professionals. In other words, mitigating these cyber-technical tricks requires the end users to be trained on how to get rid of the cyber-attacks. Therefore, we concluded that cyber-attacks are achieved through practices of either cyber-psychological tricks or/cyber-technical tricks. The effective mitigation strategy is the training for users. Thus, we recommend that cybersecurity stakeholders (targets of cyber-attacks) such as health, education, government agencies, and business enterprises establish off and on-the-job training programs at the lowest level in their organization.

6. References

1. Abroshan H, Devos J, Poels G, Laermans E. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. IEEE Access. 2021; 9:44928-44949.
2. Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning Review. J. Cybersecur. Priv. 2022; 2:527-555. Doi: doi.org/10.3390/jcp2030027
3. Alghamdi MI. Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. Int. J. Interact. Mob. Technol. 2020; 14:210-224.
4. Anti-Phishing Working Group - APWG. Phishing Activity Trends Report, 4th Quarter 2023: Unifying the Global Response to Cybercrime. Activity October-December 2023 Published 13 February 2024, 2023.
5. Anti-Phishing Working Group (APWG) APWG. Phishing Activity Trends Report, 1st BAQuarter 2024: Unifying the Global Response, 2024.
6. Balkibayeva Z. Methods of Extracting and Analyzing Metadata for Evidentiary Purposes. Uzbek Journal of Law and Digital Policy. 2024; 2(5):31-44. Doi: doi.org/10.59022/ujldp.233
7. Bhavsar V, Kadlak A, Sharma S. Study on Phishing Attacks. International Journal of Computer Applications. 2018; 182(33):0975-8887.
8. Buchanan B, Bansemer J, Cary D, Lucas J, Musser M. Automating Cyber Attacks: Hype and Reality; Center for Security and Emerging Technology: Washington, DC, USA, 2020.
9. Bundala NN. Cybercrime: Psychological Tricks and Computer Securities Challenges. Asian Journal of Research in Computer Science. 2024; 17(12):1-17. Doi: doi.org/10.97 34/ajrcos/ 2024/ v17i 12525.
10. Cobb M. 16 common types of cyberattacks and how to prevent them. Search Security. Informa TechTarget, 2024.
11. Desetty AG, Jangampet VD, Pulyala SR. Phishing Attacks: Evolving Techniques, Emerging Trends, and Countermeasure Strategies. International Journal for Innovative Engineering and Management Research. 2020; 09(12):985 -991.
12. Federal Bureau of Investigation-FBI. Internet Crime Report 2023. Internet Crime Complaint Center, 2023.
13. Geer D, Jardine E, Leverett E. On market concentration and cybersecurity risk. J. Cyber Policy. 2020; 5:9-29.
14. Government of Canada – GC. Top 10 IT Security Actions to Protect Internet Connected Networks and Information (ITSM.10.089). Canadian Centre for Cyber Security; Cyber Security Guidance, 2021.
15. Gunduz MZ, Das R. Cyber-Security on Smart Grid: Threats and Potential Solutions. Comput. Netw. 2020; 169:107094.
16. Hooks D, Davis Z, Agrawal V, Li Z. Exploring Factors Influencing Technology Adoption Rate At the Macro Level: A Predictive Model. Technol. Soc. 2022; 68:101826. Doi: 10.1016/j.techsoc.2021.101 826.
17. Hu V. Machine Learning for Access Control Policy Verification; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021.
18. Hughes-Larteya K, Li M, Botchey FE, Qin Z. The Human Factor, A Critical Weak Point In the Information Security of An Organization's Internet Of Things. Heliyon. 2021; 27:6522-6535.
19. Inkster B, Knibbs C, Bada M. Cybersecurity: A critical priority For Digital Mental Health. Front. Digit. Health. 2023; 5:1242264. Doi: 10.3389/Fdgth.2023.1242264
20. Jones EE. Phishing Facts: Be Aware and Do Not Take the Bait! College of Education and Human Services. Utah State University. Sorenson Center for Clinical Excellence, n.d.
21. Kuzior A, Tiutiunyk I, Zielińska A, Kelemen R. Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies. 2024; 17(2):220-239. Doi: 10.142 54/2071-8330.2024/17-2/12
22. Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J, *et al*. Cyber Security Threats: A Never-Ending Challenge for E-Commerce. Front. Psychol. 2022; 13:927398. Doi: 10.3389/Fpsyg.2022.927398
23. Miller B, Miller K, Zhang X, Terwilliger MG. Prevention of Phishing Attacks: A Three-Pillared Approach. Issues In Information Systems. 2020; 21(2):1-8. Doi: doi.Org/10.48 009 /2_Iis_2020_1-8.
24. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks And Defenses. ACM Trans. Comput. Healthc. 2021; 2:1-44.
25. Oz H, Aris A, Levi A, Uluagac AS. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Comput. Surv. 2022; 54:238.
26. Purwaningsih DR, Sholikhah IM, Wardani E. Redefining Banyumas Local Values: Symbolisms in Batik Motifs. Lingua Cultura. 2018; 12(3):295-300. Doi: doi.org/10.2151 2/lc.v12i3.4206
27. Rapid. Types of Cybersecurity Attacks. Accessed at Types of Cyber Attacks, Hacking Attacks & Techniques. Rapid7 on 08/12/2024, 2024.
28. Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, *et al*. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors. 2023; 23:4060. Doi: https://doi.org/10.3390/s23084060
29. Rizk A, Elragal A. Data Science: Developing

Theoretical Contributions In Information Systems Via Text Analytics. J. Big Data. 2020; 7:1-26.
30. Sakthivel RK, Nagasubramanian G, Al-Turjman F, Sankayya M. Core-Level Cybersecurity Assurance Using Cloud-Based Adaptive Machine Learning Techniques for Manufacturing Industry. Trans. Emerg. Telecommun. Technol. 2020; 33:e3947.
31. Sathish AP Kumar, Vayansky I. Phishing – challenges and solutions. Computer Fraud & Security, 2018. Doi: 10.1016/S1361-3723(18)30007-1
32. Schuetzler RM. Trends in Phishing Attacks: Suggestions for Future Research. Information Systems and Quantitative Analysis Faculty Proceedings & Presentations, 2011. https://digitalcommons.unomaha.edu/isqafacproc/25
33. Schulze H. 2021 Business Email Compromise Report. Cybersecurity Insiders, 2021.
34. Siddiqi MA, Pak W, Siddiqi MA. A Study on the Psychology of Social Engineering-based Cyberattacks and Existing Countermeasures. Appl. Sci. 2022; 12:6042. Doi: https://doi.org/ 10.3390/app1212604
35. Wang Z, Zhu H, Sun L. Social Engineering In Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access. 2021; 9:11895-11910.
36. Zende S. Digitalization in India Prospect and Challenges. Int. J. Entrep. Technopreneur (INJETECH). 2022; 2:29-37.
37. Zhao S. Metatheory, Metamethod, Meta-Data-Analysis: What, Why, and How? Sociological Perspectives. 1991; 34(3):377-390.
38. Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. J. Comput. Inf. Syst. 2022; 62:82-97. Doi: 10.1080/08874417.2020.1712269
39. Zywave. Phishing Attacks: A cyber-security Guide for Employers and Individuals, 2020.