THE ASIAN BULLETIN OF BIG DATA MANAGEMENT
Vol.4. Issue4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.274

ASIAN BULLETIN OF BIG DATA MANAGEMENT
http://abbdm.com/
ISSN (Print): 2959-0795
ISSN (online): 2959-0809

An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey

Muhammad Umar Adil*, Sajjad Ali, Ali Haider, M. Aetsam Javed, Hamayun Khan

Chronicle

Article history

Received: Nov 3, 2024
Received in the revised format: Nov 27, 2024
Accepted: Dec 11, 2024
Available online: Dec 28, 2024

Muhammad Umar Adil & Sajjad Ali are currently affiliated with the Department of Information Security, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
Email: su92-msisw-f24001@superior.edu.pk
Email: su92-msisw-f24-003@superior.edu.pk

Ali Haider is currently affiliated with the DELL SecureWorks, Pakistan.
Email: digitaleyeali@yahoo.com

M. Aetsam Javed & Hamayun Khan are currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan, Pakistan.
Email:SU92-PHCSW-F24 023@superior.edu.pk
Email: hamayun.khan@superior.edu.pk

Corresponding Author*

Abstract

The improvements in digital communication have made communication between humans very instant. However, personal and sensitive information may be available online through social networks and online services that lack the security measures to protect this information. Social engineering attacks are inevitable and imperil the integrity, security, and confidentiality of the information used on social media platforms. Prominent technologies, such as blockchain, artificial intelligence (AI), and proactive access controls, were adopted in the literature to confront the social engineering attacks on social media. Social engineering has emerged as a significant threat in the realm of cybersecurity, exploiting human vulnerabilities rather than technological weaknesses. This review paper explores the various forms of social engineering attacks, their psychological underpinnings, and their impact on organizations and individuals. Furthermore, it examines current countermeasures and highlights gaps in existing approaches, proposing directions for future research and development in mitigating social engineering threats. Lastly, we shed light on the open issues and research challenges of social engineering attacks where research gaps still exist and require further investigation.

Keywords: Social Engineering, Cybersecurity, Human Vulnerabilities, Technological Weaknesses, Social Engineering Attacks, Psychological Underpinnings, Organizational Impact, Individual Impact, Countermeasures, Vishing, Voice Mining.

© 2024 The Asian Academy of Business and social science research Ltd Pakistan.

INTRODUCTION

Advancements in technology is improving the quality of services in almost all aspects of life. Cybersecurity defenses have traditionally centered on technological solutions, such as firewalls, encryption, and antivirus software, aimed at protecting systems from unauthorized access. However, attackers increasingly focus on exploiting human psychology—a far less fortified domain [1]. Social engineering has evolved into a sophisticated cyberattack strategy that manipulates individuals into revealing confidential information, clicking malicious links, or performing actions that compromise an organization's security. The success of these attacks often depends on the ability of attackers to exploit cognitive biases and social norms, bypassing even the most advanced technological defenses [2, 3]. Social engineering is not new; it predates digital technology. Techniques like impersonation, confidence tricks, and manipulation have been used for decades to exploit trust and authority [4, 5]. Attackers used spear-phishing techniques targeting Twitter employees. They gained access to internal systems, enabling them to compromise high-profile accounts, including those of Elon Musk, Bill Gates, and Barack Obama. The attackers posted cryptocurrency scams, causing financial and reputational damage. This attack highlighted the risks of insider manipulation through social engineering [6-8]. The Verizon Data Breach Investigations Report (DBIR) 2023 revealed that 74% of breaches involved a human element, including phishing and pretexting.

Social Engineering: An Overview

Social engineering is defined as the deliberate manipulation of individuals to gain unauthorized access to systems, networks, or sensitive information. Common methods include:

- **Phishing:** A prevalent attack involving deceptive emails or messages designed to harvest login credentials or deliver malware [9]. In 2022, phishing attacks increased by 61%, targeting employees in remote work setups.

- **Pretexting:** Creating a fabricated scenario to gain trust and extract information, such as impersonating an IT support representative [10].

- **Baiting:** Using physical devices like USB drives labeled "Confidential" to lure victims into introducing malware [11].

- **Tailgating and Piggybacking:** Exploiting human courtesy to gain physical access to restricted areas [12].

- **Vishing and Smishing:** Conducting phishing attacks over phone calls and SMS, respectively [13].

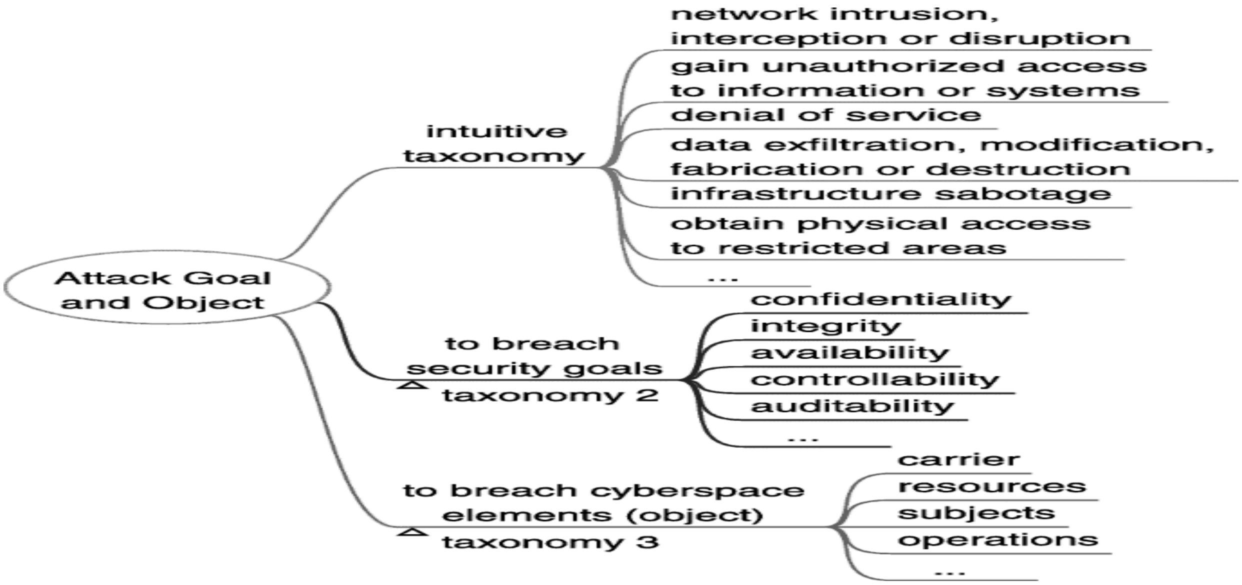
Attack Goal and Object
intuitive taxonomy
network intrusion, interception or disruption
gain unauthorized access to information or systems
denial of service
data exfiltration, modification, fabrication or destruction
infrastructure sabotage
obtain physical access to restricted areas
...
to breach security goals
taxonomy 2
confidentiality
integrity
availability
controllability
auditability
...
to breach cyberspace elements (object)
taxonomy 3
carrier
resources
subjects
operations
...

Figure 1.
Social Engineering attack Goals taxonomy [14]

According to Proofpoint's 2023 State of the Phish Report, 86% of organizations experienced phishing attacks, with 54% reporting financial losses as a direct consequence [15, 16]. This paper delves into the realm of social engineering, aiming to:

- Analyze the psychological mechanisms that make individuals susceptible to manipulation.
- Review the effectiveness of existing countermeasures, including technological and human-centric defenses.
- Identify gaps in current research and defense strategies, proposing innovative approaches to mitigate the risks posed by social engineering.
- Common Social Engineering Tactics: Highlighting phishing, baiting, vishing, and more.
- Psychological Principles Leveraged by Attackers: Exploring authority, urgency, and reciprocity.
- Countermeasures: Reviewing technological tools, training programs, and organizational strategies.
- Future Directions: Proposing advanced methods to strengthen defenses.

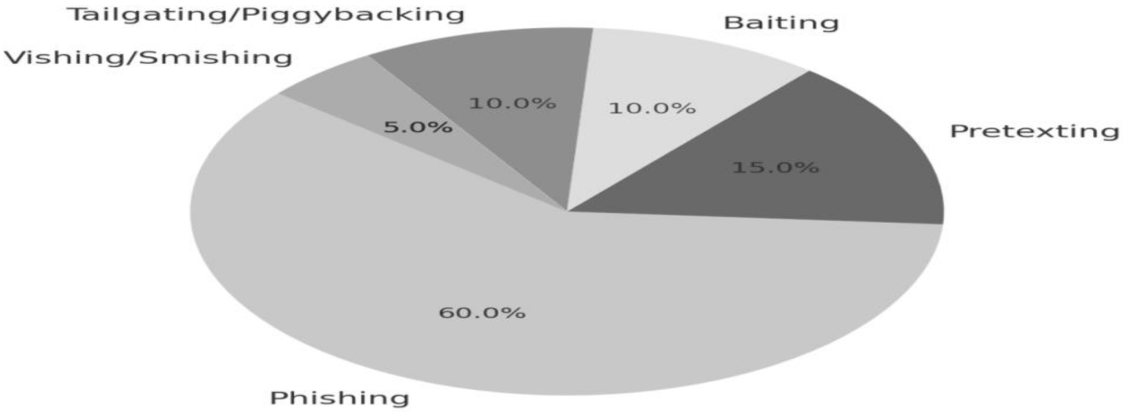

Figure 2.
Distribution of Social Engineering Attack Types

Figure 2 illustrates the breakdown of common social engineering attack types, with phishing accounting for the majority.

Social engineering exploits several psychological principles to manipulate victims:

- **Authority:** Victims comply with requests from individuals they perceive as authoritative figures, such as CEOs or government officials [19].
- **Urgency:** Creating a sense of immediate action to prevent adverse outcomes, such as account suspension or financial loss [20].
- **Reciprocity:** Triggering a sense of obligation by offering help or incentives [21].

- **Social Proof:** Leveraging trust in actions or decisions perceived as endorsed by others [22]. The consequences of social engineering attacks are profound and multifaceted:

- **Economic Losses:** Global losses from phishing attacks alone were estimated at $17 billion in 2022 [23].

- **Data Breaches:** Personal and organizational data theft leading to identity fraud and loss of competitive advantage [24].

- **Reputational Damage:** Organizations suffer long-term brand erosion and loss of customer trust [25].

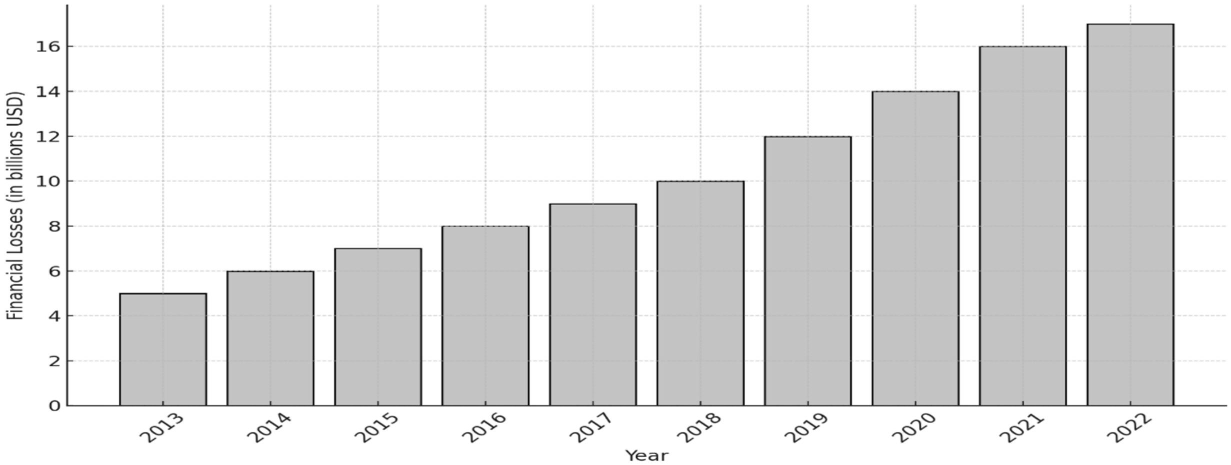

Figure 3.
Financial Losses from Social Engineering Attacks (2013-2022) [26]
This bar chart shows the annual financial losses caused by social engineering attacks, indicating a significant upward trend over the years.

Advanced Social Engineering Tactics

Attackers now use deepfake AI to generate synthetic voices or videos, impersonating trusted individuals during phone or video calls. For instance, in 2019, attackers impersonated a company CEO using a deepfake voice, tricking employees into transferring €220,000 to a fraudulent account [27, 28].

Emerging Trends

Social engineering attacks are increasingly paired with technical exploits. For example, phishing emails may deploy ransomware or malware, exploiting both human and technological vulnerabilities [29, 30]. Attackers use machine learning to analyze victim's social media and create highly personalized phishing emails, increasing the likelihood of success [31].

Social Media Exploits

Platforms like LinkedIn are used to gather sensitive information, such as job roles and internal organizational structures, to design convincing pretexting scenarios [32].

COUNTERMEASURES AGAINST SOCIAL ENGINEERING

Technological Defenses

- Email Filtering and Anti-Phishing Tools: Use AI to detect and block suspicious emails.
- Multi-Factor Authentication (MFA): Prevent unauthorized access even if credentials are compromised.
- Behavioral Analytics: Advanced tools monitor user behavior to identify anomalies, such as unusual login locations or times.
- Zero-Trust Architecture: Enforces strict identity verification for every user and device accessing a network [33].

Human-Centric Defenses

- Awareness Training: Regularly educating employees on recognizing phishing attempts and social engineering tactics.
- Gamified Training Programs: Making learning about cybersecurity engaging and interactive, increasing retention rates.
- Psychological Resilience Building: Reducing susceptibility to manipulation by addressing cognitive biases through training [34].

Organizational Strategies

- Incident Response Plans: Clearly defining steps to mitigate and report suspected attacks [35].
- Frequent Simulations: Conducting phishing simulations to test organizational readiness and identify vulnerabilities [36].
- Encouraging a Security-First Culture: Reward employees for reporting suspicious activities and improving overall vigilance [37].

TECHNOLOGICAL INNOVATIONS

Behavioral Analytics

Advanced security systems employ machine learning to analyze user behavior, identifying anomalies that indicate potential compromise. For example, if a user suddenly logs in from a new location or device, it triggers an alert. Blockchain technology is being explored for securing identity verification and ensuring data integrity, making it harder for attackers to falsify identities [38].

Compliance Requirements

Regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) mandate organizations to protect user data, indirectly reducing social engineering risks by enforcing strong security protocols. Agencies like CISA (Cybersecurity and Infrastructure Security Agency) in the U.S. regularly release guidelines and conduct awareness campaigns to educate the public about social engineering threats [39].

Gaps and Future Directions

- Limited Real-World Testing: Many countermeasures lack validation under real-world conditions.

- Insufficient Tailored Training: Generic training programs fail to address the unique needs of various organizational roles.

- Integration Gaps: Lack of synchronization between technological defenses and psychological insights.

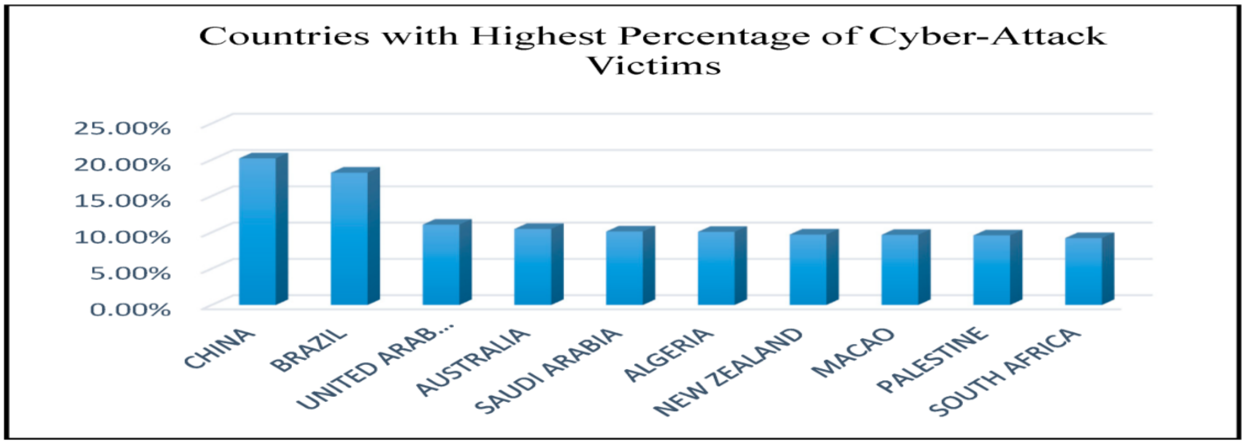

Figure 4.
Countries with the highest percentage of cyber-attack victims [40]

Proposed Directions

- AI-Driven Solutions: Develop AI tools that analyze user behavior in real time to detect social engineering attempts.

- Cross-Disciplinary Research: Collaboration between psychologists, cybersecurity experts, and sociologists to create holistic solutions.

- Global Threat Intelligence Sharing: Establish international platforms to share real-time data on emerging social engineering tactics.

Challenges in Countermeasure Implementation

- **Resource Constraints**

Small and medium-sized enterprises (SMEs) often lack the budget for robust training programs and advanced technological defenses, leaving them vulnerable.

- **Rapidly Evolving Threats:**

The dynamic nature of social engineering tactics means defenses quickly become outdated, requiring constant vigilance and adaptation.

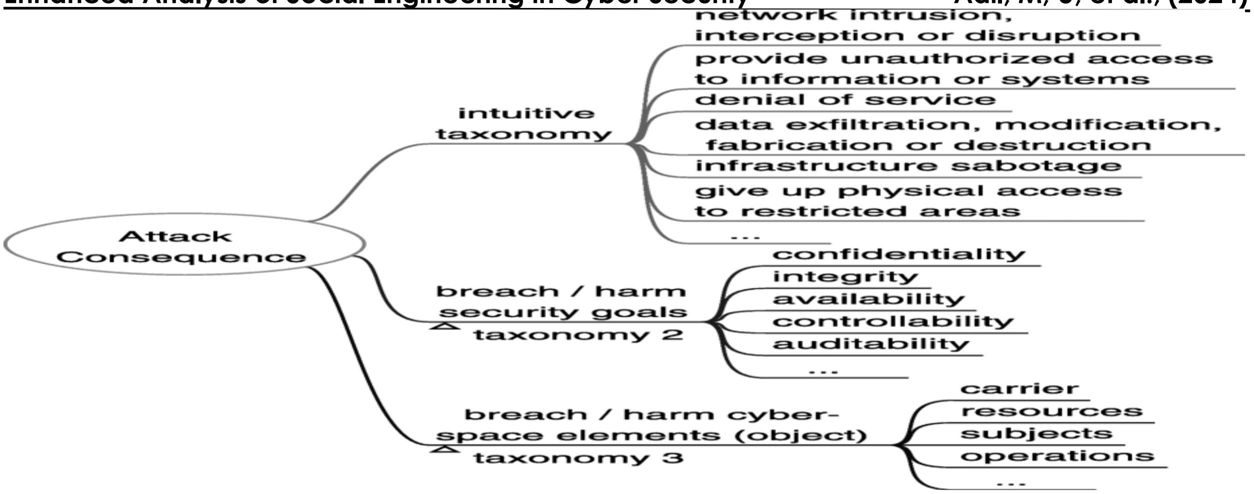
Attack Consequence
intuitive taxonomy
network intrusion, interception or disruption
provide unauthorized access to information or systems
denial of service
data exfiltration, modification, fabrication or destruction
infrastructure sabotage
give up physical access to restricted areas
...
breach / harm security goals
taxonomy 2
confidentiality
integrity
availability
controllability
auditability
...
breach / harm cyber-space elements (object)
taxonomy 3
carrier
resources
subjects
operations
...

Figure 5.
Cyber-attack Consequence[41]

Proposed Research Opportunities

- **Neuroscience-Based Insights:**

Studying cognitive biases, such as optimism bias or anchoring, to develop countermeasures tailored to human psychological weaknesses.

- **Global Collaboration:**

Sharing threat intelligence across borders can enhance the collective understanding and response to social engineering.

Real-World Attack Analysis

Attackers used phishing emails to trick employees into revealing login credentials, leading to a massive breach of sensitive data, including unreleased movies and employee information. This attack highlighted the role of social engineering in compromising even highly resourced organizations [42]. Social engineering was used to exploit a third-party vendor's credentials, allowing attackers to access Target's network. The breach resulted in the theft of 40 million credit card numbers and significant reputational damage [43].

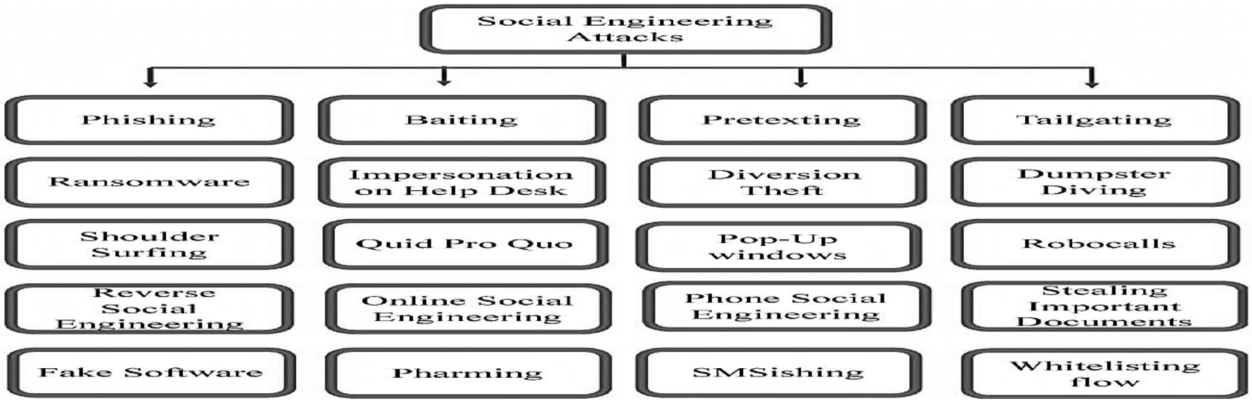

Figure 6.
Social Engineering Attacks[44]

Phishing attacks can be classified into five categories: spear phishing, whaling phishing, vishing phishing, interactive voice response phishing, and business email compromise phishing as illustrated in Figure 7.

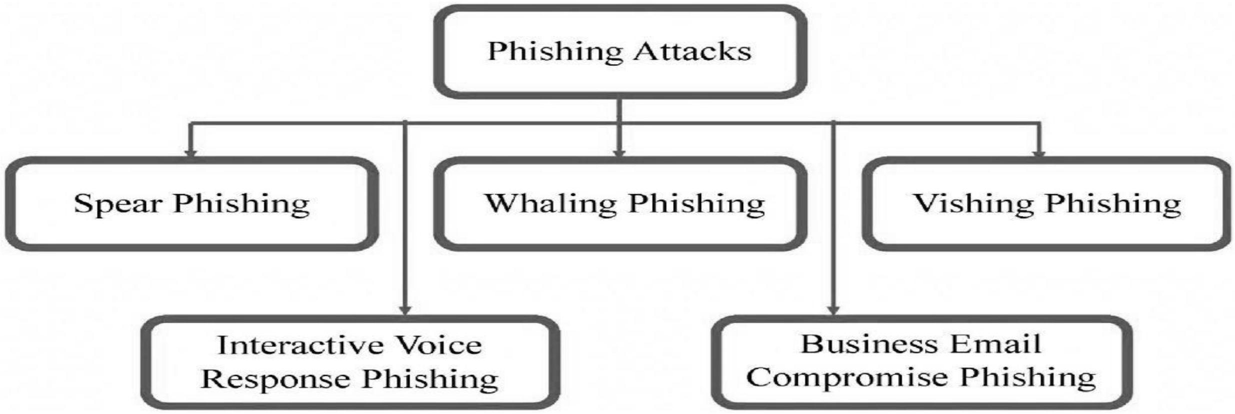
Phishing Attacks
Spear Phishing
Whaling Phishing
Vishing Phishing
Interactive Voice Response Phishing
Business Email Compromise Phishing

Figure 7.
Phishing Attacks [45]

CONCLUSION

Companies are investing large amounts of money and resources to establish effective strategies against social engineering attacks. However, existing detection methods have fundamental limitations and countermeasures are inefficient in coping with the ever-growing number of social engineering attacks. This paper provides an in-depth survey of different types of social engineering attacks with a detailed discussion on the working of attack, growth, and real-time use cases. Social engineering continues to pose a formidable challenge in cybersecurity, exploiting human vulnerabilities that cannot be easily patched with technological solutions. Its evolving nature and reliance on psychological manipulation make it a persistent and adaptable threat, often outpacing traditional security measures. The increasing sophistication of attacks, such as deepfake-based phishing and AI-driven impersonation, underscores the urgent need for robust, multi-layered defenses. Current countermeasures, though effective to an extent, often fall short of addressing the root causes of susceptibility to manipulation. While technological tools like multi-factor authentication (MFA) and advanced behavioral analytics can detect and prevent some attacks, they do not fully account for the human element. Psychological principles, such as trust, urgency, and authority, remain underexplored in the development of comprehensive solutions. Organizations must prioritize creating a culture of security awareness, where employees are empowered to recognize and report suspicious activities without fear of reprisal. Investments in regular training, simulation exercises, and psychological resilience programs are essential for reducing human susceptibility. Furthermore, leveraging emerging technologies, such as artificial intelligence and machine learning, can enhance the detection of sophisticated attacks by analyzing behavioral patterns and anomalies in real time.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), 183-196.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE) (pp. 62-68). IEEE.

Aldawood, H., & Skinner, G. (2019, May). Challenges of implementing training and awareness programs targeting cyber security social engineering. In 2019 cybersecurity and cyberforensics conference (ccc) (pp. 111-117). IEEE.

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

Heartfield, R., & Loukas, G. (2018). A taxonomy of attacks and a survey of defense mechanisms for social engineering. ACM Computing Surveys, 51(4), 1-39.

Hilas, C.S., Kazarlis, S.A., Rekanos, I.T. and Mastorocostas, P.A. (2014) A Genetic Programming Approach to Telecommunications Fraud Detection and Classification. International Conference on Circuits, Systems, Signal Processing, Communications and Computers, Venice, 29 September-1 October 2014, 77-8

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

Lansley, M., Polatidis, N., Kapetanakis, S., Amin, K., Samakovitis, G. and Petridis, M. (2019) Seen the Villains: Detecting Social Engineering Attacks Using Case-Based Reasoning and Deep Learning. Proceedings of the ICCBR Workshops, Otzenhausen, 8-12 September 2019, 39-48.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015, November). Mitigating social engineering for improved cybersecurity. In 2015 International Conference on Cyberspace (CYBER-Abuja) (pp. 91-100). IEEE.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

Salama, R., & Al-Turjman, F. (2023). Cyber-security countermeasures and vulnerabilities to prevent social-engineering attacks. In Artificial Intelligence of Health-Enabled Spaces (pp. 133-144). CRC Press.

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

Wilson, B. (2018). Introducing cyber security by designing mock social engineering attacks. Journal of Computing Sciences in Colleges, 34(1), 235-241.

Workman, M, Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674, 2008.

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

2024 by the authors; The Asian Academy of Business and social science research Ltd Pakistan. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).