International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (12)

IJCI

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (12)

December 2025

Analysis of the Study Cybersecurity Awareness for Hauman-Centered Protection Model in System Environments and Users Behavior

Anas Ahmed Nicola
Future University, Sudan
Faculty of Telecommunication and Space Technology Engineering, Suzhou University, China
anasnicola2018@gmail.com, anas_nicola@yahoo.com

Abstract

This paper explores the critical role of human behavior in cybersecurity vulnerabilities, emphasizing the psychological and social factors that influence decision- making at individual and organizational levels. Therefore, research directions in emerging technologies, behavioral analytics, and immersive community, in hold educational technologies. In the others side factors' addressing human-centric vulnerabilities, research aims to mitigate human error-driven from social digital resilience impact, across of the organizational domains. We describe why incorporating an understanding of human behavior into cyber security products and processes can lead to more effective technology. And the other illustrates how behavioral science offers the potential for significant increases in the effectiveness of cyber security. Based on feedback collected through electronic questionnaire that was distributed via social media applications form. The results, its shed light analyzing on the substantial contribution of understanding user behavior, and cognitive processes for to development of tailored cybersecurity strategies. The challenges, such as security fatigue and the scarcity of advocating for human factors engineering and strategic initiatives, leads us to develop human- centric paradigm in the next extension phase based on these results. However, we can develop and gives embracing a human-centric paradigm against dynamic and sophisticated cyber threats, by providing a model of awareness technologies training behavior cybersecurity shield of the

protection availabilities.

Keywords: Cybersecurity Awareness Training, Innovative Model, Micro-Learning Module, Cognitive Load, Bias Heuristics, Risk Communication, Health Models.

1. Introduction

Cybersecurity, faces escalating challenges, with human- centric factors emerging as pivotal elements influencing its effectiveness, as in-depth analysis of user- centric studies," this exploration aims to unravel the complexities surrounding human behavior, cognition and decision making"]2017]. In recent years, the surge in cyber incidents has underscored the significance of addressing the human dimension in cybersecurity [2018]. Understanding, analyzing, and mitigating the impact of human-centric aspects on cybersecurity. research. [2023]. underscores the significance of fostering cybersecurity awareness among students in a specific geographical context, shedding light on the challenges and strategies. One of the key challenges addressed in this analysis is the phenomenon of security fatigue [2016] identify security fatigue as an emerging issue, affecting cybersecurity personnel inundated by continuous security changes. Who proposed a framework for human-centered research in the context of cyber-attacks. This research compares three classification algorithms for malware detection, [2023], and similarly study by Hasas et al., [2024], enhancing digital security through dynamic Atta enhancing digital security through dynamic attack detection, contributing valuable insights to the evolving landscape of cybersecurity. Human and organizational factors happen to be the main contributors to, and causes of the technical and social vulnerabilities of an organization Computer and Information Security (CIS), [2020b]. adopting a holistic socio-technical system

perspective include governance and policy making issues; user-centered issues focusing on customers as well as hackers; and focused on external conditions, referred to physical, technological and economic conditions [2019].Predictive risk analytics, cyberpsychology, adaptive training, and AI-assisted behavioral monitoring are likely

to shape next-generation frameworks [2024].This dual focus on infrastructure and individual ethical behavior defines the expanded scope of modern cybersecurity strategy and underlines the urgency of a human-centered, ethically guided approach (Aksoy, 2024).

1.1 Literature review:

Authors: Albladi & Weir (2020), it explained the Predicting individuals' vulnerability to social engineering in social networks, his study examined the individual factors influencing susceptibility to social engineering attacks on social media. Kuraku et al. (2023), The study assessed the relationship between users' digital behaviors—such as password management and software updates—and their awareness of phishing threats. Results showed that improper digital habits increase exposure to attacks. And Moustafa et al. (2021), explored the psychological and behavioral traits of users, including impulsiveness and cautiousness, and their impact on cybersecurity practices. Findings emphasized the need for training programs that incorporate behavioral aspects of users. In addition, Bada et al. (2019), This paper analyzed why many cybersecurity awareness campaigns fail to bring meaningful behavioral change. It concluded that merely providing information is insufficient; addressing psychological motivations and providing practical engagement strategies are necessary. Furthermore, Wilcox & Bhattacharya (2020), The study examined how attackers exploit social and psychological factors when targeting users on social media platforms. It highlighted that cultural and contextual differences significantly influence individuals' susceptibility to social engineering. Haycock & Matthews (2020), This review explored the behavioral dimensions of cybersecurity, focusing on the psychological principles exploited in social engineering. Findings indicated that personality traits such as openness and agreeableness make some individuals more vulnerable to specific attack techniques.

2. Problem Statement

Security systems often impose rigid rules to maintain the integrity of the system. However, they fail to consider the behavioral diversity of users, which leads to consider. Such as, a Repeated human vulnerability, clicking on malicious links and using weak passwords or downloading files from unknown sources. Also, User frustration due to constant warnings and restrictions, which often leads them to ignore security instructions that they find annoying, or even attempt to bypass them. Lack of alignment between systems and users – This occurs because most systems fail to consider user behavior, which is often shaped by the individual's cultural background.

2.1 Research Objectives:

This research aims to study and analyze the role of the human user in compromising security systems, with a focus on the behaviors and practices that make the user the weakest link in the cybersecurity defense chain. The study seeks to achieve a set of objectives that can serve as a scientific foundation for the development of more effective security policies and strategies .

2.2 Methods:

On this study, researcher used analytical method, as it is the most suitable for studying social phenomena .Therefore, approach aims to describe and analyze the phenomenon, social engineering. And its associated attacks, as one of the most prominent, dangerous, and critical security threats targeting the human element . However, the data used on this research work was collected, through electronic questionnaire that was distributed via social media applications. A purposive sample was selected, consisting of individuals from the categories. The questioner used on this work, was divided into several sections with each section containing a set of questions designed to serve a specific objective. A total of 100 samples were collected from diverse groups to provide a clearer insight into these behavioral patterns.

methodology of this research work taken from different group society samples represent the analytical results. therefore, in this study the questioner taken from different sectors presented in "university, students, Private Sector Employees, Government Sector Employees, Business" and others. Furthermore", there is five section coverage on the questioner question ,below.

2.3 Research Questions:

1- Section A: General Information:

This section was designed to gather basic information about the respondents in order to categorize them into relevant groups. It includes personal questions such as; "Gender, age, level other the educational, nature of the work".

2- Section B :Awareness of Social Engineering:

This section consists of a few simple questions aimed at assessing users' awareness of social engineering techniques such as:

Have you heard of social engineering?

- Are you aware of its potential risks?
- Which social engineering techniques are you familiar with?
- Which is the risk of high attention?

3- Section C :Security Behaviors:

This section aims to understand users' security behavior patterns by asking questions that provide insight into their general practices, such as:

What would you do if you received an unexpected email requesting confidential information?

- Do you reuse passwords across multiple accounts?
- Do you regularly change your passwords?

- Do you verify the source of an email?

4. Section: D Personal Experiences:

This section collects users' personal experiences by asking whether they have been targets of social engineering attacks and requesting that they describe how they responded, providing deeper insight into user behavior under real attack scenarios.

5. Section E :Self-Analysis of Needs:

This section focuses on an important aspect—awareness of one's own knowledge limits. It includes two key questions designed to evaluate users' self-awareness and perceived need for further cybersecurity education.

How prepared do you feel to deal with social engineering attacks? The answer to this question reflects the user's self-awareness and confidence when facing such situations.

What methods do you believe are effective in raising awareness? The responses help identify approaches that resonate most with users, guiding the design of tailored frameworks and training programs to improve understanding of social engineering methods and associated risks.

In additions previously mentioned, the questionnaire was designed in a way that allows participants to respond comfortably, enabling us to gain a deeper understanding of user behavior within system environments. A total of 100 samples were collected from diverse groups to provide a clearer insight into these behavioral patterns.

3. Result and Discussion

- **Gender distribution:**

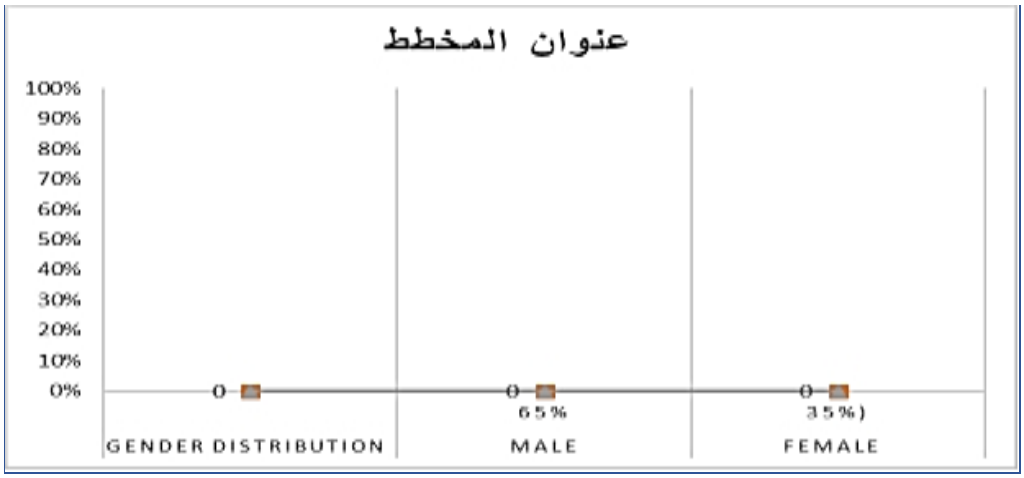

Figure (1) Gender distribution; (Male: 65%, Female: 35%)

- **Age Groups:**

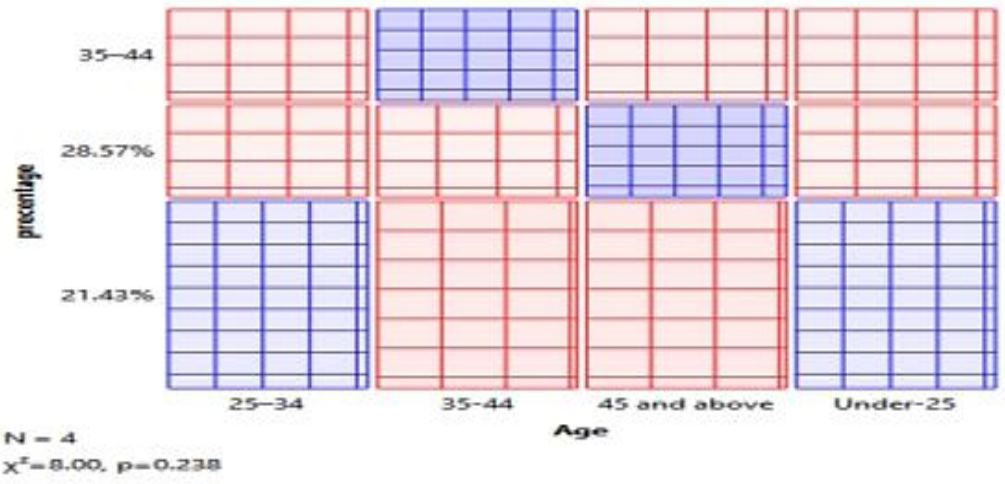

Figure (2) Age group distribution, (Under 25: 21.43%,35–44: 28.57%,35–44: 28.57%,45 and above: 28.57%)

- **Educational Level:**

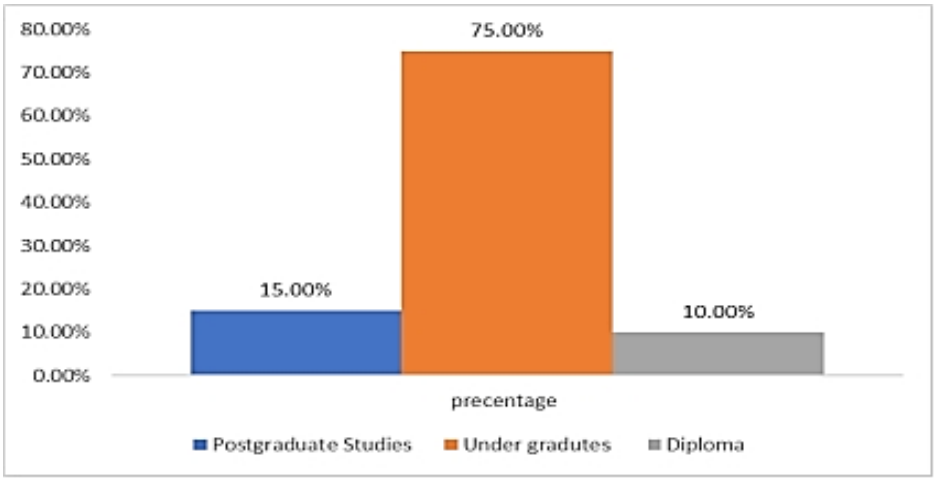

Figure (3) Sample distribution of educational levels, (postgraduate: 15%, Undergraduate's 75%, Diploma: 10%)

- **Nature of Work:**

Figure (4) E employees, job specification (Government employee: 21.43%, Private sector employee: 28.57%, Student: 35.71%, business 14.29%)

Cybersecurity training or a workshop:

Have you attending cybersecurity awareness workshop or Instruction?

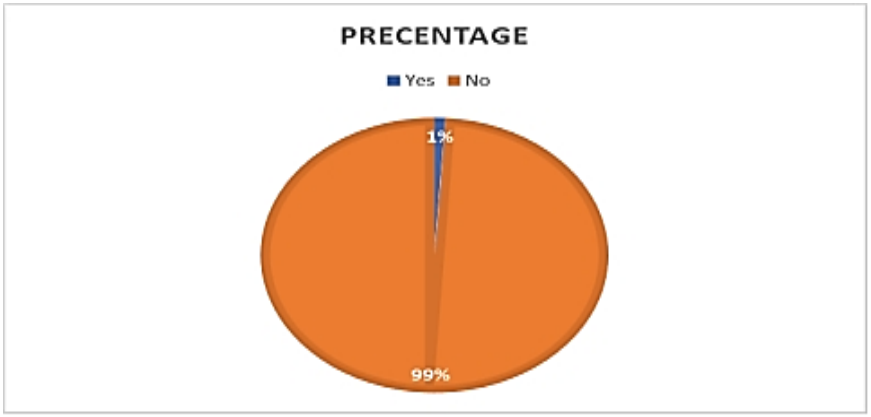

Figure (5) users' cybersecurity training workshop (Yes: 1%, No: 100%)

- **Social engineering:**

Have you known about social engineering?

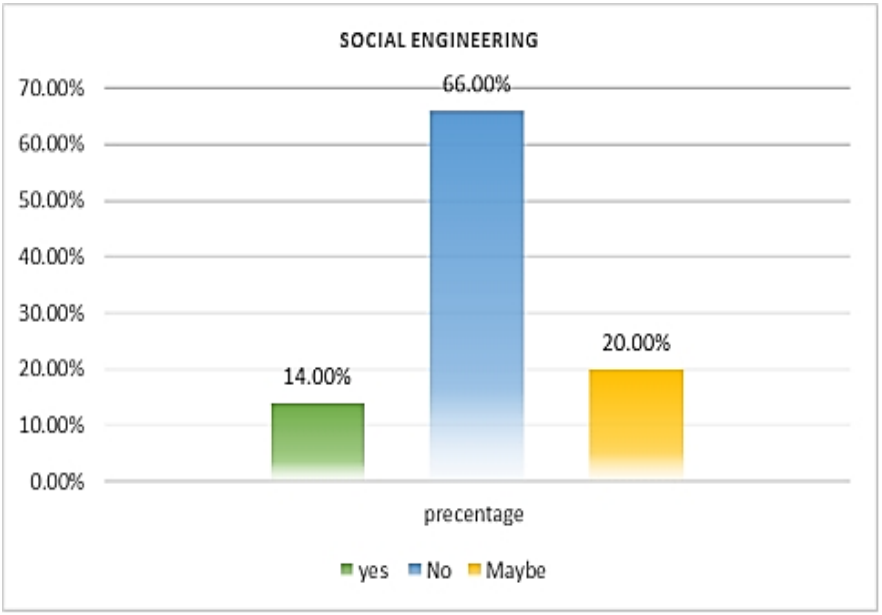

Figure (6) Users' ethnologies participated, (Yes: 14%, No: 66%, Maybe20%)

- **Social engineering attacks:**

How severe do you consider social engineering attacks?

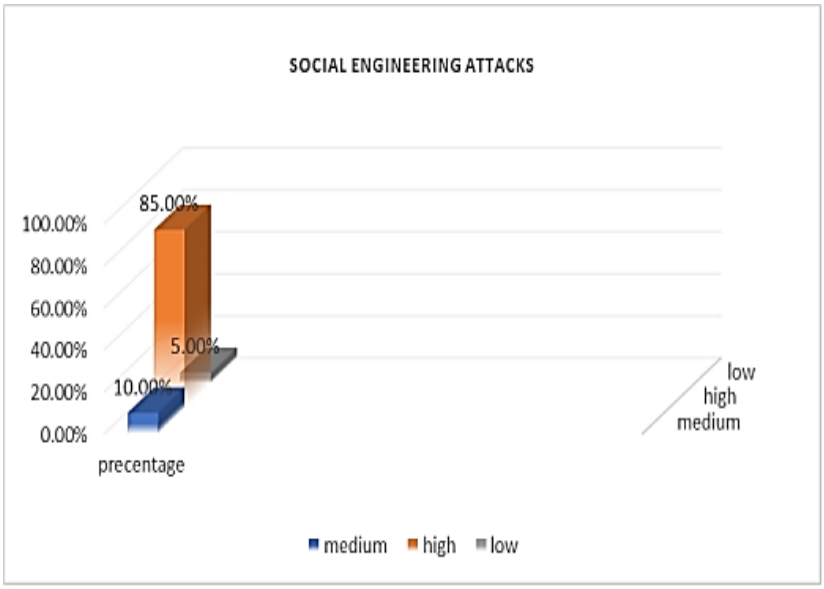

Figure (7) Social engineering attacks (Low: 10%, Medium: 5%, High: 85%)

- **Techniques: Familiar:**

Which of the following techniques are you familiar with or have heard of?

- Using Same password in Multiple Account?
- Using Different password in different account?
- Generally, create strong password?
- Not consider mostly for strong password?

International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (12)
IJCI
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (12)
December 2025

Figure (8) Techniques familiar, figure shown the level of the highest risk

Tabe (1) Explaining the level of the risk, security, in users account login

Password	**Student**	**percentage**	**level of the risk**
· Using Same password in Multiple Account?	mostly	85%	high
· Using Different password in different account?	some times	15%	high
· Generally, create strong password?	never	40%	medium
· Not consider mostly for strong password?	generally,	98%	high
Password	**Employee**	**percentage**	**level of the risk**
· Using Same password in Multiple Account?	mostly	70%	high
· Using Different password in different account?	some times	30%	Medium
· Generally, create strong password?	never	40%	Medium
· Not consider mostly for strong password?	generally,	60%	medium
Password	**Business**	**percentage**	**level of the risk**
· Using Same password in Multiple Account?	mostly	90%	high
· Using Different password in different account?	some times	10%	high
· Generally, create strong password?	never	5%	high
· Not consider mostly for strong password?	generally,	95%	high
Password	**Others**	**percentage**	**level of the risk**
· Using Same password in Multiple Account?	mostly	100%	high
· Using Different password in different account?	some times	0%	high
· Generally, create strong password?	never	0%	high
· Not consider mostly for strong password?	generally,	0%	high

Table (2) verify the source of the risk

	Student	percentage	level of the risk
Do you verify the source of the email before clicking on the link?	No	85%	high
Have you ever encountered or noticed an attempt at electronic hacking or deception?	yes	15%	high
Are you using originally software?	No	100%	high
Are you ready to face risks?	No	98%	high
Do you verify the source of the email before clicking on the link?	No	85%	high
Have you ever encountered or noticed an attempt at electronic hacking or deception?	yes	55%	high
Are you using originally software?	No	90%	high
Are you ready to face risks?	No	100%	high
Do you verify the source of the email before clicking on the link?	mostly	5%	high
Have you ever encountered or noticed an attempt at electronic hacking or deception?	some times	40%	Medium
Are you using originally software?	some times	40%	high
Are you ready to face risks?	No	95%	high
Do you verify the source of the email before clicking on the link?	No	5%	high
Have you ever encountered or noticed an attempt at electronic hacking or deception?	some times	20%	high
Are you using originally software?	No	100%	high
Are you ready to face risks?	NO	100%	high

3.1 Discussion:

In this study. the research work analyzing and shown much more points, of weakness, their data is among the most exposed to leakage due to the lack of attention by higher education institutions-particularly in Sudan. The study composed (University Students, Employee, Business, Others); However, to raising awareness among their students in the social engineering, the question here, how to protect themselves against it. Security behavior, such as. Security Awareness. We noticed that the higher educational level of users, greater their security awareness, meaning they become more prudent when operating within system environments. of the participants reuse

passwords across multiple accounts. In addition, participants percentages, the result taken shown the higher risk, when we analyzing and facing variabilities. The result refers to higher risk percentage generally between 80-95 %, lack of the preparing, and facing attacks, also, mostly results explaining that there is no protection from the attacks as shown in the table no 1 and 2. Table 3, and figure no 9. Table 4. Describe presented the security awareness percentage as in the lowest 2%, and the highest mostly much weakness, repeated in the whole sector is in the 100%, it comes from technical background of the how to facing and prepare for to prevent variabilities attacks or social engineer attacks. In addition, mostly attacks problems must to be solving by facing users in the technologies, training and cultures of the security awareness. See table (3) and 4 they explained how much variabilities attack the cultures environmental of the technologies.

Table (3) Social engineering attacks percentage

Data Table — Mon Dec 08 25, 1

Data instances: 12
Features: None
Meta attributes: 5

	Action	Stu_univ	employee	Private_Sectors	Business
1	Social engineer attacks	45%	72%	82%	70%
2	Clicking on malicious links	85%	45%	65%	55%
3	Using weak passwords	75%	67%	77%	50%
4	downloading files from unknown sources	82%	60%	75%	45%
5	Ignors secuirity instruction	87%	100%	100%	100%
6	secuirity awerness updated	2%	90%	100%	100%
7	Transfering files without cleaning	100%	100%	100%	100%
8	Using USB	100%	80%	90%	70%
9	lack of S.W protection	90%	75%	85%	85%
10	secuirty culuture training	90%	95%	98%	98%
11	Infection sources	60%	98%	95%	77%
12	Users Secuirity behaviour	70%	88%	94%	88%

International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (12)

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (12)

December 2025

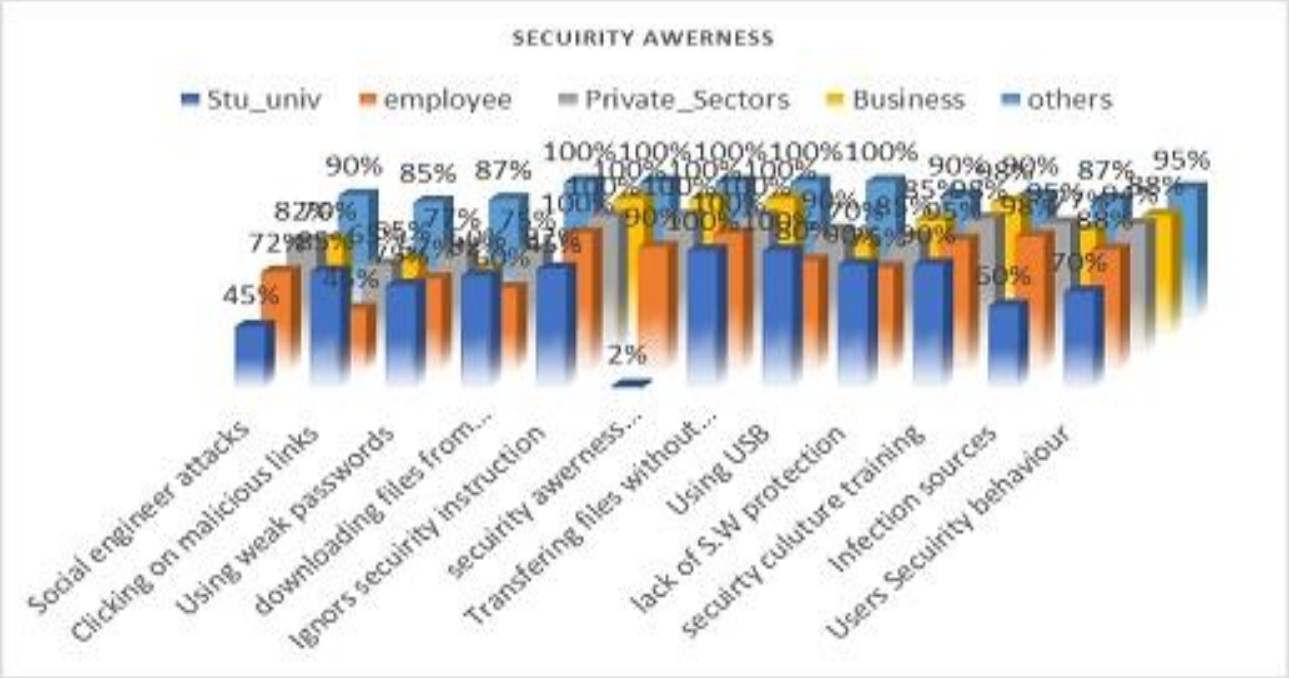

Figure (9) percentages of the social engineering attacks

Table (4) Data Instance

Data Table — Mon Dec 08 25, 1

Data instances: 12
Features: None
Meta attributes: 2

	Action	Total
1	Social engineer attacks	65%
2	clicking on malicious links	85%
3	using weak passwords	75%
4	downloading files from unknown sources.	82%
5	Ignors secuirity instruction	87%
6	secuirity awerness updated	2%
7	transfering files without cleaning	100%
8	using USB	100%
9	lack of S.W protection	90%
10	secuirty culuture training	75%
11	infection sources	80%
12	Users Secuirity behaviour	72%

According to participants and the results of research work, finding the best way to increase security awareness is come through focusing for to developing and enhancing, of the users' techniques, which come by some courses, training or workshop, and may be due to the perceived need for hands-on experience.

On the other hand, we believe that that any organizations, should conduct simulated attack tests on employees or system users in order to raise their awareness by letting them experience dealing with such attacks. Then, they can be evaluated based on their response so that tailored training sessions can be provided to meet their specific needs).

Key findings:

- **Lack of awarness:** The study finds that many users demonstrate low levels of understanding of basic cybersecuirity concepts such as fishing attacks and password.
- **Infuluence of enviroment:** the study highlights the importance of the work enviroment and orgnizational culture in shaping users' behaviour.

4. Conclusion

On this study, researcher gives remarkable and provide a summary of the most important findings; after collecting and analyzing the data through the questionnaire, we arrived at several points and results, Lack of awareness and caution can lead to system breaches. Most participants have a relative awareness of the risks of cyberattacks; however, ordinary users do not fully understand the severity of leaking their data. Traditional awareness programmed have a weak effect because, as mentioned earlier, they do not take user behavior patterns into account; they only provide information instead of offering practical training. They can suggest, here on the best way to classify users is based on the survey results. The most effective

methods to improve user behavior are through training courses and conducting simulations of real-life attacks that could occur. However, the human user is considered a fundamental pillar in the cybersecurity system, as any weakness in their awareness or a flaw in their behavior can lead to breaches of systems and sensitive information. Furthermore, the study examined the individual factors influencing susceptibility to social engineering, attacks" on social media. Findings revealed that network interaction levels and users' awareness of threats significantly affect their vulnerability to such attacks.

Reference

1. Carter, W.A. (2017). Forces shaping the cyber threat landscape for financial institutions. SWIFT Institute Working Paper No. 2016-004, October 2, 2017. Retrievedfromhttps://csisprod.s3.amazonaws.com/s3fspublic/171006_Cyber_Threat_Landscape%20_Carter.
2. Bureau, S. (2018). Human-centered cybersecurity: A new approach to securing networks. Research at RIT. Rochester Institute of Technology Research Report, Fall/Winter 2017-2018. [DOI: Not available].
3. Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in fghanistan: A Case Study of Badakhshan Province. American Journal of Education. Aand Tec.
4. hnology, 2(4), 50–61. https://doi.org/10.54536/ajet.v2i4.2248, Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88. doi:10.2478/hjbpa-2018-0024 [DOI: Not available]
5. Hakimi, M., Ahmady, E., Shahidzay, A. K., Fazil, A. W., Quchi, M. M., & Akbari, R. (2023). Securing Cyberspace: Exploring the Efficacy of SVM (Poly, Sigmoid) and ANN inMalware Analysis. Cognizance Journal of Multidisciplinary Studies, 3(12), 199-208.
6. Hasas, A., Zarinkhail, M. S., Hakimi, M., & Quchi, M. M. (2024). Strengthening DigitalSecurity: Dynamic Attack Detection with LSTM, KNN, and Random Forest. Journal ofComputer Science and Technology Studies, 6(1), 49–57.

7. Bicanic S, Brahm C, Bre C (2020) What to do now that your demand forecast is wrong. Bain & Co. https:// www. bain. com/ insig hts/ what- to- do- when- your- demand- forec ast- is-wrong/. Accessed 6Apr 2020
8. Addae JH, Sun X, Towey D, Radenkovic M (2019) Exploring user behavioral data for adaptive cybersecurity. User ModelUser-Adap Inter 29(3):701–750. https:// doi. org/ 10. 1007/s11257- 019- 09236-5
9. Huang, B. (2024). Navigating Digital Divide: Exploring the Influence of Ideological and Political Education on Cyber Security and Digital Literacy Amid Information Warfare.
10. Current Psychology, 43, 23815-23836. https://doi.org/10.1007/s12144-024-06106-1Aksoy, C. (2024). Building a Cyber Security Culture for Resilient Organizations againstCyber Attacks. İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7, 96-110.https://doi.org/10.33416/baybem.1374001
11. Albladi & Weir (2020) ource: SpringerOpen – Journal of CybersecuritySStudyink: How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks
12. Authors: Kuraku et al. (2023) Source: International Journal of Computer Trends and Technology (IJCTT)Study link: https://www.ijcttjournal.org/archives/ijctt-v71i11p111
13. Authors: Moustafa et al. (2021), "The Role of User Behaviour in Improving Cyber Security Management" Source: linkhttps://pubmed.ncbi.nlm.nih.gov/34220596
14. Authors: Bada et al. (2019), Source: arXiv (Cornell University) Study link: https://arxiv.org/abs/1901.02672
15. Authors: Wilcox & Bhattacharya, "A Human Dimension of Hacking: Social Engineering through Social Media" (2020), Source: arXiv.
16. Authors: Haycock & Matthews," Review and insight on the behavioral aspects of cybersecurity" (2020) Source: SpringerOpen – Journal of Cybersecurity.