

Strengthening Resilience to Safeguard Women from Social Engineering Attacks in Afghanistan

¹Musawer Hakimi; ²Amir Kror Shahidzay; ³Abdul Wajid Fazil;
⁴Khudai Qul Khaliqyar; ⁵Mohammad Mustafa Quchi

¹Assistant Professor at Department of Computer Science, Samangan University, Afghanistan

²Associate Professor at Faculty of Computer Science, Kabul University Afghanistan

³Assistant Professor at Department of IS, Badakhshan University Afghanistan

⁴Assistant Professor at Department of IT, Badakhshan University

⁵Assistant Professor at Department of Network Engineering, Faryab University, Afghanistan

¹musawer@adc.edu.in; ²shahizay@ku.edu.af; ³wajid@badakhshan.edu.af;
⁴kh.khaliqyar@badakhshan.edu.af; ⁵q.mustafa@faryab.edu.af

DOI: 10.47760/cognizance.2023.v03i12.009

Abstract: This study explores cybersecurity awareness and resilience among women at Women Online University in Afghanistan, focusing on social engineering threats. The introduction highlights the dynamic cybersecurity landscape, emphasizing the potent threat of social engineering attacks exploiting human vulnerabilities. Addressing a gap in understanding nuanced factors influencing women's vulnerability in academia, the research provides valuable insights for targeted interventions and policies. Using a robust quantitative methodology, the study involves 170 women from various faculties, employing a stratified sampling technique. Self-administered questionnaires with closed and open-ended inquiries capture participants' perspectives. The investigation meticulously identifies variables, categorizing them into independent, dependent, and control variables, using precise instruments like questionnaires for accuracy. Results depict diverse cybersecurity awareness, revealing variations in awareness levels and program effectiveness. ANOVA tests highlight significant differences, emphasizing the need for tailored program design. Regression analyses explore factors influencing vulnerability perception, emphasizing limited impact from personal information sharing on social media. The study uncovers notable differences in risk perception across categories, necessitating further exploration. In conclusion, this research provides nuanced insights into social engineering vulnerabilities among women in online education, emphasizing tailored interventions and considering socio-cultural nuances. Implications extend to informing policies, practices, and future research, aiming to enhance defense against social engineering threats for Women Online University in Afghanistan.

Keywords: Cybersecurity, Social Engineering, Women Online University, Resilience, Vulnerability

I. INTRODUCTION

In the ever-evolving landscape of cybersecurity, social engineering emerges as a potent and dynamic threat, exploiting human vulnerabilities. This comprehensive review navigates the intricate dimensions of social engineering attacks, examining their psychological intricacies (Krombholz et al., 2014), the impact of cultural factors (Thomson & Niekerk, 2018), and their intersections with other cyber threats like ransomware (Scaife et al., 2016). By synthesizing insights from diverse studies, this review contributes to a holistic understanding, essential for devising robust countermeasures in the face of sophisticated cyber adversaries. Cybersecurity stands at the forefront of contemporary challenges, with social engineering attacks posing intricate threats to individuals and organizations alike. As technology advances, so do the tactics employed by malicious actors,

necessitating a thorough examination of the evolving landscape. This comprehensive review delves into the multifaceted realm of social engineering attacks, shedding light on their various dimensions and the countermeasures needed to mitigate their impact. The term "social engineering" encompasses a spectrum of deceptive techniques used by adversaries to exploit human psychology and manipulate individuals into divulging confidential information or undertaking actions that compromise security. The significance of understanding social engineering lies in its ability to exploit the weakest link in the cybersecurity chain – human behavior. As observed by (Krombholz et al., 2014), advanced social engineering attacks often involve a sophisticated interplay of psychological manipulation and technical prowess. One crucial aspect explored in this review is the role of social networking sites in providing fertile ground for social engineering exploits. (Algarni et al., 2013) emphasize the need to measure the source credibility of social engineering attackers on platforms like Facebook, underlining the importance of understanding how individuals perceive and interact with potential threats in online social spaces. Furthermore, the review delves into the cultural dimensions of social engineering, recognizing the need for culturally sensitive approaches to prevent and counteract these attacks (Thomson & Niekerk, 2018). In a globalized world where digital interactions transcend geographical boundaries, an awareness of cultural nuances becomes imperative in designing effective cybersecurity policies. The interconnected nature of cybersecurity challenges is evident in the overlap between social engineering and other threats, such as ransomware attacks. The work of (Scaife et al., 2016) on Crypto lock underscores the intricate nature of these threats and the necessity for holistic cybersecurity strategies.

As the digital landscape continues to evolve, this review aims to provide a nuanced understanding of social engineering attacks, considering their psychological, cultural, and technical dimensions. By synthesizing insights from diverse studies, it contributes to the ongoing discourse on fortifying the human and technological elements of cybersecurity to create a more resilient defense against sophisticated social engineering threats.

Statement of the Problem

In the academic landscape of Women Online University in Afghanistan, a pressing concern emerges regarding the cybersecurity awareness and resilience among its diverse faculty members. Despite the increasing prevalence of social engineering attacks, there exists a noticeable gap in understanding the nuanced factors influencing women's vulnerability within this academic setting. The current study aims to address this gap by delving into the intricacies of social engineering threats, considering variables such as general and specific awareness, effectiveness of educational programs, and the impact of socio-cultural factors. Recognizing the critical importance of cybersecurity in academic institutions, this research seeks to contribute valuable insights that can inform targeted interventions and policies. The multifaceted nature of the problem requires a nuanced exploration, emphasizing the need for a comprehensive understanding of the socio-cultural dynamics and the efficacy of current awareness and resilience strategies among women at Women Online University.

II. LITERATURE REVIEW

The literature on social engineering attacks reveals a complex landscape that exploits human psychology and technological vulnerabilities. (Krombholz et al., 2014) emphasize the intricate nature of advanced social engineering attacks, which often involve a sophisticated interplay of psychological manipulation and technical expertise. Understanding the psychological intricacies of these attacks is crucial, as they target the human element, exploiting the weakest link in the cybersecurity chain. Social engineering attacks encompass a wide range of deceptive techniques designed to manipulate individuals into divulging sensitive information or taking actions that compromise security. (Algarni et al., 2013) highlight the significance of measuring the source credibility of social engineering attackers, particularly on platforms like Facebook. This underscores the importance of understanding how individuals perceive and interact with potential threats in online social spaces. As social networking sites become integral to daily life, they also become fertile ground for social engineering exploits. Cultural dimensions add another layer of complexity to social engineering. (Thomson et al., 2018) advocate for culturally sensitive approaches in preventing and counteracting these attacks. In a globalized world where digital interactions transcend geographical boundaries, an awareness of cultural nuances is imperative in designing effective cybersecurity policies. This cultural sensitivity acknowledges that social engineering tactics may vary based on cultural contexts and norms. The interconnected nature of cybersecurity challenges becomes evident when exploring the overlap between social engineering and other threats, such as ransomware attacks. (Scaife et al., 2016) delve into the intricate nature of Crypto lock, emphasizing the need for holistic cybersecurity strategies. Ransomware, as a subset of cyber threats, demonstrates the evolving tactics employed by malicious actors and the importance of a comprehensive defense strategy. The literature underscores the

multifaceted nature of social engineering attacks, emphasizing the need for a holistic understanding that incorporates psychological, cultural, and technical dimensions. This nuanced perspective is essential for devising robust countermeasures against increasingly sophisticated cyber adversaries. By synthesizing insights from diverse studies, the literature review contributes to the ongoing discourse on fortifying the human and technological elements of cybersecurity to create a more resilient defense against social engineering threats (Krombholz et al., 2014; Algarni et al., 2013; Thomson & Niekerk, 2018; Scaife et al., 2016).

Research Objective

- To Evaluate the existing level of awareness among women at Women Online University regarding social engineering attacks and their potential risks.
- To Investigate specific vulnerabilities and risk factors that make women at Women Online University susceptible to social engineering attacks.
- To Assess the effectiveness of existing security measures and awareness programs implemented at Women Online University to mitigate social engineering threats.
- To Examine how socio-cultural factors in Afghanistan contribute to the vulnerability of women at Women Online University to social engineering attacks.
- To Develop targeted recommendations and strategies to enhance the resilience of women at Women Online University against social engineering attacks, considering the specific context of Afghanistan

III. RESEARCH METHODOLOGY

This research employs a comprehensive and robust research framework that integrates both descriptive and explanatory methodologies, emphasizing a quantitative approach to unravel insights into the experiences of women in various faculties at Women Online University in Afghanistan. The key components of the research methodology are outlined below:

The study adopts a mixed-methods research design, combining both descriptive and explanatory elements. This design allows for a nuanced exploration of women's perspectives in the university setting.

Sample and Sampling Technique: The research involves a cohort of 170 women from diverse faculties at Women Online University. Utilizing a stratified sampling technique, participants are systematically categorized based on their academic disciplines, ensuring a representative presence from each faculty. This strategic sampling approach enhances the relevance and inclusiveness of the study.

Research Instrument: Data collection relies on self-administered questionnaires, thoughtfully constructed to include a mix of closed and open-ended inquiries. This meticulously structured questionnaire serves as a valuable tool for systematically acquiring pertinent data aligned with the research objectives, facilitating a comprehensive understanding of participants' perspectives.

Data Gathering Procedure: The data gathering process is meticulously designed to ensure efficiency and accuracy. Participants will be provided with the carefully crafted questionnaires, and their responses will be collected systematically to maintain the integrity of the data.

Data Analysis: Upon data collection, a thorough validation process is implemented to guarantee completeness and accuracy. The quantitative analysis is conducted using SPSS version 23, leveraging a versatile analytical toolkit. This includes descriptive statistics, inferential statistics such as ANOVA, coefficients, and correlation analyses. Regression analyses are further employed to extract meaningful insights into the intricate relationships between variables, enriching the depth of the study's findings.

Ethical Considerations: The ethical dimensions of this research are of utmost importance. The study adheres to ethical guidelines, ensuring participant confidentiality, informed consent, and the responsible use of data. Ethical considerations are woven into every stage of the research process to maintain the integrity and credibility of the study.

IV. RESULT

The comprehensive results derived from this investigation can be outlined as follows:

TABLE 1: Age of Participant

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	73	42.9	42.9	42.9
	25-30	97	57.1	57.1	100.0
	Total	170	100.0	100.0	

Table 1: The table illustrates participant age distribution, with 42.9% falling in the "18-24" range and 57.1% in the "25-30" category. The cumulative percentage confirms complete coverage of the specified age groups, totaling 100%.

TABLE 2: Education Faculty

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Medical	82	48.2	48.2	48.2
	Engineering	36	21.2	21.2	69.4
	Economic	14	8.2	8.2	77.6
	Computer Science	18	10.6	10.6	88.2
	Education	20	11.8	11.8	100.0
	Total	170	100.0	100.0	

Table 2: This table outlines the distribution of participants across faculty categories, with the majority, 48.2%, affiliated with the Medical faculty. Engineering follows at 21.2%, Economic at 8.2%, Computer Science at 10.6%, and Education at 11.8%. The cumulative percentage confirms comprehensive coverage, providing a clear snapshot of faculty representation crucial for contextualizing research findings in diverse academic disciplines.

TABLE 3: Descriptive Statistics on General Awareness

	N	Minimum	Maximum	Mean	Std. Deviation
Faculty	170	1.00	5.00	2.1647	1.42544
General Awareness	170	1.00	2.00	1.2588	.43928
Valid N (listwise)	170				

Table 3: illustrates Regarding "General Awareness," participants' ratings spanned from 1.00 to 2.00, with a mean of 1.2588 and a standard deviation of 0.43928. These statistics suggest a generally low to moderate level of awareness among participants regarding social engineering threats.

TABLE 4: Frequency on Specific Awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Familiar	38	22.4	22.4	22.4
	Slightly Familiar	35	20.6	20.6	42.9
	Moderately Familiar	97	57.1	57.1	100.0
	Total	170	100.0	100.0	

Table 4: The frequency distribution for the variable "Specific Awareness" provides a comprehensive overview of participants' responses regarding their awareness of common social engineering tactics. The majority of participants (57.1%) reported being "Moderately Familiar," indicating a moderate level of awareness. Additionally, 22.4% indicated being "Not Familiar," while 20.6% reported being "Slightly Familiar." These findings suggest a diverse range of awareness levels among participants, with a significant portion having a moderate understanding of common social engineering tactics. The cumulative percentages illustrate the distribution of responses across the various familiarity levels, contributing to a nuanced understanding of participants' awareness in the context of specific social engineering tactics

TABLE 5: ANOVA test for Educational Programs Evaluation

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	46.002	4	11.500	49.260	.000
Within Groups	38.522	165	.233		
Total	84.524	169			

Table 5: The analysis of variance (ANOVA) was employed to evaluate the effectiveness of social engineering awareness educational programs at Women Online University. The results revealed a significant difference in mean effectiveness ratings across various groups ($F = 49.260, p < 0.05$). This suggests diverse perceptions among participants regarding the efficacy of the programs. The substantial between-groups variance indicates the need for a tailored approach in program design. Understanding the factors contributing to these differences can inform targeted interventions, ensuring effectiveness across diverse groups. Further investigation into specific program aspects and subgroup analyses is recommended for a nuanced understanding and improvement of social engineering awareness initiatives.

TABLE 6: Coefficients on Identification of Vulnerabilities

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.827	.670		2.726	.007
	Identification Vulnerabilities	.081	.159	.039	.511	.610

Table 6: The regression analysis indicates that the identification of vulnerabilities related to personal information sharing on social media has a limited impact on the perception of vulnerability among women at Women Online University ($\beta = 0.039, p = 0.610$). The constant term ($B = 1.827, p = 0.007$) suggests a baseline level of perception, and the small and non-significant coefficient for the identification of vulnerabilities implies that this specific factor does not exert a statistically significant influence on perceived vulnerability. While there is a positive trend, it is not strong enough to be considered a significant contributor. Further exploration of additional factors may be necessary to gain a more comprehensive understanding of perceived vulnerability to social engineering attacks among women in the online university context

TABLE 7: ANOVA Test based on Risk Perception

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	11.528	4	2.882	15.353	.000
Within Groups	30.972	165	.188		
Total	42.500	169			

Table 7: The ANOVA results indicate a statistically significant difference in the perception of social engineering risks among women at Women Online University across different categories ($F = 15.353, p < 0.001$). The between-groups sum of squares (11.528) is higher than the within-groups sum of squares (30.972), suggesting variability in risk perception scores between categories. This signifies that there are notable

differences in how women at the university perceive social engineering risks. Further analysis, such as post-hoc tests, can help identify specific group differences and provide insights into the factors influencing varying risk perceptions.

TABLE 8: Correlations on Awareness of Institutional Policies

		Policies	Faculty
Awareness of institutional policy	Pearson Correlation	1	.049
	Sig. (2-tailed)		.528
	N	170	170
Faculty	Pearson Correlation	.049	1
	Sig. (2-tailed)	.528	
	N	170	170

Table 8: The correlation analysis between Awareness of Institutional Policies and Faculty reveals a very weak positive correlation (Pearson Correlation = 0.049) with a p-value of 0.528, which is not statistically significant. This suggests that there is no substantial linear relationship between women's awareness of institutional policies related to social engineering and their faculty affiliations at Women Online University. The lack of a significant correlation indicates that awareness of institutional policies does not vary significantly based on the faculty to which the women belong. This outcome emphasizes the need for targeted awareness initiatives across faculties to ensure a consistent understanding of institutional policies related to social engineering and cybersecurity among women at the university.

TABLE 9: Descriptive Statistics on User-Friendliness of Security Measures
Awareness of Reporting Procedures

	N	Minimum	Maximum	Mean	Std. Deviation
Faculty	170	1.00	5.00	2.1647	1.42544
User-Friendliness of Security Measures	170	1.00	2.00	1.5000	.50148
Awareness of Reporting Procedures	170	1.00	2.00	1.7765	.41784
Valid N (list wise)	170				

Table 9: The analysis of the data indicates that for the variable "User-Friendliness of Security Measures," the scores range from 1.00 to 2.00, with a mean of 1.5000, suggesting a relatively low level of perceived user-friendliness. In the case of "Awareness of Reporting Procedures," the scores range from 1.00 to 2.00, with a mean of 1.7765, indicating a moderate level of awareness regarding reporting procedures. The standard deviations provide insights into the degree of variability around the mean for each variable. These findings suggest that there might be room for improvement in enhancing the user-friendliness of security measures for women at Women Online University. Additionally, efforts could be directed towards further increasing awareness of reporting procedures to ensure a more comprehensive understanding among the university's female population. These insights can inform targeted interventions aimed at improving the cybersecurity experience for women at the university.

TABLE 10: Descriptive Statistics on Perception of Socio-Cultural Factors Gender Norms and Digital Literacy Perceived Support Structures

	N	Minimum	Maximum	Mean	Std. Deviation
Faculty	170	1.00	5.00	2.1647	1.42544
Perception of Socio-Cultural Factors	170	3.00	5.00	3.9294	.71812
Gender Norms and Digital Literacy	170	3.00	5.00	4.1882	.86338
Perceived Support Structures	170	1.00	3.00	1.8118	.86338
Valid N (list wise)	170				

Table 10: The descriptive statistics reveal key insights into participants' perceptions at Women Online University regarding socio-cultural factors, gender norms, digital literacy, and support structures in the context of social engineering vulnerability. The "Perception of Socio-Cultural Factors" is deemed highly influential (mean = 3.93), emphasizing the significant impact of socio-cultural elements on the likelihood of women falling victim to social engineering attacks. Similarly, participants attribute a high impact (mean = 4.19) to "Gender Norms and Digital Literacy," indicating a belief in their substantial contribution to vulnerability. However, perceptions about the effectiveness of "Perceived Support Structures" vary (mean = 1.81), emphasizing the need for nuanced and tailored support mechanisms. These diverse perspectives underscore the complexity of addressing social engineering vulnerability in an online academic setting, calling for comprehensive strategies that consider socio-cultural nuances, gender norms, and digital literacy.

TABLE 11: Descriptive Statistics on Evaluation of proposed strategies, Feasibility of implementation and user acceptance of resilience program

	N	Minimum	Maximum	Mean	Std. Deviation
Faculty	170	1.00	5.00	2.1647	1.42544
Evaluation of Proposed Strategies	170	1.00	3.00	2.0706	.71812
Feasibility of Implementation	170	1.00	3.00	2.0706	.71812
User Acceptance of Resilience Programs	170	3.00	5.00	3.9294	.69296
Valid N (list wise)	170				

Table 11: The descriptive statistics provide valuable insights into participants' perspectives at Women Online University regarding the effectiveness, feasibility, and user acceptance of proposed strategies aimed at enhancing resilience against social engineering attacks. The "Evaluation of Proposed Strategies" and the "Feasibility of Implementation" both exhibit similar mean scores of 2.07, suggesting a moderate perception of their efficacy and feasibility. In contrast, "User Acceptance of Resilience Programs" has a higher mean of 3.93, indicating a more favorable inclination towards the likelihood of women at the university accepting and actively participating in such programs. These nuanced perceptions underscore the importance of considering not only the effectiveness and feasibility of proposed strategies but also the user acceptance and willingness to engage in resilience programs for a comprehensive approach to addressing social engineering vulnerabilities.

V. DISCUSSION

The comprehensive investigation into cybersecurity awareness and resilience among women at Women Online University in Afghanistan has yielded crucial insights, providing a nuanced understanding of the multifaceted nature of social engineering vulnerabilities in an online academic setting. This discussion aims to unpack and evaluate the key findings, drawing connections to the existing literature and culminating in a compelling argument in support of the overall conclusion. Demographically, the study revealed a majority of participants in the "18-24" age range, and a significant representation from diverse faculties, particularly the Medical faculty. These demographic details align with the global trend of higher education becoming increasingly accessible to a younger population, emphasizing the need for cybersecurity measures that resonate with the unique characteristics of these students (Table 1 and Table 2). The assessment of general awareness (Table 3) unveiled a moderate level of awareness regarding social engineering threats. This aligns with the literature emphasizing the importance of cultivating general awareness as a foundational element in cybersecurity resilience (Krombholz et al., 2014). However, the specific awareness of social engineering tactics (Table 4) demonstrated a diverse range of awareness levels, emphasizing the necessity of targeted educational interventions tailored to the varied understanding of participants. The evaluation of educational programs (Table 5) presented significant differences in effectiveness ratings, echoing the literature's call for tailored approaches in program design (Algarni et al., 2013). The coefficients on the identification of vulnerabilities (Table 6) indicated a limited impact, suggesting the need for a more nuanced exploration of factors contributing to vulnerability perception. The ANOVA test on risk perception (Table 7) showcased substantial variability, reinforcing the call for targeted interventions based on differing risk perceptions, consistent with the literature (Scaife et al., 2016). Correlation analysis (Table 8) highlighted a weak positive correlation between awareness of institutional policies and faculty, emphasizing the importance of consistent awareness initiatives across diverse academic disciplines. Descriptive statistics on the user-friendliness of security measures and awareness

of reporting procedures (Table 9) suggested potential areas for improvement, aligning with literature emphasizing the need for user-friendly security measures and comprehensive reporting procedures (Krombholz et al., 2014). Tables 10 and 11 delved into participants' perceptions of socio-cultural factors, gender norms, digital literacy, and support structures, as well as the evaluation, feasibility, and user acceptance of proposed resilience strategies. These nuanced perceptions underscored the complexity of addressing social engineering vulnerabilities, aligning with the literature's emphasis on considering socio-cultural nuances, gender norms, and digital literacy in comprehensive cybersecurity strategies (Thomson & Niekerk, 2018). In conclusion, the study's findings provide a rich tapestry of insights, painting a detailed picture of the cybersecurity landscape at Women Online University. The alignment of these findings with existing literature underscores the relevance and applicability of the study's methodology and results. The argument in support of the overall conclusion lies in the necessity of tailored interventions that address the unique demographics, awareness levels, and perceptions of social engineering vulnerabilities among women in diverse academic disciplines. This study contributes significantly to the ongoing discourse on fortifying cybersecurity measures in online academic environments, providing actionable insights for policy, practice, and future research.

VI. CONCLUSION

In summary, this research has delved into the intricacies of cybersecurity awareness and resilience among women at Women Online University in Afghanistan, with a focus on mitigating social engineering threats. The study's robust methodology, employing a quantitative approach and a stratified sampling technique, facilitated a comprehensive exploration of diverse facets within the online academic setting. Examining demographic patterns, awareness levels, and perceptions, the findings illuminate a complex cybersecurity landscape. The study revealed a moderate overall awareness of social engineering threats, accompanied by diverse understanding levels of specific tactics among participants. Educational programs demonstrated significant variations in perceived effectiveness, emphasizing the need for tailored approaches. The exploration of risk perception, institutional policy awareness, and user-friendliness of security measures pinpointed areas for targeted improvement. Furthermore, the nuanced perceptions regarding socio-cultural factors, gender norms, digital literacy, and proposed resilience strategies underscore the multifaceted nature of social engineering vulnerabilities. In conclusion, this research contributes valuable insights to the intersection of cybersecurity and online education, emphasizing the need for tailored interventions that consider the unique characteristics and perceptions of women in diverse academic disciplines. The significance of this study lies in its potential to inform policies, practices, and future research endeavors aimed at fortifying cybersecurity measures in online academic environments. As we navigate the ever-evolving cyber landscape, this research serves as a stepping stone towards creating a more resilient defense against social engineering threats, fostering a safer online academic experience for women at Women Online University in Afghanistan.

RECOMMENDATION

Based on the findings of this study, several recommendations are put forth to enhance cybersecurity awareness and resilience among women at Women Online University in Afghanistan.

Tailored Educational Programs: Design and implement cybersecurity awareness programs that are tailored to the diverse needs and understanding levels of women across different faculties. Programs should go beyond general knowledge and address specific issues relevant to each academic discipline.

Cultural Sensitivity Training: Incorporate cultural sensitivity training into cybersecurity awareness initiatives. Recognize and respect cultural nuances, ensuring that educational content aligns with the values and beliefs of the diverse student body.

Targeted Interventions: Develop targeted interventions based on the varying levels of awareness and perceptions identified in the study. Tailor strategies to address specific vulnerabilities and risk perceptions, ensuring a more personalized and effective approach.

Collaboration and Communication: Foster collaboration and communication between faculty members, cybersecurity experts, and students. Establishing an open dialogue can enhance the sharing of knowledge and experiences, contributing to a collective effort in strengthening the university's cybersecurity ecosystem.

Continuous Assessment: Implement a system for continuous assessment of cybersecurity awareness and resilience. Regularly evaluate the effectiveness of educational programs, adapting content and strategies based on feedback and evolving cybersecurity threats.

Integration of Socio-Cultural Factors: Integrate socio-cultural factors, including gender norms and digital literacy, into cybersecurity policies and awareness initiatives. Acknowledge the impact of these factors on vulnerability and tailor interventions to address the specific challenges posed by socio-cultural dynamics.

User-Friendly Security Measures: Enhance the user-friendliness of security measures to make it easier for women at the university to adopt and adhere to cybersecurity protocols. This includes simplifying reporting procedures and ensuring that security measures align with the preferences and habits of the user community.

Resilience Programs: Develop and promote resilience programs that focus on user acceptance and active participation. Emphasize the practicality and feasibility of these programs, considering the unique needs and expectations of women at Women Online University.

By implementing these recommendations, Women Online University can create a more robust and inclusive cybersecurity environment, fostering a safer online experience for its diverse student population.

ACKNOWLEDGEMENT

We extend our sincere gratitude to the Women Online University in Afghanistan for facilitating this research and to the participants whose valuable insights made this study possible. Our appreciation goes to the faculty members and administrators for their support throughout the data collection process.

Special thanks to our research team for their dedication and meticulous contributions at every stage of the study. The authors declare no conflicts of interest. This research adhered to ethical considerations, ensuring the privacy and confidentiality of participants. The study was conducted in accordance with the guidelines and regulations of the Women Online University's research ethics committee.

This work is dedicated to the pursuit of knowledge and the advancement of cybersecurity awareness, with the hope of contributing to a safer digital environment for women in online education.

REFERENCES

1. Albladi, S., & Weir, G. (2016). Vulnerability to social engineering in social networks: A proposed user-centric framework. In IEEE International Conference on Cybercrime and Computer Forensic.
2. Algarni, A., Xu, Y., & Chan, T. (2016). Measuring source credibility of social engineering attackers on Facebook. In IEEE Hawaii International Conference on System Sciences.
3. Algarni, A., Yue, X., Taizana, C., & Yu-Chu, T. (2013). Social engineering in social networking sites: Affect-based model. In IEEE International Conference for Internet Technology and Secured Transactions.
4. Aroyo, A. M., Rea, F., Sandini, G., & Sciutti, A. (2018). Trust and social engineering in human-robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations, or gamble? IEEE Robotics and Automation Letters.
5. Arana, M. (2017). How much does a cyberattack cost companies? Open Data Security, 1–4.
6. Atwell, C., Blasi, T., & Hayajneh, T. (2016). Reverse TCP and social engineering attacks in the era of big data. In IEEE International Conference of Intelligent Data and Security.
7. Bakhshi, T. (2017). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In IEEE International Conference on Emerging Technology.
8. Barbosa, R. R. R., Sadre, R., & Pras, A. (2013). Flow whitelisting in SCADA networks. International Journal of Critical Infrastructure Protection, 6, 150–158.
9. Beckers, K., & Pape, S. (2016). A serious game for eliciting social engineering security requirements. In International Requirements Engineering Conference.
10. Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cybersecurity. In International Conference on Technology, Education and Development.
11. Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. Network Security, 9, 5–9.
12. Chargo, M. (2018). You've been hacked: How to better incentivize corporations to protect consumers' data. Transactions: Tennessee Journal of Business Law, 20, 115–143.
13. Chothia, T., Stefan-Ioan, P., & Oultram, M. (2018). Phishing Attacks: Learning by Doing. USENIX Workshop on Advances in Security Education.
14. Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6, 1–31.
15. Costantino, G., La Marra, A., Martinelli, F., & Matteucci, I. (2018). CANDY: A social engineering attack to leak information from infotainment system. In IEEE Vehicular Technology Conference.

16. Cullen, A., & Armitage, L. (2016). The social engineering attack spiral. In IEEE International Conference on Cyber Security and Protection of Digital Services.
17. De Ryck, P., Nikiforakis, N., Desmet, L., & Joosen, W. (2013). Tabshots: Client-side detection of tabnabbing attacks. In ACM SIGSAC Symposium on Information, Computer and Communications Security.
18. Everett, C. (2016). Ransomware: To pay or not to pay? *Computer Fraud and Security*, 4, 8–12.
19. Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas'ud, M. Z. (2011). Generic taxonomy of social engineering attack and defense mechanism for handheld computer study. Malaysian Technical Universities International Conference on Engineering and Technology.
20. Ghafir, I. (2016). Social engineering attack strategies and defense approaches. IEEE International Conference on Future Internet of Things and Cloud.
21. Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In International Conference on Computing, Communication, and Automation.
22. Hadlington, L. (2018). The “human factor” in cybersecurity: Exploring the accidental insider. In Psychological and Behavioral Examinations in Cyber Security.
23. Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(1).
24. Hofbauer, S., Beckers, K., & Quirchmayr, G. (2015). Defense methods against VoIP and video hacking attacks in enterprise networks. In International Conference on e-Business.
25. Ho, G., Sharma, A., Javed, M., Paxson, V., & Wagner, D. (2017). Detecting credential spearphishing in enterprise settings. In USENIX Security Symposium.
26. Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. International Conference on Information Resources Management.
27. Hakimi, M., Fazil, A. W., Khaliqyar, K. Q., Quchi, M. M., & Sajid, S. (2023). Evaluating The Impact of E-Learning on Girl's Education in Afghanistan: A Case study of Samangan University. *International Journal of Multidisciplinary Approach Research and Science*, 2(01), 107–120. <https://doi.org/10.59653/ijmars.v2i01.368>
28. Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. *Applied Computer Systems*, 21, 38–45.
29. Kaushalya, S. A., Randeniya, R. M., & Liyanage, A. D. (2018). An Overview of Social Engineering in the Context of Information Security. IEEE International Conference on Engineering Technologies and Applied Sciences.
30. Fazil, A. W., Hakimi, M., Akbari, R., Quchi, M. M., & Khaliqyar, K. Q. (2023). Comparative Analysis of Machine Learning Models for Data Classification: An In-Depth Exploration. *Journal of Computer Science and Technology Studies*, 5(4), 160–168. <https://doi.org/10.32996/jcsts.2023.5.4.16>
31. Kim, H., Yoo, D., Kang, J., & Yeom, Y. (2017). Dynamic ransomware protection using deterministic random bit generator. In IEEE Conference on Applications, Information and Network Security.
32. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2016). Cutting the Gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.
33. Koyun, A., & Aljanaby, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology*, 4, 1–6.
34. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122.
35. 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 Afghanistan: A Case Study of Badakhshan Province. *American Journal of Educational Technology*, 2(4), 50–61.
36. Libicki, M. (2018). Could the issue of DPRK hacking benefit from benign neglect? *Georgia Journal of International Affairs*, 19, 83–89.
37. Lohani, S. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies in Science and Research*, 5.
38. Madain, A., Ala, M. A., & Al-Sayyed, R. (2017). Online social networks security: Threats, attacks, and future directions. In *Social Media Shaping e-Publishing and Academia*.