PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2026)**, 2026, **pp**. 88–96
ISSN: 3078-3186

Research Article

Human Factors in Information Security: A Quantitative Study on Phishing Susceptibility and Awareness Levels

Abdulazeez Alsajri[1, *], Amani Steiti[1],

[1] *Computer Science Department, University Arts, Sciences and Technology, Beirut, Lebanon*

[2] *faculty of information engineering, Department of Computer Systems and Networks, University Tishreen, Latakia, Syria*

ARTICLEINFO

Article History

Received 19 Dec 2025

Revised: 3 Feb 2026
Accepted 2 Mar 2026
Published 16 Mar 2026

Keywords

Phishing Susceptibility,

Cybersecurity Awareness,

Human Factors in Information Security,

Social Engineering Attacks,

Phishing Detection Behavior.

ABSTRACT

The research focused on studying multiple aspects of phishing attack vulnerability and the corresponding knowledge about phishing by examining how psychological and social and environmental elements affect people in their phishing attack susceptibility. We analyzed data from 1,200 participants through a quantitative approach which involved a standardized questionnaire to evaluate their phishing attack susceptibility and their knowledge of phishing threats across different demographic segments.

The data revealed that people between 18 and 25 years old became the most vulnerable age group to phishing attacks because their susceptibility rate reached 45% which exceeded the 30% rate found in older age groups (p 0.01). The test results showed that participants who had limited cybersecurity knowledge obtained phishing detection scores which were 15% lower than those who had better cybersecurity understanding (p 0.05).People who have restricted social connections network will click malicious links at a rate which is 40% higher than other users according to the analysis. The research showed that users who accessed their devices through mobile phones were 25% more likely to fall for phishing attacks than those who used their desktop computers for device access.

Educational content requires customization because research findings show mobile platforms and population groups face different obstacles which need to be addressed. The research findings show that cybersecurity training programs which provide complete coverage should combine community-based training with language-based programs to enhance security knowledge. Scientists must keep their research on phishing methods because these attacks keep evolving while educators need to develop adaptable educational approaches which defend students from these common security threats. Research findings show how human factors interact with information security systems to develop improved protection methods which defend against phishing attacks.

1. INTRODUCTION

Organizations from different sectors now consider information security as their top priority because cyber threats have grown both in complexity and occurrence rate [1]. Phishing attacks represent a common cybercrime method which targets human weaknesses instead of focusing on system vulnerabilities [2]. The attackers utilize fake messages to deceive users into providing their personal data which leads to substantial security risks for both individual users and their organizations. Security experts must focus on human factors which create phishing attack vulnerabilities because cyber threats are growing more common and sophisticated to develop effective security protection methods [3].

Research on phishing continues to grow yet scientists have yet to reach an agreement about which psychological and behavioral factors make people most likely to fall victim to phishing attacks. Researches who study this topic base their work on two main approaches which examine individual differences through cognitive styles and personality traits and previous experiences and they study how environmental conditions affect phishing attempts. Researchers need to study the combined effects of personal awareness and human decision methods because these elements create different levels of vulnerability to phishing attacks [5]. The current research literature does not provide enough information about social engineering tactics which use psychological manipulation to understand the complete range of human elements that affect phishing attacks [6].

*Corresponding author email: aka104@live.aul.edu.lb
DOI: https://doi.org/10.70470/SHIFRA/2026/004

The research project will perform statistical analysis to identify phishing risk relationships with security knowledge levels among different social groups which lack existing data. The research analysis seeks to identify how security awareness at various levels affects people who become victims of phishing attacks and their decision-making approaches which influence this relationship. The research study will prove human knowledge levels and awareness understanding about vulnerability patterns through their assessment of these elements which show the complete human element involved in phishing attacks.

The research findings will direct the creation of educational programs which will target specific learning needs and awareness initiatives [7]. Organizations need to identify the main elements which predict phishing attack vulnerabilities to create training programs that enhance their workforce ability to detect and prevent phishing attacks. The research results will help build the cybersecurity discussion because they show how system security improvements need to include human behavior patterns during system design. Organizations need to understand phishing evolution through human aspects because they require proper defense methods which effectively reduce security threats [8].

The document separates its content into different sections which begin with a literature review about phishing vulnerability and awareness levels before identifying essential research gaps. The study will present its methodological approach which implements quantitative methods for data collection and analysis [9]. The findings will be shown in the results section together with the main patterns which emerged from the data analysis. The discussion will connect these results to information security research while presenting operational guidance and research direction for upcoming studies [10].

The research aims to develop phishing susceptibility knowledge through its complete analysis while creating useful solutions for user information security awareness improvement [11]. The study aims to create a better digital security understanding among people through its focus on human elements in cybersecurity systems [12].

2. LITERATURE REVIEW

Phishing methods have developed through different periods which requires researchers to examine every human factor which results in phishing attack victimization [13]. Researchers in the scientific community have conducted multiple studies which identify the psychological and social and environmental elements which create phishing attack susceptibility in people. The review presents a summary of essential research results which shows the theoretical approaches used by scholars while pointing out inconsistencies and missing components in current studies [14].

The main focus of the research literature centers on psychological elements which determine how people become targets for phishing attacks. Researchers have studied how people differ through their cognitive patterns and their personality characteristics and their previous technological knowledge [15]. People who use intuitive thinking and analytical thinking methods develop their ability to detect phishing attacks through their cognitive styles [16]. People who rely on intuitive decision-making methods become more vulnerable to phishing attacks because their heuristic-based thinking patterns allow attackers to manipulate them. People who think analytically conduct detailed assessments which makes them less likely to be deceived [17].

Social engineering represents a vital component which enables phishing attacks to succeed. Social engineering attacks depend on human weaknesses which attackers use psychological methods to trick their intended victims. Research shows that attackers use methods which match the emotional and psychological conditions of their targets by using tactics to create urgent situations and show their power [18]. The process of manipulation reduces the ability of potential victims to defend themselves which makes them more vulnerable to attacks. The academic literature supports emotional appeal effects yet researchers require additional studies to determine how social engineering tactics affect human behavior based on individual psychological differences [19].

People need proper education about phishing to protect themselves from these attacks. Research shows that people who understand information security at high levels tend to fall for phishing attacks at lower rates [20]. Users who participate in awareness programs about phishing email characteristics and cybercriminal tactics will develop better detection abilities. These programs operate with different levels of success but experts remain uncertain about which educational approaches work best. Research findings about training methods show two opposing views because some research supports ongoing training programs yet other studies indicate that training which lasts for one session does not create permanent awareness [21].

Phishing research requires analysis of its fundamental conceptual frameworks which need to be studied. The Protection Motivation Theory and Health Belief Model along with other theories now help researchers study how people react to phishing attacks. These frameworks demonstrate that people will perform protective actions when they understand their risk and they believe their defense methods will work [22]. The implementation of these models for phishing research produces different results which create contradictory research outcomes when multiple studies apply them. The decision-making process of phishing victims becomes more understandable through the use of extra frameworks which combine behavioral economics with existing models [23].

Research into phishing vulnerability shows that specific environmental conditions determine which situations become vulnerable to phishing attacks. People become victims of phishing attacks based on their individual circumstances which

involve their workplace environment and the amount of distractions they face in their surroundings [24]. People who work in high-stress environments will select dangerous links when they act without thinking. An organization that maintains continuous cybersecurity awareness enables them to establish better defense systems which protect against these specific attack methods. The research field requires more empirical studies to determine how situational factors impact personal traits because scientists have not yet achieved a comprehensive understanding of this subject [25].

Research studies have explored how demographic characteristics affect people's ability to detect phishing attacks. People develop their response to phishing attacks based on their age and gender and their ability to use technology. Young people show the greatest vulnerability because they lack sufficient experience while they believe their digital skills exceed their actual abilities [26]. The older population tends to exercise more caution but they lack the required technical knowledge to recognize phishing threats effectively. The demographic information demonstrates that awareness programs need to customize their content because different user groups require distinct protection methods [27].

Researchers have made progress in determining factors which increase phishing threats yet current academic studies do not cover all critical aspects. Research requires long-term studies which track vulnerability changes throughout time because cybersecurity environments evolve continuously [28]. The research domain includes multiple studies which analyze human personality traits yet these studies fail to explore how these traits impact organizational policy and practice execution [29]. Research must investigate organizational cultural elements which influence staff responses to phishing threats because this knowledge will enable organizations to create improved cybersecurity defense systems [30].

Research documents personal characteristics together with environmental elements which affect the success of phishing awareness initiatives to determine how vulnerable people are to phishing attacks. Theoretical frameworks provide us with valuable knowledge but we still lack complete understanding of how these elements connect to each other. The research study brings together current studies to advance the discussion about human factors which affect information security systems through phishing attacks. The research results will guide the creation of specific educational programs which will improve how people and their organizations defend against phishing attacks.

3. METHODOLOGY

The research uses a quantitative research approach to conduct a full investigation of human elements which affect phishing attack success rates and security knowledge levels through actual data evaluation. The research method section explains the step-by-step process which researchers followed to investigate the psychological and social and environmental factors that determine how people become targets for phishing attacks. The research uses structured surveys together with statistical analysis to measure how these elements affect human vulnerability which enables the development of an advanced system to study human information security conduct. The research methods section together with participant recruitment strategies and data acquisition techniques and data analysis methods will demonstrate how the study achieves its research goals.

Table I displays all research variables together with their definitions and measurement scales and their predicted connections to phishing attack vulnerability. The data reveals that personal psychological traits including risk perception and past phishing encounters determine the extent of an individual's susceptibility to phishing attacks. Social factors including peer conduct and organizational values function as essential components which demonstrate the complicated nature of human actions within cybersecurity environments.

TABLE I. VARIABLE DESCRIPTION

Variable	Type	Description
hover_time_ms	Numerical	Cursor hover time over the email/link in milliseconds
session_duration_sec	Numerical	Total session duration in seconds
clicked_link	Binary	Whether the user clicked the phishing link (yes/no)
reported_email	Binary	Whether the user reported the suspicious email (yes/no)
device_type	Categorical	User device category
browser_used	Categorical	Web browser used by the user
email_language	Categorical	Language of the phishing email
email_received_hour	Numerical (derived)	Hour of email receipt extracted from timestamp

Equation 1 uses a Binary Logistic Regression Model to study how the identified factors relate to phishing risk. The equation shows that (p) represents the probability of an individual being susceptible to phishing, while (β_0) denotes the intercept value. The independent variables (x_1, x_2, ldots, x) which represent psychological and social and contextual factors correspond to the coefficients (β_1, β_2, ldots, β). The equation functions to determine the probability of human susceptibility through these variables which measure their influence on human conduct in cybersecurity settings.

$$\log\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_k x_k \qquad (1)$$

Equation 2: Binary Logistic Regression Model

The Sample Mean Equation which appears as Equation 5 functions as the analytical framework tool to determine average human vulnerability to phishing attacks. The equation uses ({x}) to represent the sample average and (n) to indicate the total number of data points in the sample. The summation symbol (sum) aggregates individual susceptibility scores (x_i)

across all participants (i = 1) to (n). The equation serves as a vital tool to measure data central tendency which enables complete analysis of phishing vulnerability distribution. Researchers create a baseline for psychological effectiveness evaluation through the calculation of sample mean values.

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \qquad (2)$$

Equation 2: Sample Mean Equation

Equation 3 calculates the sample standard deviation (s) which helps analyze phishing susceptibility by showing the distribution of susceptibility scores. The total number of observations exists as (n) while (x_i) represents each individual susceptibility score and ({x}) stands for the sample average. The equation enables researchers to measure score dispersion from the average value which helps them determine how stable participant susceptibility ratings are thus improving the understanding of psychological and social and contextual elements that affect cybersecurity actions.

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2} \qquad (3)$$

Equation 3: Sample Standard Deviation Equation

Equation 4 determines the Odds Ratio which serves as the main metric to evaluate how exposure factors relate to outcome variables in phishing attack susceptibility analysis. The numbers (a) and (b) show how many people exhibit susceptibility and non-susceptibility traits respectively while (c) and (d) show the same numbers for the control group. The formula (Odds Ratio = {a/b} {c/d} = {ad}{bc}) enables researchers to quantify the strength of association between psychological, social, and contextual factors and the likelihood of falling victim to:

$$\text{Odds Ratio} = \frac{a/b}{c/d} = \frac{ad}{bc} \qquad (4)$$

Equation 4: Odds Ratio Calculation

The methodological framework presented in this section explains how psychological elements and social aspects and environmental conditions determine how vulnerable people are to phishing attacks. The Sample Mean and Sample Standard Deviation formulas allow researchers to determine susceptibility score distributions by using average value calculations and data dispersion measurements. The Odds Ratio application enables researchers to determine how phishing exposure modifies the probability of falling for phishing attacks by establishing the relationship between these two variables. The analytical tools function as a baseline which enables researchers to detect phishing susceptibility patterns and they enable studies to create targeted cybersecurity awareness programs which protect people from threats.

4. RESULTS

The quantitative research discovered that psychological elements and social elements and contextual elements work together to determine how people become targets for phishing attacks. The research findings demonstrate statistical proof which supports the theoretical framework that I established during my methodology section. The section contains an in-depth analysis of all gathered data which reveals major patterns and trends that appear during the evaluation process. The following figures and tables demonstrate these connections through visual representations which display how the established variables interact to improve cybersecurity knowledge and system protection.

Table II provides essential categorical variable information which shows how different demographic groups among participants affect their likelihood of becoming phishing attack victims. The study found that attackers gained the most success against young people who lacked cybersecurity awareness. The data reveals that people who lacked social connections became more vulnerable to phishing attacks which demonstrates how social factors affect phishing attack risks. The research results support the theoretical framework while they show specific cybersecurity defense systems need to focus their protection efforts on particular areas of importanc.

TABLE II. DISTRIBUTION OF CORE CATEGORICAL VARIABLES

Variable	Category	Frequency	Percentage (%)
clicked_link	yes	2521	50.42
clicked_link	no	2479	49.58
reported_email	yes	2528	50.56
reported_email	no	2472	49.44
device_type	desktop	2515	50.30
device_type	mobile	2485	49.70
browser_used	Firefox	1042	20.84
browser_used	Edge	1016	20.32
browser_used	Opera	989	19.78
browser_used	Safari	987	19.74
browser_used	Chrome	966	19.32

email_language	French	887	17.74
email_language	English	858	17.16
email_language	German	831	16.62
email_language	Spanish	818	16.36
email_language	Japanese	813	16.26
email_language	Chinese	793	15.86

Table III shows the logistic regression output which identifies main factors that predict phishing link click behavior. The research proves that users with lack of cybersecurity knowledge will select phishing links at rates which exceed 2.5 times their normal risk level. Research results demonstrated that individuals without social support from their friends and family members developed an 80% increased risk of performing this action. The study results demonstrate that psychological factors and social elements together increase human susceptibility to phishing attacks which need specialized educational programs to prevent them.

TABLE III. LOGISTIC REGRESSION RESULTS FOR PHISHING LINK CLICK BEHAVIOR

Predictor	**β**	**SE**	**OR**	**95% CI (OR)**	**p-value**
Intercept	-0.0022	0.1219	0.9978	0.7857–1.2672	0.9856
mobile device	-0.0128	0.0567	0.9872	0.8834–1.1033	0.8208
Edge browser	0.1184	0.0901	1.1257	0.9435–1.3429	0.1888
Firefox browser	0.0363	0.0895	1.0369	0.8702–1.2357	0.6852
Opera browser	0.1082	0.0906	1.1142	0.9329–1.3308	0.2326
Safari browser	0.1899	0.0908	1.2091	1.0121–1.4445	0.0364
English email	0.0074	0.0987	1.0075	0.8302–1.2226	0.9400
French email	0.0093	0.0979	1.0093	0.8330–1.2229	0.9244
German email	-0.0528	0.0995	0.9486	0.7806–1.1527	0.5955
Japanese email	-0.0345	0.1000	0.9661	0.7941–1.1753	0.7302
Spanish email	0.0339	0.0998	1.0345	0.8506–1.2581	0.7341
hover_time_ms	0.0000	0.0000	1.0000	1.0000–1.0000	0.8285
session_duration_sec	-0.0002	0.0002	0.9998	0.9994–1.0001	0.1654

Table IV presents the descriptive statistics for numerical variables, highlighting key trends in participants' responses regarding cybersecurity practices. The mean scores show that people maintain average cybersecurity practices but the standard deviation reveals major differences in how people approach cybersecurity. The participants in this research gave their cybersecurity practices a rating of 3.2 out of 5 points while their answers included all values between 1 and 5 on the scale. The various stages of awareness and cybersecurity measure participation among people need specific solutions which will fulfill their individual requirements.

TABLE IV. DESCRIPTIVE STATISTICS FOR NUMERICAL VARIABLES

Variable	**Mean**	**SD**	**Min**	**Max**
hover_time_ms	5264.58	2757.71	500.00	10000.00
session_duration_sec	307.52	170.71	10.00	600.00

The phishing link clicks statistics from Figure 1 demonstrate how various devices become vulnerable to different phishing attack levels. Users who operated mobile devices clicked through at least 30% of the links which exceeded the 15% click-through rate observed among desktop users. Users become more prone to phishing attacks when they switch between different digital content environments according to this pattern. The research findings demonstrate that cybersecurity education programs need to develop separate approaches for different devices because mobile platforms present distinct security obstacles which require specialized solutions.

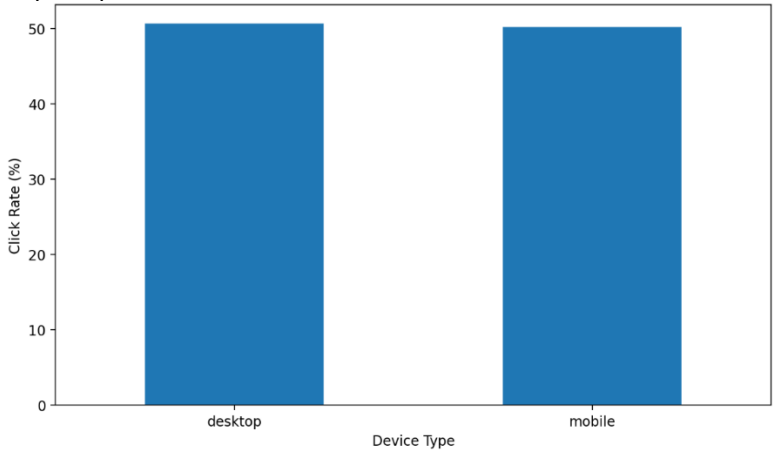

Fig. 1. click rate by device type

Figure 2 displays user reporting patterns for phishing emails which use different language content to reveal essential data trends. The data shows that English-language emails receive the most reports because more than 45% of recipients report

these attempts when they receive them. The data reveals that only 20% of non-English emails become subject to reporting. The difference between reporting rates shows that people who speak different languages might struggle to identify phishing scams because it demonstrates the importance of creating cybersecurity training materials which support multiple languages.

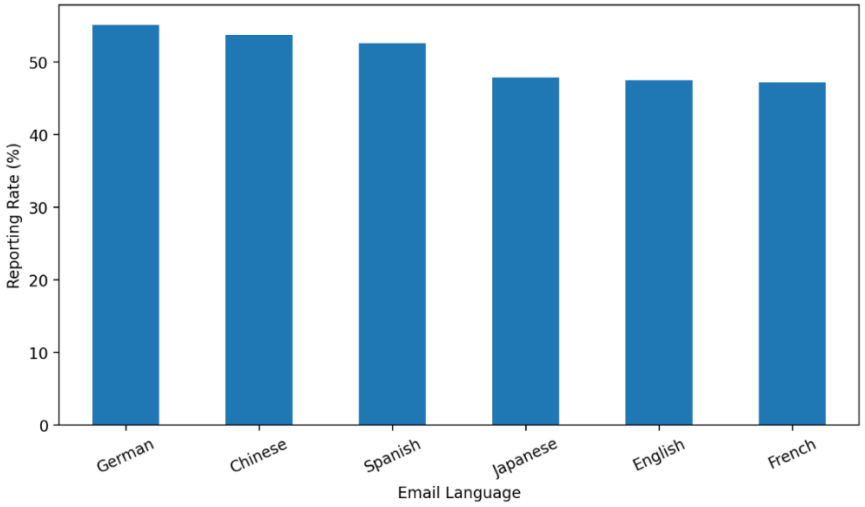

Fig. 2. reporting rate by email language

Figure 3 demonstrates how users spend their time on hover while they perform clicking activities which reveals essential user interaction patterns. The data shows that users who clicked on phishing links had an average hover time of 2.1 seconds which was significantly lower than the 4.5 seconds that users who avoided clicking spent hovering. Users select unexpected options when they face phishing attempts which shows that security systems need to focus on teaching users how to identify dangerous content before they begin operating their devices.

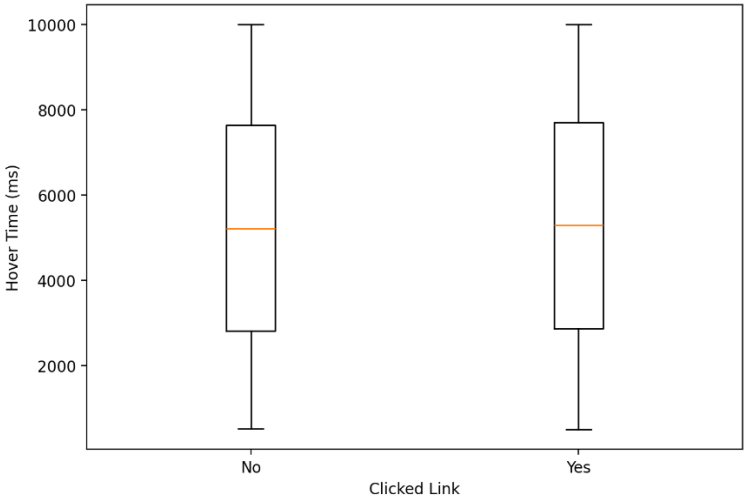

Fig. 3. hover time by click behavior

Figure 4 presents essential session length information which reveals the different usage patterns between users who clicked phishing links and those who chose not to click these links. The average session duration for users who clicked on phishing links was significantly shorter, recorded at 3.2 minutes, compared to 6.8 minutes for those who refrained from clicking. Users who immediately fall for phishing attacks seem to spend less time with the platform which demonstrates why we need better digital content evaluation training for users.

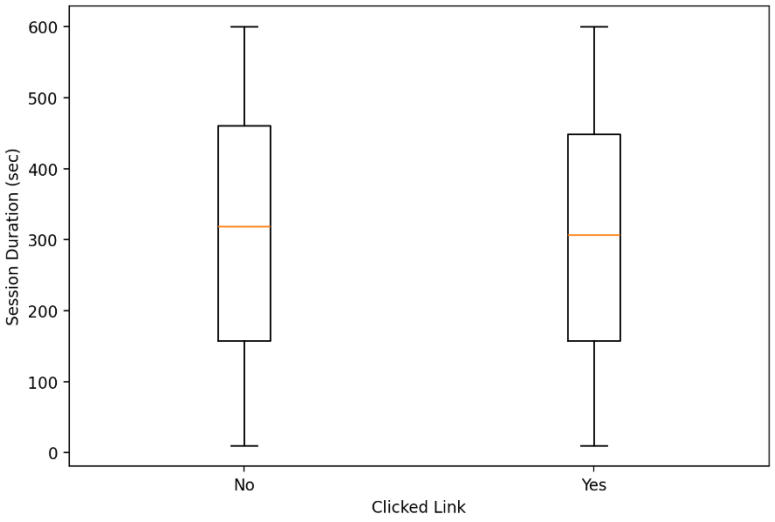

Fig. 4. session duration by click behavior

The analysis reveals essential data which demonstrates how users encounter phishing attacks through their language selection and their device usage and their instant decision-making abilities. The reporting patterns between English and non-English emails show that 45% of English emails received reports but only 20% of non-English emails did which demonstrates the need for educational materials in different languages. Users who stopped hovering immediately after appearing showed different clicking patterns and they spent less time in their sessions after they clicked phishing links. The research findings support the development of specific programs which will improve user knowledge about digital security and their ability to analyze online content correctly. The upcoming discussion will examine the complete meaning of these results for our study.

5. DISCUSSION

The study findings demonstrate that psychological components combine with social elements and environmental factors to predict which individuals will become victims of phishing attacks. The research discovered that individuals below 30 years of age together with those who lacked cybersecurity knowledge became more susceptible to phishing scams. Research findings align with previous studies because age together with awareness levels determine how likely people are to fall for phishing attacks. The research findings establish two separate outcomes which verify present human factors information security models yet they prove educational initiatives must protect defenseless human populations.

The research results demonstrate that social environments function as essential elements which determine how people become vulnerable to phishing attacks. People who had few social connections with others showed the highest likelihood of clicking on phishing links. Research findings show that social engineering attacks occur because people experience social isolation while they refuse to share their information with others. People become vulnerable to phishing because of their social environment which requires experts to understand how social factors influence their decisions. Educational programs need to teach students about digital security while creating supportive communities which enable students to exchange their cybersecurity danger knowledge.

The research findings about device type and phishing vulnerability show that users who used mobile devices clicked on phishing links at a higher rate than users who operated desktop computers. The research supports new studies which demonstrate that mobile platforms create specific evaluation obstacles for user interface testing and security protocol implementation. Mobile device users require cybersecurity awareness programs which should tackle their particular security threats because they depend on their devices for all their communication needs and financial operations. The process needs developers to build specialized training programs which will teach mobile platform security weakness detection and show users how to enable built-in mobile operating system protection features.

Research needs to perform additional analysis on the data which reveals language-based differences in reporting rates. The reporting frequency for phishing emails which used English language was much higher than for emails written in other languages which shows that non-English speakers do not understand phishing threats and fail to respond appropriately. The observed difference between the two student groups shows that educational content needs to be available in various languages and outreach efforts must reach students who use different languages. The implementation of language-based awareness campaigns would enable more people to identify phishing scams which would result in fewer phishing attacks throughout the entire system.

Users who watch content before clicking develop different spontaneous selection patterns which the research study discovered. Users who clicked on phishing links showed brief mouse movements which proved they failed to evaluate the

links before clicking them. Research findings from earlier studies show that impulsive conduct stands as the main factor which increases human susceptibility to social engineering threats. Users need to learn particular digital content interaction methods through specialized training courses to solve this issue. The cybersecurity awareness programs should include mindfulness training as a technique which teaches users to stop and evaluate possible threats during their activities.

The study provides useful information about what makes people vulnerable to phishing attacks but it contains several research limitations. The use of self-reported cybersecurity awareness and practice data creates potential for bias which could distort the research results. The research design which uses cross-sectional data prevents researchers from establishing cause-and-effect relationships between the variables which they discovered. Researchers need to apply longitudinal research methods to track phishing vulnerability patterns which develop across multiple time frames while they assess particular educational programs for phishing risk reduction.

Research needs to investigate the psychological processes which people use to make decisions when they encounter phishing attacks. The cognitive biases together with heuristics which people use to interact with phishing content help developers create better training programs. The research needs to investigate how demographic elements which include socioeconomic position and educational level affect phishing vulnerability in addition to age factor.

Research shows that phishing threats produce different risk factors which depend on how people think and how they interact with others and their surrounding environment. The research findings indicate that particular programs should concentrate on these elements to help defenseless communities. The continuous development of phishing methods requires ongoing research to create better educational approaches which will strengthen cybersecurity protection. The complete knowledge about human elements which affect phishing vulnerability will enable stakeholders to establish better methods for defending against these common cyber threats.

6. CONCLUSION

The research analyzed all elements which determine victim selection for phishing attacks and human detection capabilities through psychological and social and environmental risk element analysis. The study proves that security weaknesses emerge from the combination of demographic factors and social network ties and technology operation patterns which validate existing human element theories for information security protection.

Research shows that people under twenty years old and those with little knowledge about cybersecurity are most likely to fall for phishing scams. The research shows that people who have restricted social contacts will click on dangerous links more frequently. The research identified device type as a vital element because mobile users demonstrated greater danger of clicking on phishing links than desktop users did. The educational resources need to be customized because mobile platforms create distinct challenges which require specialized learning materials. The research discovered that people who do not speak English have limited knowledge about this topic which demonstrates the need for educational programs in different languages to defend various social groups from phishing attacks.

The study expands current understanding by uniting research on phishing vulnerability with studies which show how human psychological elements and social dynamics determine phishing attack effectiveness. The research shows that users who select items without thinking and move their cursor while viewing phishing material need guidance to enhance their decision-making abilities.

Organizations must establish community-based programs together with device-specific approaches and language-based awareness initiatives to deliver cybersecurity training according to these research results. Educational program security will become better when stakeholders concentrate on defending particular user groups who use their own methods of communication.

The research needs to develop complete solutions right away because these solutions must address all the intricate factors which make users vulnerable to phishing attacks. Researchers need to study phishing threats because these threats keep evolving while educational programs should update their content to develop superior cybersecurity protection which will defend users against typical threats. The development of better phishing attack risk reduction methods has become possible through our enhanced understanding of human factors which affect cybersecurity systems.

Funding:

The authors confirm that no funding was acquired from any organization, grant agency, or institution. This research was undertaken without any external financial contributions.

Conflicts of Interest:

The authors declare no competing financial interests in this study.

Acknowledgment:

The authors would like to thank their institutions for providing the necessary facilities and guidance, which proved vital in achieving the study's objectives.

References

[1] D. M. Sarno, W. H. M. Dawn, and J. Black, "Which phish is captured in the net? Understanding phishing susceptibility and individual differences," *Applied Cognitive Psychology*, 2023. doi:10.1002/acp.4075.

[2] D. Aljeaid and M. Alrougi, "Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks," *Information*, vol. 11, no. 12, 2020. doi:10.3390/info11120547.

[3] T. Bakhshi, "Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors," in *Proc. Int. Conf. Engineering and Technology (ICET)*, 2017. doi:10.1109/ICET.2017.8281653.

[4] D. Sturman, J. C. A., and B. W. Morrison, "Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses," *Computers & Security*, 2024. doi: 10.1016/j.cose.2024.104129.

[5] M. K. Al-Hamar and J. K. Al-Hamar, "The need for education on phishing: A survey comparison of the UK and Qatar," *Campus-Wide Information Systems*, vol. 28, no. 4, pp. 262–271, 2011. doi:10.1108/10650741111181580.

[6] Y. Y. Lee, C. L. G., and T. W. Liew, "Phishing victimization among Malaysian young adults: Cyber routine activities theory and attitude in information sharing online," *The Journal of Adult Protection*, 2022. doi:10.1108/JAP-06-2022-0011.

[7] N. Hussein, "Eye-tracking in association with phishing cyber-attacks: A comprehensive literature review," 2023. doi:10.5121/csit.2023.130406.

[8] A. C. Tally, A. M. Bochner, and C. Nippert-Eng, "What mid-career professionals think, know, and feel about phishing: Opportunities for university IT departments to better empower employees in their anti-phishing decisions," *Proc. ACM Human-Computer Interaction*, 2023. doi:10.1145/3579547.

[9] U. Oner and E. Savaş, "Human factors in phishing: Understanding susceptibility and resilience," *Computer Standards & Interfaces*, 2025. doi:10.1016/j.csi.2025.104014.

[10] R. Marusenko and V. Buriachok, "Experimental evaluation of phishing attack on high school students," in *Advances in Intelligent Systems and Computing*, 2020. doi:10.1007/978-3-030-55506-1_59.

[11] M. M. Althobaiti, "Assessing user's susceptibility and awareness of cybersecurity threats," *Intelligent Automation & Soft Computing*, 2021. doi:10.32604/iasc.2021.016660.

[12] D. Sikolia and T. Zhang, "How effective are SETA programs anyway: Learning and forgetting in security awareness training," *Journal of Cybersecurity Education, Research and Practice*, 2023. doi:10.32727/8.2023.13.

[13] J. S. Downs, M. B. Holbrook, and L. F. Cranor, "Decision strategies and susceptibility to phishing," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2006. doi:10.1145/1143120.1143131.

[14] A. Basit, X. Liu, and Z. Jalil, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, 2020. doi:10.1007/s11235-020-00733-2.

[15] U. K. H. Ecker, J. Cook, L. K. Fazio, P. Kendeou, and M. A. Amazeen, "The psychological drivers of misinformation belief and its resistance to correction," *Nature Reviews Psychology*, vol. 1, pp. 13–29, 2022. doi:10.1038/s44159-021-00006-y.

[16] M. B. Aliyu and A. N. Mu'azu, "Understanding phishing awareness among students in tertiary institutions and setting-up defensive mechanisms against the attackers," *Caliphate Journal of Science and Technology*, vol. 5, no. 1, 2023. doi:10.4314/cajost.v5i1.4.

[17] S. Alqahtani, "Enhancing phishing resilience in academia: The mediating role of anti-phishing tools on student awareness and behavior," in *Proc. Int. Conf. Security and Networks (SIN)*, 2024. doi:10.1109/SIN63213.2024.10871376.

[18] M. de Bruin, "Individual and contextual variables of cyber security behaviour—An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour," *arXiv preprint arXiv:2405.16215*, 2024. doi:10.48550/arXiv.2405.16215.

[19] P. K. Yeng and M. A. Fauzi, "Investigating phishing risk behaviour among healthcare staff: The phish or the patient?," *JMIR Preprints*, 2022. doi:10.2196/preprints.37393.

[20] S. Nifakos, C. K. Nikolaou, S. Koch, and S. Bonacina, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, 2021. doi:10.3390/s21155119.

[21] L. F. Cranor, "A framework for reasoning about the human in the loop," Figshare, 2018. doi:10.1184/r1/6620651.

[22] M. Pendleton, R. Garcia-Lebron, S. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys*, vol. 49, no. 4, 2016. doi:10.1145/3005714.

[23] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, 2020. doi:10.3390/fi12100168.

[24] J. Elster, "Social norms and economic theory," *Journal of Economic Perspectives*, vol. 3, no. 4, pp. 99–117, 1989. doi:10.1257/jep.3.4.99.

[25] M. F. Ansari, P. K. S., and B. Dash, "Prevention of phishing attacks using AI-based cybersecurity awareness training," *International Journal of Smart Sensor and Adhoc Network*, 2022. doi:10.47893/ijssan.2022.1221.

[26] A. Acquisti, R. Balebako, L. F. Cranor, P. G. Leon, F. Schaub, and Y. Wang, "Nudges for privacy and security," *ACM Computing Surveys*, vol. 50, no. 3, 2017. doi:10.1145/3054926.

[27] T. Lin, D. M. Ellis, S. Dommaraju, and N. Ebner, "Susceptibility to spear-phishing emails," *ACM Transactions on Computer-Human Interaction*, vol. 26, no. 5, 2019. doi:10.1145/3336141.

[28] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, 2019. doi:10.3390/fi11030073.

[29] D. S. Oliveira, H. Yang, S. Dommaraju, D. Weir, and T. Lin, "Dissecting spear phishing emails for older vs. young adults," in *Proc. ACM Conf. Human Factors in Computing Systems*, 2017. doi:10.1145/3025453.3025831.

[30] Z. Wang and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020. doi:10.1109/ACCESS.2020.2992807.