International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Phishing Victimization Risk Factors: A Lifestyle-Routine Activities Theory Analysis of Scam Types and Demographic Influences

Rhem Rick N. Corpuz[1], Carmina T. Del Rosario[2], Gerviene C. Lugtu[3], Angeline D. Macasio[4], Antonio Jose D. Basa[5]

[1,2,3,4,5]Author, Angeles University Foundation

Abstract:
Phishing scams have become a significant and growing threat in the digital age, with cybercriminals increasingly targeting individuals through deceptive online tactics. These scams exploit personal information and online behaviors, making it essential to understand the factors that contribute to phishing victimization. This study, conducted in Angeles City with 140 respondents, used a descriptive correlational research design to explore the relationships between phishing victimization and exposure to phishing attempts, online behaviors, and the lack of protective measures. The study also examined the influence of different types of phishing scams (email, SMS) and sociodemographic characteristics, including age, sex, and household income. The results revealed that individuals engaging in online activities such as e-commerce and banking were more vulnerable to phishing scams. Additionally, those with more personal information or those involved in frequent online financial transactions were at higher risk. The study found that individuals using cybersecurity practices like security software and participating in phishing awareness programs were less prone to being targeted by phishing attacks. Furthermore, the data highlighted that exposure to one type of phishing scam increased the likelihood of encountering other types. Overall, the study highlights the significance of proactive cybersecurity measures and public awareness in mitigating phishing risks.

Keywords: Phishing; Phishing Attacks; Routine Activities Theory; Risk Factors; Exposure; Target Attractiveness; Lack of Capable Guardianship

Introduction

Phishing attacks have become one of the most pervasive and damaging forms of cybercrime in the digital age, exploiting individuals' trust and technological vulnerabilities to steal sensitive information. As digital A**s** activities like online shopping, entertainment, and banking increased, so did the opportunities for cybercriminals to target individuals. unsuspecting users, often leading to significant financial and personal losses. The rise in online fraud, including phishing scams, highlighted the increasing importance of understanding the key factors influencing phishing victimization to develop effective prevention strategies. This study aimed to examine the interaction of different risk factors.—such as online exposure, target attractiveness, guardianship, and demographic characteristics—in determining susceptibility to phishing. By examining how these factors contributed to phishing

victimization, the study aimed to provide insights into how individuals could better protect themselves in an increasingly interconnected world.

Research indicates that phishing scams, where attackers impersonate legitimate institutions to steal sensitive information, have become a significant cybercrime (Cross, 2019). The Philippines, for example, ranked fifth in Southeast Asia for phishing incidents in 2022, with over 4.5 million cases reported (Philstar, 2022). A 2023 Statista survey found that 50% of respondents were targeted by phishing attacks, while 42% experienced smishing (Balita, 2024). Younger individuals, in particular, were found to be more vulnerable due to their higher online activity (Berre et al., 2022), while experience with internet banking also increased the chances of becoming a victim to phishing (Manoharan et al., 2022). Lack of awareness was another contributing factor, with individuals knowledgeable about phishing being 78% less likely to fall prey (De Liema et al., 2023). Research by Koning et al. (2023) highlighted the higher susceptibility of both younger and older populations due to varying levels of digital literacy and trust in online interactions.

This study aimed to investigate the relationship between phishing victimization and risk factors like exposure to phishing attempts, target attractiveness, guardianship, and sociodemographic factors. Increased exposure to phishing attempts, higher digital engagement, and the availability of personal data heightened the risk of victimization (Bossler & Berenblum, 2018; Chanti & Chithralekha, 2022). A lack of effective cybersecurity measures and low awareness further contributed to vulnerability (Cross, 2019). Moreover, sophisticated phishing scams and demographic factors such as age, sex, and household income played a role in moderating susceptibility to phishing (Chanti & Chithralekha, 2022; Berre et al., 2022). Ultimately, the study sought to enhance the understanding of these risk factors in order to improve phishing prevention strategies and inform more effective cybersecurity practices.

This study investigated the growing threat of phishing scams in the Philippines, emphasizing how increased online activity and insufficient cybersecurity measures have made individuals more vulnerable to these attacks (Lee & Cua, 2023). It analyzed how demographic factors like age, income, education level, and internet usage influenced individuals' susceptibility to phishing (Gomez & Ramos, 2021). This demographic analysis aimed to uncover victimization patterns and identify groups most at risk. The research also assessed the effectiveness of current protective measures, including government policies, cybersecurity protocols, and public awareness campaigns (Santos & Mendoza, 2022). The study identified gaps in these efforts and proposed targeted strategies to improve digital security and reduce phishing attacks. Ultimately, the goal was to develop better interventions to enhance digital resilience and security, especially in Southeast Asia, where cybercrime is a growing threat (Lee & Cua, 2023).

General Objective:

The study highlights key vulnerabilities such as exposure to phishing attempts and target attractiveness, offering valuable guidance for enhancing prevention strategies. Policymakers, organizations, and law enforcement can use these insights to strengthen defenses, raise awareness, and develop more effective cybersecurity frameworks to combat phishing and improve resilience.

Specific Objectives:

1. To assess the relationship between exposure to potential phishing attempts and the likelihood of victimization.
2. To evaluate the impact of target attractiveness (e.g., availability of personal information, frequency

of online financial transactions) on the probability of becoming a victim of phishing scams.
3. To examine the effect of lacking capable guardianship (e.g., weak cybersecurity measures, lack of awareness) on the likelihood of phishing scam victimization.
4. To analyze how different types of phishing scams influence the rates of victimization, with a focus on the complexity and sophistication of the scams.
5. To investigate the moderating role of demographic factors (age, sex, and household income) in the relationship between exposure to phishing attempts and the likelihood of victimization.

Scope of the Study

The study focused on participants aged 18 to 60 years from Angeles City, a rapidly growing area both economically and digitally, which made it particularly vulnerable to phishing scams. It aimed to investigate factors contributing to phishing victimization, such as the use of financial banking services, the availability of personal information online, online activity, shopping frequency, awareness, and password-changing habits. However, the study did not explore factors like the specific types of apps used, devices involved, or other similar details, choosing instead to concentrate on the most relevant aspects that directly contributed to phishing victimization. This focused approach allowed for a clearer and more manageable investigation of the key determinants in phishing scams.

Significance or Importance

This study explored the factors leading to phishing victimization, with an emphasis on exposure to phishing attempts, the attractiveness of targets, and the lack of effective cybersecurity measures. It also examined the role of phishing scam types and demographic factors—such as age, sex, and household income—in moderating risks. The findings provided insights into vulnerabilities exploited by phishers, identifying high-risk individuals and groups. These insights informed tailored prevention strategies and educational initiatives, particularly for vulnerable demographics, while contributing to the development of more adaptive cybersecurity measures.

Theoretical Framework

Cohen and Felson (1979), alongside Lynch (2020), introduced Routine Activity Theory (RAT) in the 1970s to explain the paradox of persistently high urban violent crime rates despite improvements in conditions previously thought to reduce crime. Their theory emphasized the role of everyday lifestyle choices in creating opportunities for both criminal activity and victimization. According to RAT, changes in routine activities can align the three essential components necessary for crime: suitable targets, motivated offenders, and lack of capable guardianship. When these elements converge in time and space, victimization becomes more likely.

Subsequent studies applying RAT have shown that victim-offender proximity and engagement in deviant activities increase the likelihood of various forms of online victimization (Bossler & Holt, 2010; Dodel & Mesch, 2017; Leukfeldt & Yar, 2016; Holt et al., 2020; Pratt et al., 2010; Reyns & Henson, 2015; Reyns et al., 2011).

The Lifestyle-Routine Activities Theory (LRAT) further refines RAT by suggesting that daily routines create criminal opportunities. It posits that behaviors, particularly those that heighten exposure to potential offenders, increase the chances of becoming a target (Holt et al., 2020; Miethe & Meier, 1990). A key feature of LRAT is exposure to offenders, which refers to how physically accessible individuals

or objects are to criminals (Akdemir & Lawless, 2020; Cohen et al., 1981). Additionally, target suitability encompasses factors that make individuals or objects vulnerable, including specific attributes that appeal to offenders (Akdemir & Lawless, 2020; Finkelhor & Asdigian, 1996). Lastly, the lack of capable guardianship, such as a person or system that can prevent criminal activity, significantly raises the risk of victimization. Guardianship reduces threats and deters offenders by making targets less appealing (Akdemir & Lawless, 2020; Cohen et al., 1981).

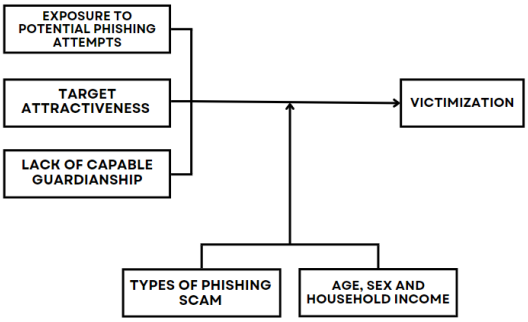
This study applied the LRAT framework to examine factors contributing to phishing victimization. It investigated (1) exposure to potential phishing attempts; (2) target attractiveness; and (3) lack of capable guardianship. Additionally, the study assessed (4) types of phishing scams and (5) demographic factors such as age, sex, and household income, as moderating factors influencing exposure to phishing attempts.

Conceptual Framework

The study aimed to explore factors contributing to phishing victimization by examining the relationships between key independent variables and phishing victimization. It focused on three main variables: exposure to phishing attempts, target attractiveness, and lack of capable guardianship. Additionally, the study considered the moderating effects of phishing scam types and demographic factors (age, sex, and household income). Hypotheses were tested, including: (1) increased exposure to phishing attempts would correlate with higher victimization risk (H1); (2) individuals with more attractive targets (e.g., abundant personal info, frequent online transactions) would be more likely to fall victim (H2); (3) **a** lack of effective guardianship (e.g., weak cybersecurity measures) would increase vulnerability (H3); (4) sophisticated phishing scams would result in higher victimization rates (H4); and (5) demographic factors would moderate the exposure-victimization relationship (H5). The study aimed to offer a thorough understanding of how exposure, vulnerabilities, and scam sophistication interact to shape phishing victimization.

Paradigm of the Study

Factors Influencing Victimization in Phishing Scams



Methods

Study Design

The study employed a descriptive correlational research design, which allowed for the examination of relationships between variables quantitatively. This design was chosen because it enabled the investigation of the relationships between phishing victimization and several key factors such as exposure to potential phishing attempts, target attractiveness, and lack of capable guardianship. The

descriptive aspect detailed the prevalence of phishing victimization among the sample, while the correlational aspect explored the links between phishing victimization and independent variables, including demographic factors. The design focused on statistical analysis to identify patterns and relationships among the variables, without incorporating qualitative analysis.

Locale of the Study

The study was conducted in Angeles City, covering all 33 barangays (neighborhoods) within the city. With a population of 462,928 residents, as reported by PhilAtlas (2020), Angeles City provided a representative sample for examining phishing victimization and its associated factors. The choice of this city allowed the study to capture a broad and diverse demographic, reflecting the varied characteristics and behaviors of its residents. By focusing on the entire population, the study aimed to generate findings that were relevant and generalizable to the community, thereby enhancing the accuracy of its analysis on the impact of phishing scams.

Study Participants

The participants of the study included residents of Angeles City aged 18 to 60 years. This age range ensured the inclusion of adult individuals who were likely to engage in online activities and were relevant to the investigation of phishing scam victimization. By encompassing a wide demographic, the study sought to identify the prevalence and patterns of phishing victimization across different segments of the population. This inclusive approach allowed for a thorough assessment of how phishing scams impacted the community, providing valuable insights into the broader issue of online security and fraud in Angeles City.

Sample Size and Sampling Method

The study included 140 respondents, determined using the G-Power Sample Size Calculator, based on a population of 462,928 residents in Angeles City. A 5% margin of error and a 95% confidence level were applied for statistical significance. The sample was selected using cluster random sampling, where the population was divided into subgroups (barangays). The distribution of respondents varied, with Balibago having the largest share (13 respondents, 9.29%), and smaller barangays like Agapito del Rosario, Lourdes Sur, and San Nicolas contributing only one respondent each (0.71%). This uneven distribution, common in cluster sampling, could influence the statistical analysis, potentially causing overrepresentation or underrepresentation of certain clusters. Future studies could address this through weighting methods or more balanced sampling designs, although the random selection process ensured an unbiased, representative sample.

Inclusion and Exclusion Criteria

Inclusion Criteria

a. Participants were required to be residents of Angeles City, having lived there for at least six months to ensure familiarity with the local context.
b. Participants were required to be between 18 and 60 years old to capture a broad demographic range of adults likely to engage in online activities.
c. Participants were required to possess a mobile phone and maintain an active phone number and email address.

Exclusion Criteria

a. Participants who had experienced victimization within six months prior to the study were excluded. This was essential to prevent triggering the effects of victimization, which could pose risks to their well-being and lead to potential post-traumatic stress, making it unsuitable for a healthy study environment.
b. Participants using company emails were also excluded, as the primary focus of this thesis was to engage individuals who utilized their personal email accounts.

Data Collection Procedures

The study began with the development of a structured survey, which underwent a rigorous validation process to ensure its accuracy and relevance. The validation included face validity, where experts reviewed the survey items for relevance to the study's objectives, and content validity, where a thorough evaluation was conducted to ensure the survey comprehensively covered all key dimensions of the topic. The survey aimed to assess critical variables such as exposure to phishing attempts, target attractiveness, lack of capable guardianship, and various demographic factors. To analyze the data, the study employed statistical techniques like bivariate correlation to identify significant relationships between these variables and phishing victimization. The study used a descriptive correlational design to explore how independent variables, such as exposure to phishing scams and target attractiveness, influence phishing victimization. Additionally, the research examined the moderating effects of demographic factors like age, sex, household income, and the types of phishing scams encountered.

Prior to data collection, the survey underwent pilot testing to verify its reliability and validity.. The pilot testing aimed to identify any issues with the survey design, wording, or structure, and to confirm that the survey effectively measured the intended variables. Following pilot testing, the study initiated the process of securing informed consent from participants. The consent forms were stored digitally in a secure, password-protected folder on Google Drive, ensuring that only authorized research team members had access. To protect participant privacy, sensitive data was encrypted, and each participant was assigned a unique identifier. Data was collected through validated surveys, administered in person across all 33 barangays of Angeles City. Participants were informed of the study's purpose and their right to refuse without consequences. A total of 140 questionnaires were distributed in sealed envelopes to ensure confidentiality and minimize discomfort.

The collected data were recorded on a dedicated data sheet, accessible only to the research team and adviser, ensuring secure handling and storage. The data were then coded using Google Docs, with restricted access solely granted to the research team. The information was stored on Google Drive, under strict oversight, to maintain confidentiality and data integrity. Access control measures were rigorously enforced, with only designated researchers able to access informed consent forms. Physical copies of consent forms were securely stored in a locked filing cabinet, ensuring authorized access only. All procedures followed ethical guidelines and regulations to protect participant rights and privacy, and participants were fully informed about the security of their consent forms and data privacy.

The findings were analyzed to provide a comprehensive understanding of phishing victimization in Angeles City. The quantitative results identified significant factors linked to phishing risk, offering valuable insights for developing evidence-based recommendations aimed at enhancing phishing prevention strategies within the community.

Research Instruments

The questionnaire used in the study was carefully designed to explore participants' experiences and perceptions regarding phishing victimization. It focused on several key factors, including exposure to phishing attempts, target attractiveness, lack of capable guardianship, and the types of phishing scams encountered by participants. The questionnaire featured a combination of demographic questions and a 4-point Likert scale format for quantitative analysis.

The first section gathered demographic information such as age, sex, and household income, which was essential for understanding the sample's characteristics and for analyzing how these factors might influence vulnerability to phishing scams. Additionally, an eligibility criteria section was included to ensure participants met the study's inclusion requirements, such as owning a mobile phone, having an active phone number and email address, and being regular internet users.

The second section of the survey focused on participants' experiences and perceptions of phishing victimization. It used the 4-Likert scale with a range from "Strongly Agree" to "Strongly Disagree," to assess factors such as exposure to phishing attempts, target attractiveness, lack of capable guardianship, and the different types of phishing scams participants had encountered. Each category contained five questions to better understand how these factors relate to the likelihood of falling victim to phishing.

The Exposure to Potential Phishing Attempts section assessed how often participants engaged in behaviors that could increase their vulnerability, such as online shopping, using online banking, receiving unsolicited emails, and clicking on unfamiliar links. The Target Attractiveness section evaluated whether certain behaviors, like frequent online financial transactions or sharing detailed personal information, made individuals more attractive to phishing attackers. The Lack of Capable Guardianship section explored participants' awareness of cybersecurity practices, such as using security software, understanding phishing tactics, and adhering to best online security practices. The Phishing Victimization section asked participants directly whether they had ever been victims of phishing attacks, providing a clear measure of the study's dependent variable.

Lastly, the Types of Phishing Scams section identified the different phishing tactics participants had encountered, including email phishing, smishing, vishing, pharming, pop-up phishing, spear phishing, and angler phishing. This section also used a Likert scale to measure the frequency with which participants had experienced these scams, offering insights into the variety and sophistication of phishing tactics impacting victimization rates.

The questionnaire collected data on factors influencing phishing victimization, such as demographics, exposure, target attractiveness, cybersecurity awareness, and scam types. This approach identified key relationships to guide effective prevention strategies.

Validity

The face validity of the questionnaire was assessed by experts to ensure the questions were clear, understandable, and aligned with the study's constructs, such as exposure to phishing attempts and target attractiveness. Content validity was ensured through a thorough evaluation by experts from law enforcement and psychology, ensuring the questions comprehensively covered relevant aspects of phishing while being sensitive to participants' experiences and avoiding distress.

Reliability

Reliability testing of the questionnaire was performed using Cronbach's Alpha, resulting in an overall

reliability score of 0.87, indicating high internal consistency across the sections. Pilot testing was also conducted to refine the survey, with feedback from a small, representative sample helping to identify areas for improvement; adjustments were made based on both quantitative and qualitative data, ensuring the final survey instrument was clear, comprehensive, and effective for the main study.

Ethical Considerations

The study implemented several ethical safeguards to ensure the rights and welfare of participants were safeguarded throughout. Before participation, all respondents received an informed consent form that clearly explained the study's purpose, procedures, potential risks, and benefits. The form reassured participants about data security and their right to withdraw from the study at any time without consequences. Additionally, an email address was provided for further inquiries, emphasizing transparency and participant support.

Confidentiality was a primary concern because of the sensitive nature of the data gathered. To protect privacy, completed questionnaires were immediately placed in labeled envelopes and collected by the researchers. These physical forms were securely stored before being transferred to an encrypted electronic storage system, accessible only to authorized research team members.

The researchers also took steps to minimize potential risks by ensuring data collection occurred in comfortable environments. Factors such as temperature and participant comfort were carefully considered.

Ethical considerations also extended to the communication of the study's benefits. Participants were informed that their involvement would contribute valuable insights that could enhance policy development and law enforcement strategies related to cybersecurity, especially in combating phishing scams. The findings were expected to inform the creation of more effective anti-phishing strategies, including updated regulations and targeted interventions. By participating, respondents directly contributed to improving policies and practices aimed at reducing the threat of phishing scams, which often exploited vulnerabilities through tailored tactics targeting specific groups.

Statistical Analysis of Data

Given the use of a 4-point Likert scale and a sample size of 140 respondents, the statistical methods selected were designed to account for the ordinal nature of the data. The Likert scale, which measures responses ranging from "strongly disagree" to "strongly agree," generated ordinal data, necessitating statistical tests that respected its non-interval nature while allowing for meaningful analysis of relationships between variables.

To assess the relationship between exposure to phishing attempts and the likelihood of victimization, bivariate correlation was employed. This method was ideal for exploring the association between ordinal independent variables, such as levels of exposure measured on the 4-point scale, and the binary outcome of victimization (victim vs. non-victim). Similarly, the effect of target attractiveness, including factors such as the availability of personal information and frequency of online financial transactions, was analyzed in the same manner to determine how these elements influenced the likelihood of phishing victimization. The analysis of lacking capable guardianship, such as weak cybersecurity measures and low levels of awareness, also utilized bivariate correlation to model the relationship between ordinal variables like cybersecurity awareness and behaviors and phishing victimization. This approach helped identify how deficiencies in protective measures increased the risk of falling victim to phishing attempts.

In evaluating how different types of phishing scams influenced victimization rates, with a focus on scam complexity and sophistication, bivariate correlation was used to evaluate the relationship between scam types and victimization outcomes. Additionally, bivariate correlation was used to examine the moderating role of demographic factors, such as age, sex, and household income, in the relationship between exposure to phishing attempts and victimization likelihood.

By using bivariate correlation consistently across all variables, the study was able to assess the intensity and nature of the connections between key factors influencing phishing victimization. This approach allowed for a comprehensive understanding of how exposure, target attractiveness, lack of guardianship, scam type, and demographic factors interact to influence the likelihood of falling victim to phishing scams.

Results

Exposure to Potential Phishing Attempts

The data indicates general agreement among respondents regarding their exposure to potential phishing attempts through online activities, with an overall mean of 2.64. The statement with the highest mean (2.69), "I often click on links or download attachments from unfamiliar sources while online," reflects the most agreement, suggesting that respondents are more likely to engage in this behavior. The lowest mean (2.59), "I frequently engage in online activities that expose me to potential phishing attempts," still falls within the agreement category, but to a lesser degree.

Standard deviations range from 0.98 to 1.05, showing some variability in responses. The highest standard deviation (1.05) is observed for the statement about clicking links or downloading attachments, indicating greater variation in responses regarding unfamiliar sources, while the lowest (0.98) is associated with online activities exposure.

Table 1. Exposure to Potential Phishing Attempts of the Respondents

	N	Mean	Verbal Interpretation	Std. Deviation	Variance
Online Exposure	140	2.59	Agree	0.98	0.96
E-commerce Exposure	140	2.61	Agree	1.03	1.06
Banking Vulnerability	140	2.67	Agree	1.01	1.01
Message Exposure	140	2.63	Agree	1.04	1.08
Clicking Risk	140	2.69	Agree	1.05	1.09
Average	140	2.64	Agree	1.02	1.04

Target Attractiveness

The data shows that respondents generally report moderate engagement with behaviors that increase their exposure to phishing attempts, with an overall mean of 2.78, indicating agreement with statements related to online activities and vulnerability. The highest mean (3.59), linked to using the same passwords for multiple accounts, suggests strong agreement with this risky behavior. The lowest mean (2.29) reflects a lesser agreement with frequently engaging in activities that expose respondents to phishing.

Standard deviations range from 0.96 to 1.06, indicating moderate variability in responses. The highest standard deviation (1.06) is associated with entering personal information on insecure websites, showing greater variability, while the lowest standard deviation (0.96) is found in conducting online financial transactions, indicating more consistent responses.

Table 2. Target Attractiveness of the Respondents

	N	Mean	Verbal Interpretation	Std. Deviation	Variance
Exposure to Phishing	140	2.29	Agree	1.02	1.04
Financial Transactions	140	2.74	Agree	0.96	0.93
Profile Details	140	2.64	Agree	1.05	1.11
Unsecure Sites	140	2.66	Agree	1.06	1.12
Reused Passwords	140	3.59	Strongly Agree	1.00	1.01
Average	140	2.78	Agree	1.02	1.04

Lack of Capable Guardianship

The data reveals that respondents generally report low engagement with practices designed to protect against phishing attempts, with an overall mean of 1.73, indicating a tendency toward disagreement with security practices. The highest mean (2.59) corresponds to awareness of phishing scams, showing moderate agreement, while the lowest mean (1.43) reflects a strong disagreement with using security software to protect against phishing. Standard deviations range from 0.76 to 1.05, indicating some variability in responses. The statement about awareness of phishing scams had the highest standard deviation (1.05), suggesting more varied responses, while the statement about following best practices for online security showed the lowest standard deviation (0.77), indicating more consistency in responses.

Table 3. Lack of Capable Guardianship of the Respondents

	N	Mean	Verbal Interpretation	Std. Deviation	Variance
Phishing Protection	140	1.43	Disagree	.86	.74
Awareness Protection	140	2.59	Agree	1.05	1.11
Password Security	140	1.48	Disagree	.77	.60
Ongoing Phishing Education	140	1.56	Disagree	.76	.58
Software Updates	140	1.61	Disagree	.84	.70
Average	140	1.73	Disagree	.86	.74

Phishing Victimization

The data shows that respondents generally report low levels of phishing victimization. The overall mean is 1.04, indicating strong disagreement with the statement "I have been a victim of phishing attempts." The standard deviation is 1.04, suggesting considerable variability in responses, with some respondents agreeing while most disagree with having been targeted by phishing attempts.

Table 4. Phishing Victimization of the Respondents

	N	Mean	Verbal Interpretation	Std. Deviation	Variance
Phishing Victimization	140	1.04	Disagree	1.04	1.08
Average	140	1.04	Disagree	1.04	1.08

Types of Phishing Scams

The data shows that respondents generally agree with encountering phishing attempts across various channels, with an overall mean score of 2.79. The highest mean (3.45) was reported for phishing attempts received via SMS or text messages, indicating strong agreement. Conversely, the lowest mean (2.02) was for being targeted by highly personalized phishing attempts, reflecting more moderate agreement. Standard deviations ranged from 0.76 to 1.06, suggesting variability in responses. The highest variability (1.06) was seen in phishing attempts through fake websites, while the lowest (0.76) was associated with SMS phishing attempts, indicating more consistent responses.

Table 5. Types of Phishing Scams Encountered by the Respondents

	N	Mean	Verbal Interpretation	Std. Deviation	Variance
Email Phishing	140	3.39	Strongly Agree	.94	.89
Smishing	140	3.45	Strongly Agree	.76	.58
Vishing	140	3.43	Strongly Agree	.88	.78
Pharming	140	3.02	Strongly Agree	1.06	1.11
Pop-up Phishing	140	2.17	Agree	.92	.85
Spear Phishing	140	2.02	Agree	.87	.75
Angler Phishing	140	2.09	Agree	.89	.80
Average	140	2.79	Agree	.90	.82

Correlations of the Variables

Increased exposure to phishing attempts is linked to a higher risk of victimization (H1).

The correlation data reveals significant relationships between phishing victimization and online behaviors such as e-commerce exposure ($r = 0.581$), banking vulnerability ($r = 0.544$), and message exposure ($r = 0.582$). The strongest correlation was found between banking vulnerability and risky online behaviors ($r = 0.861$). These results underscore the need for improved cybersecurity measures.

The findings support the hypothesis that increased exposure to phishing attempts correlates with higher victimization risk (H1). Significant positive correlations were observed between phishing victimization and e-commerce exposure ($r = 0.581$, $p < 0.01$), banking vulnerability ($r = 0.544$, $p < 0.01$), and message exposure ($r = 0.582$, $p < 0.01$), aligning with previous studies by Kirwan et al. (2018) and Berre et al. (2022) highlighting the vulnerability of highly active internet users.

Table 6. Increased exposure to phishing attempts is linked to a higher risk of victimization

Variable	Phishing Victimization	Online Exposure	E-commerce Exposure	Banking Vulnerability	Message Exposure	Clicking Risk
Phishing Victimization	1.000	.536**	.581**	.544**	.582**	.483**
Online Exposure	.536**	1.000	.631**	.487**	.482**	.548**
E-commerce Exposure	.581**	.631**	1.000	.793**	.792**	.806**
Banking Vulnerability	.544**	.487**	.793**	1.000	.796**	.861**
Message Exposure	.582**	.482**	.792**	.796**	1.000	.767**
Clicking Risk	.483**	.548**	.806**	.861**	.767**	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

Individuals with more personal information or frequent online financial transactions are more likely to be targeted by phishing scams (H2).

The data supports the hypothesis that individuals with more personal information or frequent online financial transactions are more likely to be targeted by phishing scams (H2). Significant correlations were found between phishing victimization and factors such as exposure to phishing attempts (r = 0.492), financial transactions (r = 0.460), profile details (r = 0.421), and visits to unsecure sites (r = 0.320). These results suggest that individuals who engage in risky online behaviors are more likely to fall victim to phishing.

The correlation with exposure to phishing attempts (r = 0.492) indicates that greater exposure increases the likelihood of victimization, aligning with findings by Manoharan et al. (2022) that users with varied online experiences, like internet banking, exhibit different levels of vulnerability to phishing scams. This highlights the importance of awareness and experience in mitigating phishing risks.

Table 7. Individuals with more personal information or frequent online financial transactions are more likely to be targeted by phishing scams.

Variables	Phishing Victimization	Exposure to Phishing	Financial Transactions	Profile Details	Unsecure Sites	Reused Passwords
Phishing Victimization	1.000	0.492**	0.460**	0.421**	0.320**	0.235**
Exposure to Phishing	0.492**	1.000	0.676**	0.707**	0.605**	0.243**
Financial Transactions	0.460**	0.676**	1.000	0.725**	0.573**	0.273**
Profile Details	0.421**	0.707**	0.725**	1.000	0.511**	0.316**

Variables	Phishing Victimization	Exposure to Phishing	Financial Transactions	Profile Details	Unsecure Sites	Reused Passwords
Unsecure Sites	0.320**	0.605**	0.573**	0.511**	1.000	0.455**
Reused Passwords	0.235**	0.243**	0.273**	0.316**	0.455**	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

A lack of effective cybersecurity measures or awareness increases the likelihood of falling victim to phishing (H3).

The data reveals a significant relationship between online security behaviors and phishing victimization. A strong positive correlation ($r = 0.557$, $p < 0.01$) was found between using security software and adopting best practices, such as strong, unique passwords. Additionally, security software use was positively correlated with educating oneself about phishing tactics ($r = 0.255$, $p < 0.01$) and regularly updating software ($r = 0.306$, $p < 0.01$), suggesting that individuals who use security software are more likely to adopt broader security measures and stay informed about phishing threats.

These findings support the hypothesis that a lack of cybersecurity measures increases vulnerability to phishing (H3). The correlation between security software use and best practices ($r = 0.557$, $p < 0.01$) shows that security software users tend to be more proactive. Furthermore, the link with phishing awareness ($r = 0.255$, $p < 0.01$) aligns with De Liema et al. (2023), who found that awareness can reduce the likelihood of phishing victimization by 78%, emphasizing the importance of education and security measures.

Table 8. A lack of effective cybersecurity measures or awareness increases the likelihood of falling victim to phishing.

Variables	Phishing Protection	Awareness Protection	Password Security	Ongoing Phishing Education	Software Updates	Phishing Victimization
Phishing Protection	1.000	-0.124	0.557**	0.255**	0.306**	-0.136
Awareness Protection	-0.124	1.000	0.073	0.172*	0.013	-0.095
Password Security	0.557**	0.073	1.000	0.541**	0.604**	-0.034
Ongoing Phishing Education	0.255**	0.172*	0.541**	1.000	0.735**	-0.061
Software Updates	0.306**	0.013	0.604**	0.735**	1.000	0.139
Phishing Victimization	-0.136	-0.095	-0.034	-0.061	0.139	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

Variables	Phishing Protection	Awareness Protection	Password Security	Ongoing Phishing Education	Software Updates	Phishing Victimization

*. Correlation is significant at the 0.05 level (2-tailed).

More sophisticated phishing tactics lead to higher victimization rates (H4).

The correlation data reveals significant relationships between different types of phishing attempts and victimization. Strong positive correlations were found between email phishing and other phishing forms, such as SMS ($r = 0.659$, $p < 0.01$), phone calls ($r = 0.527$, $p < 0.01$), and fake websites ($r = 0.354$, $p < 0.01$), suggesting that individuals exposed to email phishing are more likely to encounter other phishing tactics. Furthermore, exposure to phishing emails correlates with increased phishing victimization, indicating that encountering one type of phishing raises the likelihood of falling victim to others.

These results support the hypothesis that more sophisticated phishing tactics lead to higher victimization rates (H4). The correlations between email phishing and other methods (SMS, vishing, pharming) suggest that multiple phishing channels increase the sophistication of attacks, elevating victimization risks. This aligns with Alabdan (2020), who emphasized how varied phishing methods heighten the risk, underscoring the need for heightened awareness and security.

Table 9. More sophisticated phishing tactics lead to higher victimization rates

Variables	Email Phishing	Smishing	Vishing	Pharming	Pop-up Phishing	Spear Phishing	Angler Phishing	Phishing Victimization
Email Phishing	1.000	0.659**	0.527**	0.354**	-0.010	-0.010	0.166	0.321**
Smishing	0.659**	1.000	0.706**	0.390**	0.084	0.061	0.175*	0.308**
Vishing	0.527**	0.706**	1.000	0.446**	0.041	0.019	0.147	0.268**
Pharming	0.354**	0.390**	0.446**	1.000	0.000	-0.010	0.096	0.121
Pop-up Phishing	-0.010	0.084	0.041	0.000	1.000	0.065	0.013	-0.083
Spear Phishing	-0.010	0.061	0.019	-0.010	0.065	1.000	0.139	0.120
Angler Phishing	0.166	0.175*	0.147	0.096	0.013	0.139	1.000	0.228**
Phishing Victimization	0.321**	0.308**	0.268**	0.121	-0.083	0.120	0.228**	1.000

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Demographic factors like age, sex, and household income may influence the likelihood of phishing victimization (H5).

The correlation data reveals weak correlations between age, sex, and phishing victimization. Age is positively correlated with phishing victimization ($r = 0.178$, $p = 0.035$), indicating that older individuals are more likely to be victimized, though the correlation is weak. Similarly, sex shows a weak positive

correlation (r = 0.188, p = 0.026), suggesting females may be slightly more prone to phishing victimization. Both correlations are statistically significant but indicate that age and sex alone do not strongly predict phishing victimization.

These findings align with Berre et al. (2022), which suggest older adults are more susceptible to phishing due to factors like lower digital literacy and higher trust in online communications. While age plays a role, it is not a strong predictor. The weak correlation between sex and phishing victimization also supports the idea that gender may influence susceptibility, but other factors likely contribute more significantly to phishing victimization.

Table 10. Demographic factors like age, sex, and household income may influence the likelihood of phishing victimization

Variables	Age	Sex	Household's Annual Income	Phishing Victimization
Age	1.000	0.062	0.136	0.178*
Sex	0.062	1.000	-0.004	0.188*
Household's Annual Income	0.136	-0.004	1.000	0.134
Phishing Victimization	0.178*	0.188*	0.134	1.000

*. Correlation is significant at the 0.05 level (2-tailed).

Discussion

The data from this study strongly supports the hypothesis that increased exposure to phishing attempts correlates with a higher risk of victimization (H1). Significant positive correlations were observed between phishing victimization and online behaviors such as e-commerce exposure (r = 0.581), banking vulnerability (r = 0.544), and message exposure (r = 0.582). These correlations highlight that individuals who are more engaged in online activities, particularly in e-commerce and banking, are more vulnerable to phishing attacks. This aligns with the findings of Kirwan et al. (2018) and Berre et al. (2022), who also found that active internet users are particularly susceptible to such risks. The strongest correlation was observed between banking vulnerability and risky online behaviors (r = 0.861), suggesting that users who frequently conduct financial transactions online are at heightened risk.

Similarly, the study supports the hypothesis that individuals with more personal information or frequent online financial transactions are more likely to be targeted by phishing scams (H2). Significant correlations were found between phishing victimization and variables like exposure to phishing attempts (r = 0.492), financial transactions (r = 0.460), and profile details (r = 0.421). These findings emphasize the vulnerability of individuals who share extensive personal information or engage in financial transactions online, aligning with the work of Manoharan et al. (2022), which highlighted how online banking increases susceptibility to phishing attacks.

The hypothesis regarding the lack of effective cybersecurity measures or awareness contributing to higher phishing victimization (H3) was also supported. A strong positive correlation (r = 0.557) was found between the use of security software and good cybersecurity practices, such as using strong passwords. Moreover, using security software was linked to greater awareness of phishing tactics (r = 0.255) and regular software updates (r = 0.306). These correlations suggest that individuals who take proactive measures in securing their online activities are less likely to fall victim to phishing attacks.

This aligns with De Liema et al. (2023), who found that awareness significantly reduces phishing victimization, highlighting the role of education and preventive practices.

Furthermore, the data confirmed the hypothesis that more sophisticated phishing tactics lead to higher victimization rates (H4). Strong correlations were observed between email phishing and other types of phishing, such as smishing ($r = 0.659$), vishing ($r = 0.527$), and pharming ($r = 0.354$). This indicates that exposure to one type of phishing attack increases the likelihood of encountering other forms, supporting Alabdan (2020), who argued that varied and sophisticated phishing methods amplify the risks of victimization.

Lastly, while demographic factors such as age and sex showed weak correlations with phishing victimization (age: $r = 0.178$, sex: $r = 0.188$), they were still statistically significant. Older individuals appeared more vulnerable to phishing, a finding consistent with Berre et al. (2022), which attributed this increased susceptibility to lower digital literacy and higher trust in online interactions. Although these demographic factors are relevant, they alone do not strongly predict phishing victimization, suggesting that online behaviors and cybersecurity measures play a more substantial role in determining vulnerability.

Conclusion

This study examines the factors contributing to phishing victimization, highlighting the significant role of online behaviors and cybersecurity practices. The findings confirm that increased engagement in activities such as e-commerce, banking, and responding to unsolicited messages significantly correlates with higher vulnerability to phishing attacks, supporting Hypothesis 1. This relationship aligns with previous research by Kirwan et al. (2018), which identified a link between online activity and susceptibility to phishing. Additionally, the study validates Hypothesis 2, demonstrating that individuals with more personal information or those engaged in frequent online financial transactions are more likely to become phishing victims. This is evident from the positive correlations observed between phishing victimization and risky online behaviors, such as sharing profile details, conducting financial transactions, and visiting unsecured websites.

The study also confirms Hypothesis 3, emphasizing the importance of cybersecurity measures and awareness in preventing phishing victimization. The data shows that individuals who employ strong cybersecurity practices—such as using security software, securing their passwords, and participating in phishing awareness programs—are less susceptible to falling victim to phishing attacks. This supports the findings of De Liema, Li, and Mottola (2023), who argued that proactive security measures and heightened awareness can significantly reduce the risk of phishing. Furthermore, the study validates Hypothesis 4, revealing that more sophisticated phishing tactics, including email and SMS phishing, result in higher victimization rates. Exposure to one phishing tactic appears to increase the likelihood of encountering others, thereby amplifying the overall risk of victimization.

Finally, while demographic factors like age and sex were weakly correlated with phishing victimization, the study underscores the influence of behavioral factors over demographic ones. This suggests that the likelihood of phishing victimization is more strongly shaped by an individual's online activities and security practices than by personal characteristics. In conclusion, the study stresses the need for continued vigilance and proactive cybersecurity measures, especially for individuals engaged in high-risk online behaviors. Promoting public awareness and encouraging secure online practices are essential steps in reducing phishing risks and protecting users from cyber threats.

References

1. *Angeles City profile – PhilAtlas*. (1990, May 1). https://www.philatlas.com/luzon/r03/angeles.html
2. Anjum, W., Alyana, S. H. D. S. I., Watto, S. A., Munawar, N., & Mahmood, S. (2023). A Qualitative Inquiry Of Intra And Extra Familial Influences On Substance Abuse Among Male Adolescents. *Journal of Positive School Psychology*, 1638-1648.
3. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), 168.
4. Alharthi, D. N., Hammad, M. M., & Regan, A. C. (2020). A taxonomy of social engineering defense mechanisms. In *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 2* (pp. 27-41). Springer International Publishing.
5. Allodi, L., Chotza, T., Panina, E., & Zannone, N. (2019). The need for new antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy*, *18*(2), 23-34.
6. Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.
7. Ayaburi, E., &Andoh-Baidoo, F. K. (2019). Understanding phishing susceptibility: an integrated model of cue-utilization and habits.
8. Berre, T. T., Eggemoen, V., Haugrud, T. D., Le, W. H., & Sandnes, M. (2015). Phishing awareness among students at NTNU. In *6th International Conference on Applied Human Factors and Ergonomics* (Vol. 9, pp. 1117-1124).
9. Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. https://doi.org/10.1080/0735648x.2019.1692426
10. Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(1), 4-23.
11. Carroll, F., Adejobi, J. A., &Montasari, R. (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. *SN Computer science*, *3*(2), 170.
12. Chanti, S., &Chithralekha, T. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, *9*(89), 446-476.
13. Collins, I., & Muhammad, J. (2022, January). Phishing Attack Awareness. In *ADMI 2022: The Symposium of Computing at Minority Institutions*.
14. Cross, C. (2019). Online fraud. *Oxford research encyclopedia of criminology*, 1-32.
15. Dagooc, E. M. (2023, July 19). Philippines ranks fifth with most phishing attacks in 2022. *Philstar.com*. https://www.philstar.com/the-freeman/cebu-business/2023/07/20/2282414/philippines-ranks-fifth-most-phishing-attacks-2022
16. Datta, P., Tanwar, S., Panda, S. N., & Rana, A. (2020, June). Security and issues of M-Banking: A technical report. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1115-1118). IEEE.
17. DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, *47*(3), 1042-1059.

18. Eijigu, T. D., & Teketel, S. Z. (2021). Bullying in schools: prevalence, bystanders' reaction and associations with sex and relationships. *BMC psychology*, *9*, 1-10.
19. Haan, K. (2024, June 24). *49 Email marketing Statistics in 2024*. Forbes Advisor. https://www.forbes.com/advisor/business/software/email-marketing-statistics/#email_usage_statistics_section
20. Holt, T. J., van Wilsem, J., van de Weijer, S., &Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, *38*(2), 187-206.
21. Junger, M., Koning, L., Hartel, P., &Veldkamp, B. (2023). In their own words: deception detection by victims and near victims of fraud. *Frontiers in psychology*, *14*, 1135369.
22. Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 123-128.
23. Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails?. *Telematics and Informatics*, *48*, 101343.
24. Lynch, C. D. (2020). *Understanding the Association Between Routine Activites, Social Bonds, Violent Victimization, and Violent Offending* (Master's thesis, The University of Texas at El Paso).
25. Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2021). To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. *Information and Computer Security*, *30*(1), 37–62. https://doi.org/10.1108/ics-04-2021-0046
26. Msambila, A. A., & Abdallah, A. A. (2021). Economic Factors Influencing Sexual Violence against Children (SVAC) in Primary Schools of Urban District, Zanzibar, Tanzania. *Asian Research Journal of Arts & Social Sciences*, *15*(4), 23-32.
27. O'Hagan, L. (2018, June). Angler phishing: Criminality in social media. In *5th European Conference on Social Media ECSM 2018* (p. 190).
28. Phishing activity trends reports. APWG. (n.d.). https://apwg.org/trendsreports/
29. Simply Psychology. (2023, July 31). *Cluster Sampling: Definition, method and Examples*. https://www.simplypsychology.org/cluster-sampling.html
30. Shahbaznezhad, H., Kolini, F., &Rashidirad, M. (2021). Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?. *Journal of Computer Information Systems*, *61*(6), 539-550.
31. Statista. (2024, April 29). *Most frequent consumer fraud schemes Philippines Q4 2023*. https://www.statista.com/statistics/1271755/philippines-most-frequent-consumer-fraud-schemes/#:~:text=According%20to%20a%20survey%20on,or%20phishing%20using%20text%20messages
32. Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296.