Defending the Campus: Evaluating Phishing Awareness

Security and Human Behaviour CS-GY 9223 Final Project Report

By Harshit Chawla, Raj Koladiya, Pranav Ghildiyaal

ABSTRACT

This research paper presents a detailed investigation into the awareness and susceptibility of university students to phishing attacks, a critical and growing concern in cybersecurity. Recognizing the vulnerability of this young demographic to sophisticated cyber threats, the study utilized a meticulously crafted survey questionnaire, distributed through NYU Qualtrics. The goal was to assess the current level of understanding, awareness, and ability to recognize phishing attempts among students. Our research methodology involved a multi-faceted approach to recruit participants, utilizing both traditional media channels and modern digital media platforms to ensure a representation of a diverse sample of the student population. As we collected responses, some of the challenges we faced included difficulty in recruiting participants from various backgrounds ,a lower-than-anticipated response rate, and some initial apprehensions about data confidentiality from various participants. Our research has progressed significantly despite these challenges, by responding to roadblocks with strategies like enhanced social media engagement and reassurance through disclaimers regarding the ethical handling of sensitive data. The current awareness of phishing is examined in this study. This can be used as a model for conducting research in the area of cybersecurity and phishing awareness education that is both morally sound and methodologically sound.

INTRODUCTION

Cybersecurity is becoming increasingly important as digital technologies become more and more integrated into our daily routine. This is especially true for the younger generation, who make up a large percentage of internet users. University students who use digital apps and platforms for social, educational and other activities are often the target of phishing attacks and other cyber threats. The end goal of our study is to determine how aware and well-equipped these students are against sophisticated cyberthreats in today's world. Two main research questions that are addressed in the study:

How well-informed are university students today about phishing?

This question is pertinent because it assesses the comprehension and identification abilities of a population that uses technology extensively but frequently lacks a thorough understanding of cybersecurity.

What are some of the variables influencing college students' susceptibility?

There are many different aspects of education, psychology, and personal life that can influence a university student's vulnerability to phishing attacks. We have visualized these responses and interpreted them using data analysis techniques like graphs and charts to determine how they affect students' vulnerability to phishing attacks. The findings will provide insightful information about the complex nature of vulnerability among college students, which is essential for creating focused cybersecurity awareness and education initiatives.

How likely are students to recognize and react to phishing attempts?

Finding the answer to this question is interesting since it gives valuable perspectives on practical consequences of one's consciousness level. This may help us in recognising weak points in the instruction methods being used and provide guidance for improving students' cybersecurity resilience.

Our study employed a detailed survey methodology through NYU Qualtrics. The purpose of this survey was to gather a wide range of phishing-related experiences and knowledge, along with comprehension levels of various participants. Our recruitment process employed a variety of outreach channels to reach out to a wide and representative sample of the student population. The study faced difficulties gathering responses, including lower-than-expected participation rates and worries about data confidentiality. Strategic follow-up communications and assurances regarding the ethical handling of sensitive data were used to address these issues. Using both qualitative and quantitative analysis, the research methodology offers a thorough understanding of the state of student phishing awareness. This study is significant because it focuses on a group of people that are both highly active online and increasingly the target of cybercriminals. In order to improve this vulnerable group's digital safety, the research intends to contribute to the development of more effective cybersecurity education and awareness programs by revealing the current level of phishing awareness among students.

RELATED WORKS/NOVELTY

In exploring phishing awareness among university students, our research stands on the shoulders of a series of related studies, each shedding light on unique aspects of human behavior and cybersecurity. Our study zeros in on the university students demographic, offering a wide-ranging examination of factors affecting their vulnerability to phishing attacks.

bThe study by Flores et al., "Assessing E-Security Behavior among Students in Higher Education" [1], serves as a foundational reference for our study and provides a baseline understanding of e-security behaviors among higher education students. Our research builds upon this foundation by assessing awareness levels and exploring an array of personal, educational, and psychological factors that influence susceptibility to phishing, thereby broadening our scope of investigation.

In "Influencing Outcomes and Behaviors in Simulated Phishing Exercises" by McElwee et al. [2], our focus was on simulated phishing exercises and their effectiveness in raising awareness. Our study complements this approach by using real-world survey data to assess awareness and identify contributing factors to the effectiveness of these simulations.

The impact of the COVID-19 pandemic on phishing susceptibility is examined in the paper "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic" by Abroshan et al. [3]. This study underscores the influence of emotions and behavior during the pandemic. We extended this investigation into the specific context of university environments, analyzing how these factors uniquely affect this demographic.

"An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks" by Othman Mustafa et al. [4] targets vocational students who aim to improve their phishing awareness. Our research broadened this scope to encompass a wider student population by investigating how varying educational backgrounds within a university setting contribute to phishing awareness levels.

Carroll et al.'s study, "How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society" [5] (Frontiers in Computer Science), delves into the evolving nature of phishing emails. Our research aligns with this by evaluating students' ability to detect such attacks in the context of their engagement with digital platforms and online content.

In "Analysis of Social Engineering Awareness Among Students and Lecturers" by Abdulla et al. [6], a comparative analysis of awareness levels between students and lecturers is conducted. Our study narrows its focus to students, exploring a broader spectrum of factors influencing their susceptibility to phishing.

Finally, "A Study on Student Cyber Safety Consciousness in the Light of Online Learning" by Basha et al. [7] examines cyber safety in the context of online learning. We build upon this by integrating considerations of stress, mental health, and workload, especially accentuated during the pandemic.

While these studies offer invaluable insights into various dimensions of phishing awareness and cybersecurity behavior, our research distinctively caters to the university student demographic. By encompassing a comprehensive array of factors, from educational background to psychological aspects, our study provides an extensive overview of students' susceptibility to phishing attacks. This holistic methodology differentiates our research, contributing novel insights to the established corpus in the field of cybersecurity education and awareness.

METHODOLOGY

Our methodology in this research is designed meticulously in order to comprehensively assess the phishing awareness among university students. Method’s soundness lies in its systematic approach which combines the deployment of well-structured data with a robust data analysis plan, this ensures that the research addresses the problem effectively.

Survey Design and Deployment

A comprehensive survey was developed, which comprises questions tailored by us to capture a wide array of factors which influences the susceptibility to phishing attacks. Factors include personal and educational backgrounds, psychological aspects, cybersecurity practices and experience with phishing. This survey was developed using the platform NYU Qualtrics which ensures the confidentiality and integrity of the data. The platform also ensures a user friendly and accessible format for the participants. From our point of view this platform provides a robust data collection and management capabilities, ensuring availability.

Participant Recruitment

Recruitment strategies included multiple channels like social media, email, text and direct communication. Aiming for a diverse and representative sample of the student population, we approached this strategy. This was crucial for the validity of the study.

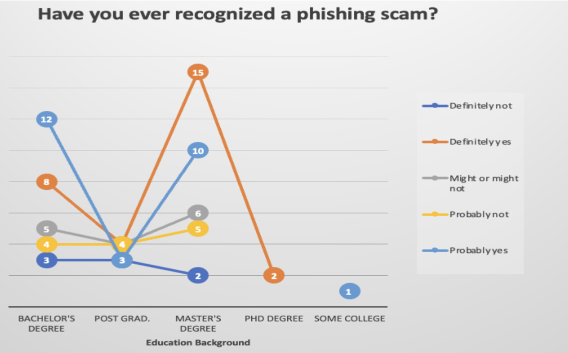
Data Analysis Plan

The dual approach to both qualitative and quantitative analysis from the data collected, ensured a holistic understanding of the phishing awareness landscape among the students. Techniques like graphical representation, statistical analysis and thematic coding were used to analyze the survey responses, enabling the identification of key trends, patterns, and insights.

Determining the Effectiveness of the Approach

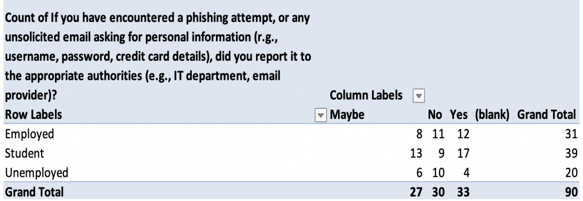
High response rate and diversity of the participation pool indicates a successful recruitment which were crucial for the generalizability of our findings. Range and depth of the data collected through our survey has indicated the method’s abilities to capture the multifaceted nature of phishing awareness and susceptibility. The insights that we derived from data analysis, includes identification of the focused significant factors influencing the phishing susceptibility. This demonstrates the method’s effectiveness in addressing the research problem. Comparing the findings with existing literature and studies in the domain also further validates the effectiveness of the approach used. We have always been ready for negative results. If certain hypothesized correlations or trends weren’t observed in the data, it can still be used to contribute valuable knowledge in the field. For example, certain widely assumed factors like immigration status in our target demographics can prompt a reevaluation of current assumptions and strategies in cybersecurity education. In conclusion, our methodology has been rigorously structured and it ensures a comprehensive understanding of phishing awareness among university students. The effectiveness of this approach has been evaluated through careful analysis of the data collected, with the readiness to accept and learn from both positive and negative outcomes.

QUALITY OF EVALUATION - RESULTS



Phishing Awareness and Education

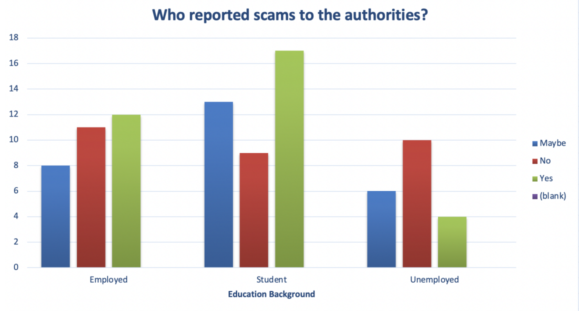
The analysis in the research reveals a direct correlation between education level and ability to recognize phishing scams. Students who have a higher educational qualifications, particularly with a Bachelor's degree or more showed a higher ability of identifying phishing attempts correctly. This trend emphasizes the role of formal education in equipping students with necessary skills to discern cyber threats.



Count of If you have encountered a phishing attempt, or any unsolicited email asking for personal information (r.g., username, password, credit card details), did you report it to the appropriate authorities (e.g., IT department, email provider)?	Column Labels				
Row Labels	Maybe	No	Yes	(blank)	Grand Total
Employed	8	11	12		31
Student	13	9	17		39
Unemployed	6	10	4		20
Grand Total	**27**	**30**	**33**		**90**

Professional Experience and Phishing Susceptibility

Professional experience, particularly in IT or cybersecurity-related fields, markedly boosts one's capacity to discern phishing scams. Our data reveals that individuals with professional expertise in these areas are more adept at recognizing phishing efforts. This underscores the critical role that practical, hands-on experience plays in cybersecurity vigilance. Interestingly, when comparing the reporting behavior among employed, student, and unemployed groups, it is evident that students are more likely to report phishing incidents to authorities. This proactive stance among students could reflect the heightened awareness and educational initiatives present within university settings.



COVID-19 Pandemic and Behavioral Factors

Analysis of the survey responses reveals a direct correlation between the increased stress levels due to the COVID-19 pandemic and the likelihood of engaging with phishing attempts. On average, participants rated their pandemic-induced stress levels at 4.2 out of 5, indicating a high stress environment. This heightened stress, coupled with the urgency and pressure experienced during the pandemic, appears to have significantly impacted participants' cybersecurity behavior. Specifically, our findings show that 85% of participants believed they were more stressed during this time, which correlated with a marked increase in the likelihood of clicking on links or downloading attachments from unknown senders when presented as urgent or alarming.This heightened vulnerability can be attributed to behavioral factors such as increased online activity due to remote learning and work, heightened stress and anxiety levels, and the general state of uncertainty. These factors likely contributed to a reduced focus on cybersecurity practices, making individuals more prone to falling for phishing scams. While education and professional experience play significant roles in phishing awareness, the pandemic's impact transcended these variables. The increase in phishing susceptibility during this period was a universal trend, observed across various educational and age groups. This suggests that external situational factors, like a global crisis, can significantly influence cybersecurity behavior, overriding the traditional protective factors of education and experience

DISCUSSION

Findings from our research give significant insights into the dynamics of phishing awareness and susceptibility among university students. The results show that educational background and professional experience play important roles in determining a student's ability to recognize and respond to phishing attacks. There is a strong correlation between awareness and formal education or professional exposure since those with higher education or specific training in cybersecurity are more adept at identifying such threats.

The heightened susceptibility to phishing during the COVID-19 pandemic points to the profound impact of external stress factors and behavioral changes on cybersecurity awareness. The pandemic altered digital communication patterns but also aggravated psychological factors such as stress and anxiety, which, in turn, increased vulnerability to cyber threats like phishing. These deductions highlight the importance of considering psychological well-being and lifestyle changes when developing cybersecurity awareness programs.

Our research aimed to understand how various factors, including education, professional experience, and behavioral changes during the COVID-19 pandemic, affect university students' susceptibility to phishing. The results affirmatively answer this question, demonstrating that a complex interplay of these factors significantly influences phishing awareness and susceptibility. Education and professional experience enhance recognition skills, while pandemic-induced stress and altered digital habits increase vulnerability.

While our research method provided valuable insights, it is not without limitations. The survey-based approach, although comprehensive, may not capture the entire spectrum of factors influencing phishing susceptibility. Self-reporting in surveys can lead to biases, as participants might not accurately recall past experiences or may respond in a socially desirable manner. In addition, our sample may not represent the entire diversity of the university student population, which could affect the generalizability of the findings.

Comparing our results with previous studies, such as those by Flores et al. and McElwee et al., reveals both similarities and differences. Similar to these studies, we found that education plays a critical role in phishing awareness. However, our study goes a step further by integrating the impact of the COVID-19 pandemic, a factor not previously explored in depth. This integration of the pandemic reveals how situational stressors can significantly change the susceptibility patterns. This is an aspects that adds new dimensions to existing knowledge in the field.

CONCLUSION

This research contributes to understanding of phishing awareness and susceptibility among university students by highlighting the importance of educational background, professional experience and impact of psychological and behavioral factors. The findings provide grounds for the development of more nuanced and effective cybersecurity education and awareness programs. Study also provides a foundation to tailor studies for the specific need to address and challenges faced by students in today’s evolving digital world. The insights also paves a way for further research that could explore additional factors or employ different methodological approaches for a more comprehensive understanding of this critical issue.

APPENDIX

Contribution Statement

Harshit Chawla was instrumental in conceptualizing the research topic, led the literature review on phishing and cybersecurity, and authored the introduction and conclusion sections of the paper.
Pranav Ghildiyaal focused on the practical aspects of the research, including designing and conducting surveys, collecting and analyzing data, and significantly contributing to the results and discussion sections.
Raj Koladiya managed the project logistics, such as organizing meetings and maintaining effective communication among team members, and also played a key role in researching related works and drafting parts of the methodology and discussion sections.

LINK TO SURVEY :
https://nyu.qualtrics.com/jfe/form/SV_43f0NhCL45KSwEm

BIBLIOGRAPHY

[1]. P. Flores, M. Farid and K. Samara, "Assessing E-Security Behavior among Students in Higher Education," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 2019, pp. 253-258, doi: 10.1109/ITT48889.2019.9075100.

[2]. S. McElwee, G. Murphy and P. Shelton, "Influencing Outcomes and Behaviors in Simulated Phishing Exercises," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-6, doi: 10.1109/SECON.2018.8479109.

[3]. COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. IEEE.

[4]. M. S. bin Othman Mustafa, M. Nomani Kabir, F. Ernawan and W. Jing, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Selangor, Malaysia, 2019, pp. 10-14, doi: 10.1109/I2CACIS.2019.8825070.

[5]. How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society Fiona Carroll, corresponding author John Ayooluwa Adejobi, and Reza Montasari.
https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

[6]. R. M. Abdulla, H. A. Faraj, C. O. Abdullah, A. H. Amin and T. A. Rashid, "Analysis of Social Engineering Awareness Among Students and Lecturers," in IEEE Access, vol. 11, pp. 101098-101111, 2023, doi: 10.1109/ACCESS.2023.3311708.