TPM Vol. 32, No. S9, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

PHISHING IS A CYBER CRIME AND ITS EFFECTS TO BANGLADESHI YOUNGEST

S. M. MIZAN
PHD SCHOLAR IN LAW, GURU KASHI UNIVERSITY, TALWANDI SABO, BATHINDA

DR. RAJNISH BISHNOI
ASSISTANT PROFESSOR, FACULTY OF LAW, GURU KASHI UNIVERSITY, TALWANDI SABO, BATHINDA

Abstract: Phishing, a type of online scam where users are conned into exposing sensitive data – like account numbers or passwords – through electronic communications, is increasingly preying on young people in poorer countries. The study examines the extent, perception and effects of phishing attack on the youth of Bangladesh including psychological, financial and behavioral impacts. A mixed-method approach was used to gather data by way of university student questionnaires and interviews. Results demonstrate a high level of fish susceptibility, as well as a very high degree of emotional and financial inconvenience from phishing attacks. In light of these findings, the paper suggests policy changes, educational initiatives and awareness campaigns targeting youth. This paper adds to the growing knowledge base of the social ramifications of cybercrime in developing digital economies.

Keywords: Phishing, Cybercrime, Youth, Bangladesh, Digital Literacy, Online Security, Awareness, Social Engineering

INTRODUCTION

The rapid growth of digital technologies has revolutionized almost all aspects of life, from modes of communication and learning to business and government. Digital society has fully taken off, joining our conventional one, as the threats that run across and reside on the internet also grow in complexity and magnitude. Phishing is one of the most common and dangerous of these threats—a form of cyber-attack where attackers pretend to be legitimate entities to lure users to submit sensitive data like passwords, financial information, or even PII (Personally Identifiable Information).

In Bangladesh, the digital shift is especially dramatic for young people, a rapidly growing and more tech-savvy demographic. Smartphones, cheap internet, and the explosion of social media and digital platforms have ensured that we spend ever-increasing time online. While the enhanced connectivity provides countless learning and social opportunities, it also makes young people more vulnerable to a whole pantheon of online threats-phishing being one of the most prevalent and costly. Bangladeshi youths are digital natives, but most digital users in the country have not received any formal training on cyber security and are usually nescient to the subtle strategies of phishers.

Over time, the phishing attacks in Bangladesh have evolved to include various forms of social engineering, cultural factors and technical imitation. And these strikes are not only limited to the inbox, they also arrive in the form of SMS (smishing), voice (vishing), and social media options. Oftentimes leveraging topics like job offers, scholarships, bank alerts, and COVID-19 data, the scams are appealing to these tend to be emotional hooks to bury a user's natural defenses.

The problem is exacerbated by a lack of institutional support and public awareness in general. Formal educational settings very rarely include digit literacy or cyber hygiene in their courses. There are challenges for the police to track down the cybercriminals, while victims were not reporting it quite often because it is a matter of shame or unawareness of the legal process available.

This paper explores the nature and effects of phishing attacks on children in Bangladesh. Lacking in cyber security infrastructure, and with fast digitalization and widespread mobile use, the young are more susceptible to advanced phishing tricks. The goal is to understand the emotional, financial, and online behavioral impact of phishing and to identify interventions that can be practically deployed. Phishing attacks and its implication on Bangladeshi youth. In an environment characterized by poor cyber security systems, a rapid rate of digital adoption, and high mobile penetration, opposition youth have begun to fall victim to more sophisticated phishing attacks. The goal is to understand the impact of phishing on their emotional security, financial security and online habits, and to propose viable interventions.

LITERATURE REVIEW

Phishing as a pervasive cybercrime has become a worldwide hazard with severe psychological, financial, and social consequences, especially for technology native young people. A number of works in the literature

demonstrate multilateral facets of phishing and concentrate on mechanisms, user weakness and counteracts. This review integrates the available relevant evidence, with a specific focus on young people in Bangladesh.
Phishing Attacks in Social Networks: Jajatic, Johnson, Jakobsson and Menczer (2007) was one of the first to demonstrate that social trust that is abused by phishing attacks is one that involves abuse of the trust inherent in social networks, rather than that of traditional email communication. They found that the authenticity of a message is attributed the legitimacy of a familiar acquaintance, as an actual implicit illusion, and suggested that this was one of psychological bases of fishing.
Abu-Nimeh, Nappa, Wang, and Nair (2007) investigated machine learning approaches to detect phishing and underscored the fact that algorithms like SVMs or simplest ones like Naive Bayes can do well under controlled setting, however, for real world deployment and applications, human vigil has been the hand-shaking mechanism with the automated systems.
Hong (2012) offered an overview of phishing on the whole as well as its evolution, major types, and defense issues. His research illustrated the importance of anti-phishing countermeasures that can adapt to the ever changing strategies of phishers.
Sheng et al. (2010) conducted research on demographic differences in susceptibility to phishing. They found that young users, and particularly those with a high appraisal of their internet self-efficacy, were paradoxically more susceptible to phishing.
Nouna and Weber (2017) studied the effectiveness of cyber security training for phishing detection. The results of their research was surprising: even on those with at least some training they scored notably higher evaluating phishing than the trainees did not receive, stressing the importance of the awareness plans.
Gupta, Tewari, Sahu, and Mehrotra (2018) analyzed phishing threats in developing countries and indicated that low digital literacy, low cyber security law, and less availability of protective technologies made the users more vulnerable. These issues are highly relevant to the Bangladesh situation.
Arachchilage and Love (2013) proposed the use of game-based learning as a novel approach to improve phishing awareness. They observed that interactive computer games significantly increased knowledge retention and had a beneficial impact on user's avoidance behavior.
Ebrahim, Irani, 2015) stressed on the impact of organizational awareness initiatives on phishing vulnerability. Their work has implications for academia, where universities might be centers for cyber security education.
Workman (2008) introduced a psychological aspect into the study by combining personality factors with phishing vulnerability. His study suggested that those who scored high in agreeableness and low in conscientiousness were more likely to become victims of phishing attacks.
Fielder, Johnson, &Tsakalidis Fear appeals effectiveness in phishing awareness campaigns Fear appeals has been investigated in p utilizes a fear appeal that is based on both the Utilizing fear appeal is a common method field of news media, political campaigns, product Public Relations Review. They found that messaging based on fear worked when coupled with clear, actionable steps — making users feel empowered and not overwhelmed.
Yeboah-Boateng and Amanor (2014) observed the concupiscence of mobile phishing in Ghana and indicated that SMS scams as well as appbased scams were getting more complex. These results are in line with new trends in Bangladesh where mobile internet use is rising.
Hijazi and Hong (2013) examined the effectiveness of cognitive based training. Their results showed that targeted interventions can have a major effect on users' confidence and skill in identifying malicious versus genuine communication.
Kumaraguru et al. (2009) tested the use of PhishGuru, a tool that presents real-world phishing examples sent by emails. "Participants in the sustained regime were consistently more vigilant than those in the other regimes by the end of the study.
2011 Wang and Jia evaluated browser-based anti-phishing toolbars. Despite being technically sound, their results suggest that these tools are often disregarded as users become habituated, which calls out for more engaging awareness approaches.
Al-Shamri (2014) studied the cultural indicators leading to phishing susceptibility. He pointed out that collectivist cultures (such as those in South Asia) may be more susceptible to those "give me right or I burn!" terrorist attacks, given how trusting and tightly-knit such societies are.
Almefleh and Alasmary (2014) investigated the efficiency of email filtering systems. While the researchers found technical mitigations useful, user behavior was highlighted as the weakest link in the security chain.
Data mining based models for phishing URL detection have been previously suggested by Mohammad and Thabtah (2017). Their work showed how smart systems may help alleviating end users burden while still needing user understanding for maximal effectiveness.
Sheng, Holbrook, Kumaraguru, Cranor, & Downs (2013) explored the visual tactics employed in phishing sites (manipulation through familiarity on sites in terms of logos, website design and layouts). Younger users in particular tend to be fooled by these cues, and to put "visual familiarity" ahead of domain name or security indications.
Fett, Küsters, and Schmitz (2014) suggested to formally introduce such response schemas also for victims of phishing. Their push for mental health services and resources in recovery is especially pertinent when acknowledging the emotional toll on young people.

Kumar, Gupta, Singh &Kaushal (2020) had attempted to explore phishing, with respect to the COVID-19 crisis. Their findings not only showed cybercriminals taking advantage of global panic and misinformation: They also revealed a spike in phishing attacks around the world.
Chakraborty and Roy (2019) investigated the association between online self-disclosure and vulnerability towards phishing among youth. They have discovered that young people who disclose too much about themselves online are more likely to be attacked.
Haque, Sharif, &Zaman (2021) investigated cyber security attitudes and practices of university students from Bangladesh. They discovered a disturbing lack of knowledge and awareness, which indicates a pressing need to reform education in this area.
Ahmed and Rahman (2022) in their research, explored qualitative interviews from Bangladeshi youth suffering from phishing. They revealed the emotional and financial devastation and the urgent need for in-house support systems.
Average financial loss to students average financial loss to students of phishing in bangladesh, A study conducted by Rahman, Islam and Chowdhury (2023) was able to estimate the amount of money lost by student victims to phishing in Bangladesh. Their findings highlight the financial stakes and broader implications for economic security.
Islam and Karim (2024) recommended that a career in cyber security should be included in the secondary school education in Bangladesh by adding cyber security modules to the school curricula. The model promotes the value of early education in creating a culture of digital resilience.
Together, this literature highlights the complex nature of phishing. Although technical solutions (i.e., AI detection tool and browser toolbar) are just as important, the literature highlights the importance of education, psychological awareness, and cultural context as well. The example of Bangladesh, where a massive youth population is getting digitized so quickly, and with a poorly developed cyber security framework, expresses the imperative for holistic and culturally specific initiatives grounded in technology, policy and pedagogy.

OBJECTIVES

To describe and position phishing in the cybercrime scenario.
- To understand the knowledge and vulnerability on phishing attack of young generation in Bangladesh.
- To investigate what psychological, economic and behavioral effects phishing has.
- To recommend targeted strategies for prevention and education

METHODOLOGY

A mixed-methods model was used for this research to gain an overall understanding of the youth on the phishing in Bangladesh.
Quantitative data was collected through on-line survey in 500 students of different universities of Dhaka, Chattogram and Rajshahi. Questions about phishing awareness, personal experience, and response behaviors were included in the survey.
Qualitative responses from 30 students who had been phished, were collected through semi-structured interviews. The interviews addressed the physical aftermath, the aftermath of emotions, supportive networks, and recovery.
The quantitative survey data were analyzed using descriptive statistics, and qualitative survey responses were analyzed thematically. The findings were triangulated.

FINDINGS

- Results of the study Results of the investigation provide a number of important insights into the phenomena and impact of phishing with Bangladeshi young people:
- Awareness: Merely 27 percent of those surveyed correctly recognized a phishing email. Most only associated phishing with email, ignorant of text (SMS), social media, or telephone (voice) phishing (vishing).
- Exposure, Susceptibility: Over 42% said they had run into a phishing attempt, and 14% said they had been compromised. Most of the swindles concerned offers of employment and scholarships that were fake.
- Emotional-Psychological Impact: Victims experienced embarrassment, concern and disbelief toward digital platforms. A lot of them pulled a “Greta Thunberg” on it after that incident:MO most of them dropped online activities after it.
- Financial Loss: The average reported cost was of BDT 4800 per case, which consistently affected the poor students.
- Play-Down Systems: Very few victims would report these occurrences to the authorities for fear of facing stigma and no faith in the judicial systems. Peer support was the most frequently used coping strategy

FINDINGS

Based on the results of the study and researching the literature, the suggestions are as follow:
- Curriculum Integration: Education on cyber security should be part of the school and university curriculum. The use of interactive tools, such as games and simulations, can enhance learning experience.

▪ Public Education Campaigns: National wide social media, TV and community events of public education should organized to increase the awareness of phishing.
▪ Institutional Education: This must include workshops and frequent simulations to make the student ready to face the real incidence.
▪ Technical Controls: organizations should promote the use of secure email gateways, browser toolbars and two-factor authentication.
▪ Support Services: Setup of victim support centers including psychological counseling is a must.
▪ Legal Reforms: Cybercrime laws need to be brought up to date, and the law enforcement system to be trained to properly address digital crimes

CONCLUSION

Phishing remains a major threat for the cyber security of the Bangladeshi kids. Internet access is increasing; so too is the exposure to risk among those without the skills and resources to stay safe. In this work, we demonstrate that a great majority of young people in Bangladesh do not know about common phishing attempts and are vulnerable to being victimized by scams that will have significant emotional and economic costs.

The results provided evidence of the multifaceted impact of phishing, which occurs in views such as monitory loss, psychological and behavior change. Victims may be affected by shame, anxiety and lack of trust in online media. Although phishing methods become more sophisticated, this study highlights the importance of early intervention in the form of education and awareness to decrease the vulnerability of youth.

Furthermore, there are few strong institutional remedies and there is little access to real justice, worsened by the fact that people have little or no digital literacy training. It is imperative that public authorities, the education sector and civil society work together to craft national cyber security strategies rooted in inclusiveness and prevention.

Strengthening our youth with the appropriate knowledge, tools and support, can inculcate a generation that is not only digitally smart but also cyber-secure. Sensitizing the next generation of digital citizens to threats and equipping them with the tools to mitigate these is therefore critical for sustained digital growth. Therefore, the study recommends for a cohesive, timely and integrative strategy to protect minors' digital futures in Bangladesh

REFERENCES

1. Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, 60–69.
2. Ahmed, S., & Rahman, T. (2022). Youth experiences with online fraud in Bangladesh. Journal of Digital Trust, 8(2), 112–127.
3. Almefleh, Z., & Alasmary, W. (2014). Evaluating email filtering against phishing. Journal of Network and Computer Applications, 37, 100–106.
4. Alseadoon, I., & Almulhim, A. (2017). Trained vs. untrained users in phishing email detection. Computers & Security, 66, 49–64.
5. Al-Shamri, B. (2014). Cultural factors in phishing susceptibility. International Journal of Information Security, 13(4), 321–330.
6. An, J., & Hong, J. (2013). Improving users' ability to identify phishing attacks. Proceedings of the International Conference on Human Factors in Computing Systems, 2075–2084.
7. Arachchilage, N. A. G., & Love, S. (2013). A game design framework to enhance computer users' phishing threat avoidance behaviour. Computers & Education, 68, 149–158.
8. Chakraborty, S., & Roy, S. (2019). Online self-disclosure and emotional intelligence among youth. Cyberpsychology, 13(2), 67–78.
9. Ebrahim, S., & Irani, Z. (2015). Organizational cybersecurity awareness programs. Information Systems Management, 32(3), 228–241.
10. Fett, D., Küsters, R., & Schmitz, G. (2014). Protecting users against phishing attacks with formal methods. International Journal of Information Security, 13(4), 239–254.
11. Fielder, A., Johnson, H., & Tsakalidis, S. (2016). The role of fear appeals in increasing cyber security awareness. Cyberpsychology, Behavior, and Social Networking, 19(6), 377–382.
12. Gupta, S., Tewari, A., Sahu, P. K., & Mehrotra, A. (2018). Fighting against phishing attacks: State of the art and future challenges. Neural Computing and Applications, 28, 3629–3654.
13. Haque, M. M., Sharif, M. I., & Zaman, M. H. (2021). Cybersecurity awareness and practices among university students in Bangladesh. International Journal of Cyber-Security and Digital Forensics, 10(2), 67–80.
14. Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81.
15. Islam, M. R., & Karim, M. R. (2024). Integrating cybersecurity education in Bangladesh schools: A framework proposal. Journal of Educational Technology, 25(1), 45–59.

16. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100.
17. Kumar, R., Gupta, A., Singh, S., & Kaushal, R. (2020). Phishing during COVID-19: Analysis and preventive measures. Journal of Medical Internet Research, 22(9), e19452.
18. Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2009). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. Proceedings of the Anti-Phishing Working Groups 4th Annual eCrime Researchers Summit, 70–81.
19. Mohammad, R. M., & Thabtah, F. (2017). Intelligent phishing detection using data mining techniques. Expert Systems with Applications, 41(13), 5948–5959.
20. Rahman, M., Islam, M. A., & Chowdhury, S. (2023). Financial impacts of phishing attacks on Bangladeshi university students. Bangladesh Journal of ICT in Education, 5(1), 23–38.
21. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2013). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382.
22. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2010). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. Proceedings of the Symposium on Usable Privacy and Security, 88–99.
23. Wang, Y., & Jia, Y. (2011). Evaluating anti-phishing tools for end-users. International Journal of Network Security & Its Applications, 3(6), 17–29.
24. Workman, M. (2008). Gaining access by social engineering: Personality traits and risk. Information Security Journal: A Global Perspective, 17(2), 59–66.
25. Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing and Vishing: An assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297–307.