You Received an Email from Your Advisor? A Case Study of Phishing Scams in a University Setting

Aiping Xiong, Sian Lee, Zekun Cai, Ephraim Govere, and Harish Kolla

The Pennsylvania State University

1 Introduction

Phishing is a social engineering attack [7] that typically aims at tricking people into revealing their personal information [10]. To deceive victims, phishing attackers typically send spoofed emails [8] or instant messaging [9] as from trusted sources. Falling prey to phishing scams could have devastating consequences (e.g., financial loss) for both individuals and organizations [6].

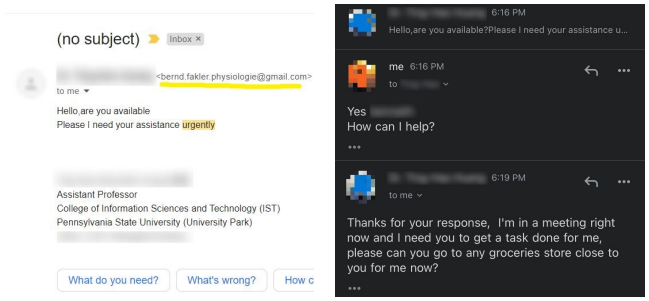
Despite the advancements of automated detection ([15, 16], see [10] for a review), a large number of phishing emails continue to evade the detection and a large proportion of people who receive them continue to be deceived. Previous studies have examined how users perceive and react to phishing emails and legitimate emails [3, 14, 18]. Most studies have shown that users are not good at separating phishing emails from benign ones (e.g., [17]). Moreover, attackers exploits the use of phishing emails in various situations. For example, in a specific phishing technique called spear phishing, emails are sent as from the receiver's friends [1], colleagues [4], or social and professional groups [12], exploiting human weakness [11]. Recent studies have also shown that mobile device users are more vulnerable to phishing attacks as compared to desktop users [5].

In this work, we describe our efforts on evaluating one real-world spear phishing attack in a university setting. We seek to answer the following research questions (RQs):

- RQ1: Why was the phishing attack successful in the setting of an academic-research team within a universality?
- RQ2: How can we better detect and mitigate the spear phishing attack on academic-research teams?

2 Case Investigation

Our case study includes two parts: 1) we examine the phishing emails to understand the aims behind the attack; and 2) we conduct group interviews with two research groups targeted by the investigated phishing attack to gain insights about how to better detect and mitigate such attacks in the future.



(a) Desktop Version-Gmail (b) Mobile Version-Outlook

Figure 1: The Phishing Emails

2.1 Phishing Email Analysis

Before the interview, we examined the phishing emails in the investigated case. We asked the involved faculty members ($n = 2$) and the students ($n = 4$) to send us the phishing emails that they received. Our team analyzed the phishing emails and there are a few interesting findings.

The reported phishing emails came from both desktops and mobile devices (see Fig. 1). Both faculty members and students have forwarded their university Office 365 emails to their Gmail accounts. User interfaces (UIs) of popular email services (e.g., Gmail and Office 365) typically vary across those devices. Critically, with the mobile interface, users could only see the name of the sender but not the email address (see Fig. 1b top row). Both students who had communicated with the phisher (i.e., replied to the phishing email) used a mobile device. Based on the investigation results, we prepared mobile and desktop interfaces for the group interviews.

2.2 Group Interview

We conducted semi-structured, group interviews to investigate the tactics used by the attacker and common patterns across the two groups under attack. We also elicited insights from students and faculty members involved in the phishing attack about how to mitigate similar scams in the future.

Method. We recruited two research teams involved in the

phishing attack. There were a total of five participants, two faculty members (both male) and three Ph.D. students (one female). Two to three participants from each group joined the interviews, which were conducted online using Zoom. Each interview lasted between 75 to 90 min. We obtained an IRB approval for the study. Participants were not compensated.

After verbal consent, each interview started with warm-up questions, in which participants described their everyday email processing, including devices and apps. Then, we asked them to share their *phishing attack experience* with screenshots of emails on both desktop and mobile interfaces. Participants were later asked to elaborate on their *email processing* on both interfaces and especially the cues that are important for them to detect phishing emails. Their awareness of the interface differences across devices (i.e., desktop vs. mobile) was also examined.

Data Analysis. Interviews were audio recorded with the interviewees' permission. Each recording was initially auto-transcribed by Zoom and corrected by two researchers. Each transcript was then analyzed by at least two researchers. Using open coding, researchers constructed their own independent codebooks focusing on the participants' phishing scam experience and their daily email processing behavior. The researchers then met to discuss the codes that they identified. Through iterative coding and discussion sessions, the researchers reached an agreement on the analyzed results.

3 Results

The Phishing Attack Experience. The reported phishing attack was a gift card scam. The attacker did not reveal the real intention in the phishing email initially. Two students using the mobile device responded to the phisher. After three rounds of email exchanges, the real intention was revealed (see Fig. 1b). Once the phisher requested a gift card, one student stopped the communication immediately and then reported the incident to the faculty member. However, the other student (the victim) mentioned that the urgent request prevented her from checking the validity further. Also, as an international student, she did not have any prior knowledge about the gift card scam. The victim student described that the scams occurred over multiple iterations and the requested money increased throughout the iterations.

Both faculty members learned about the phishing attacks on their team from the students. There were several attacks on different members (e.g., current and alumni students) in each group. When more than one case was reported, the faculty members informed other students of the phishing attack. For each team, neither the students nor the faculty members notified their IT department when there was a single case.

Email Processing. Both faculty members and students used mobile phones to check their university emails. They also noticed that the desktop version gives more information compared to the mobile version. Specifically, the students noticed that the mobile UI does not show email addresses but only shows the name of the sender. Students can remember their advisors' email addresses, so it is easy for them to check the email address to verify the legitimacy. However, the students also mentioned that typically they ignored the email address when opening an email.

4 Discussion

College students are one of the most vulnerable populations with regard to phishing attempts [13]. The case we investigated was similar to that reported in 2019 [2]. Critically, our investigation revealed that the use of mobile devices and students' lack of knowledge and awareness of the phishing scam are two primary reasons for such phishing attacks being successful in the setting of an academic-research team (RQ1).

In recent years, more phishing attacks have been evident for mobile users [5]. Our case study results are consistent with prior findings showing that the cues to detect possible phishing emails are unavailable on mobile devices (RQ1). In particular, our case study revealed that such a lack of cues might have resulted in more interactions between users and attackers, leading to successful attacks.

Students and faculty members are encouraged to report suspected phishing emails during cyber security training or simulated phishing campaigns. Yet, neither the faculty members nor the students in our case study reported the phishing scam under the initial attack (RQ1). Such behavior suggests that *reporting phishing scams immediately* should be highlighted in phishing training (RQ2).

Participants gave suggestions on email UIs to enhance their awareness and detection of phishing emails, such as highlighting the mismatch between the sender's name and the email address (RQ2). The victim student described that she would like to see warnings or alerts about keywords related to known phishing attacks (e.g., gift cards).

While the above findings are generalizable to other settings, we obtained two *unique* insights about spear phishing mitigation in university settings. First, the faculty members offered insights regarding the source of the phishing attack. They conjectured the phishing attack could be due to the linkability between their homepage and the students' LinkedIn pages (RQ1). Such insights are intriguing, which highlights the importance of protecting students' *privacy* (e.g., emails) to prevent them from phishing scams. Second, the victim case in our investigation revealed that *international students* are vulnerable to phishing attacks. Considering the ratio of international students in the academic research teams, additional training should be considered to equip them with knowledge and skills to detect phishing attacks.

Our case study highlights challenges in preventing phishing scams in the education setting. We believe that our findings could inform future research to design interfaces and develop training to help college students detect and report spear phishing scams. We also recommend enhancing privacy awareness and protection of college students.

References

[1] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. Unpacking spear phishing susceptibility. In *Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21*, pages 610–627. Springer, 2017.

[2] Pavlo Burda, Tzouliano Chotza, Luca Allodi, and Nicola Zannone. Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10, 2020.

[3] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, 58(8):1158–1172, 2016.

[4] Deanna D Caputo, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1):28–38, 2013.

[5] Diksha Goel and Ankit Kumar Jain. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, 73:519–544, 2018.

[6] Anti-Phishing Working Group et al. Apwg phishing activity trends report, 2nd quarter 2012, 2012.

[7] Surbhi Gupta, Abhishek Singhal, and Akanksha Kapoor. A literature survey on social engineering attacks: Phishing attack. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pages 537–540. IEEE, 2016.

[8] Hang Hu and Gang Wang. End-to-end measurements of email spoofing attacks. In *Proceedings of the 27th USENIX Security Symposium*, pages 1095–1112, 2018.

[9] Markus Jakobsson. Two-factor inauthentication–the rise in sms phishing attacks. *Computer Fraud & Security*, 2018(6):6–8, 2018.

[10] Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4):2091–2121, 2013.

[11] Tian Lin, Daniel E Capecci, Donovan M Ellis, Harold A Rocha, Sandeep Dommaraju, Daniela S Oliveira, and Natalie C Ebner. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(5):1–28, 2019.

[12] Bimal Parmar. Protecting against spear-phishing. *Computer Fraud & Security*, 2012(1):8–11, 2012.

[13] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382, 2010.

[14] Kuldeep Singh, Palvi Aggarwal, Prashanth Rajivan, and Cleotilde Gonzalez. Training to detect phishing emails: Effects of the frequency of experienced phishing emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 63, pages 453–457. SAGE Publications Sage CA: Los Angeles, CA, 2019.

[15] Sami Smadi, Nauman Aslam, and Li Zhang. Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. *Decision Support Systems*, 107:88–102, 2018.

[16] Michelle P Steves, Kristen K Greene, and Mary F Theofanos. A phish scale: rating human phishing message detection difficulty. In *NDSS Workshop on Usable Security (USEC)*, 2019.

[17] Enis Ulqinaku, Hala Assal, Abdou AbdelRahman, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing eliminated with fido? social engineering downgrade attacks against fido protocols. In *Proceedings of the 30th USENIX Security Symposium*, pages 3811–3828, 2021.

[18] Jingguo Wang, Yuan Li, and H Raghav Rao. Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11):1, 2016.