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

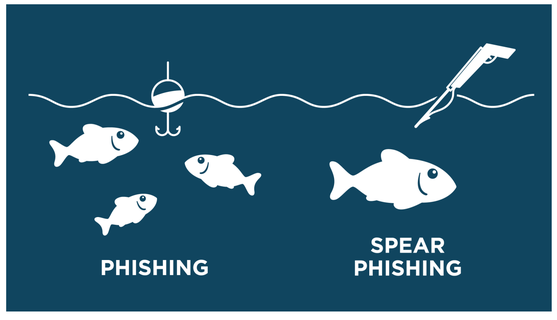
Aiping Xiong, Sian Lee, Zekun Cai, Ephraim N. Govere, Harish Kolla

College of Information Sciences and Technology, The Pennsylvania State University

Motivation

Phishing is a social engineering attack [1] that typically aims at tricking people into revealing their personal information [2], resulting in financial loss for individuals and organizations.

In **spear phishing**, emails are sent as from the receiver's friends, colleagues, or social and professional groups, exploiting human weakness [3].



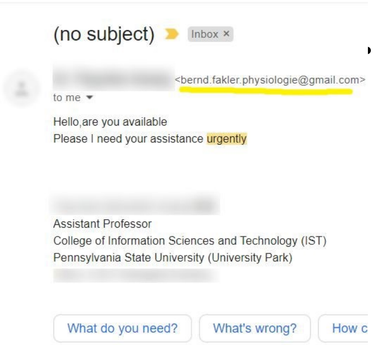
We evaluated one real-world spear phishing attack in a **university setting**, to seek answers to the following research questions:

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

Our case study includes two parts:
1) Analyzing the phishing emails;
2) Group interviews with two research groups that were targeted by the phishing attack.

Analyzing Phishing Emails & Group Interviews

The **phishing emails** received by the faculty members (n = 2) and the students (n = 4) were collected and analyzed.



The reported phishing emails came from both mobile devices and desktops. On the *desktop interface*, the student could see the name as well as the email address of the sender. With the *mobile interface*, the student could only see the name of the sender but not the email address.

- Two students who communicated with the phisher (i.e., replied to the request) used a *mobile device*.
- The attacker did not disclose the real intentions initially. However, after two rounds of email exchanges, the attacker demanded a gift card.

Semi-structured, group interviews were conducted to further investigate the factors causing the phishing scam and gain insights about how to better detect and mitigate such attacks in the future.

- Two research teams (five participants) involved in the phishing attacks were recruited for the group interviews.
  - Two faculty members (both male)
  - Three Ph.D. students (one female)
- We asked participants to share their *phishing attack experience* and then elaborate on their *email processing* on both interfaces, especially the cues that they think are important for detecting phishing emails.

Results & Discussion

The Phishing Attack Experience

- The victim student used the mobile device to communicate with the phisher.
- The victim student did not have any prior knowledge about the gift card phishing scam.
- Under initial attacks, neither the students nor the faculty members notified their IT department.

Email Processing

- Students mentioned that they paid less attention to the email address when opening an email.
- All participants used *mobile phones* to check their university emails.
- Students noticed that the mobile UI does not show email addresses but only senders' names.

Suggestions and Recommendations

- Enhancing the interface such that users can easily detect *visual discrepancies* between names and email addresses.
- Presenting *warnings or alerts* about keywords associated with phishing attacks (e.g., gift cards).
- Highlighting the importance of reporting phishing attacks *immediately*.

- Faculty members conjectured that attackers may use several linked web pages (e.g., the faculty member's homepage and the students' LinkedIn pages) to collect their team members' *private* (e.g., emails) information.
- Extra training on possible phishing attacks for *international students* who take a substantial proportion in the academic-research team and equip them with knowledge and skills to detect phishing attacks.

References

1. Gupta, S., Singhal, A., and Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *2016 International Conference on Computing, Communication and Automation* (ICCCA) (pp. 537-540). IEEE.
2. 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
3. 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