JOHANNES KEPLER
UNIVERSITY LINZ

SECURITY AWARENESS IN UNIVERSITIES
Management Paper

Target

The seminar paper on security awareness in universities targets academic institutions, particularly universities, to address the escalating cybersecurity challenges they face, especially concerning phishing attacks. The research is tailored for university stakeholders, including administrators, IT personal, faculty members, students, and general staff, who play important roles in safeguarding university systems and data. By focusing on universities, the paper aims to provide tailored solutions and recommendations to enhance security practices within the unique academic environment.

Problem Statement

The seminar paper looks at cybersecurity problems in universities, especially focusing on the common issue of phishing attacks. It points out that phishing incidents are increasing, and attackers are getting smarter, making it harder for university members to tell the difference between real and fake emails. The research aims to find out which characteristics of phishing emails are most likely to trick students and staff. By identifying these weaknesses, the paper suggests targeted educational programs and awareness campaigns to help university members recognize and stop phishing attempts. The main goal is to make universities more secure against cyber threats, especially phishing attacks, through better and proactive security measures.

Objective

The primary objective is to investigate the necessity of security concepts and awareness measures in universities to combat cyber-attacks, particularly phishing. By focusing on the challenges and opportunities within educational institutions, the goal is to identify research gaps and provide recommendations for enhancing security practices. Specifically, the research aims to analyse different phishing strategies to address vulnerabilities in universities. By conducting a comparative analysis of the traits that make phishing emails deceptive to university students and staff, the study aims to suggest educational interventions that can effectively reduce these vulnerabilities.

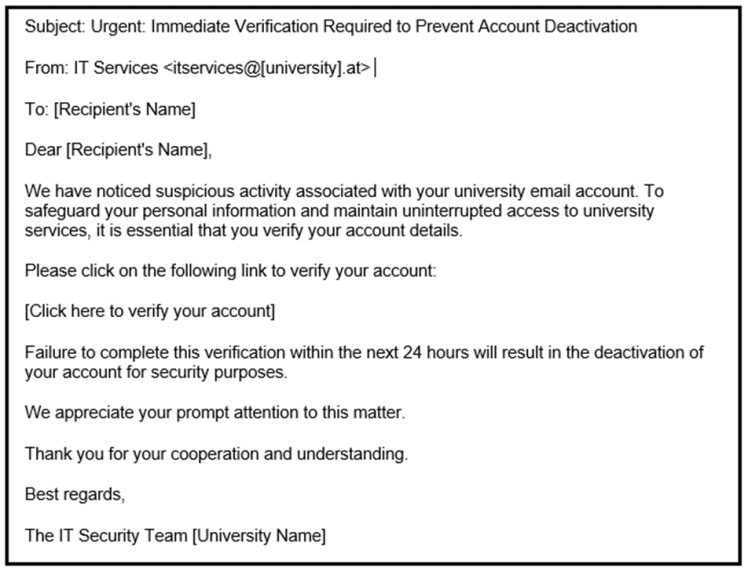
Project Overview

This project explores the critical area of security awareness in universities, concentrating specifically on addressing phishing attacks. Through a comprehensive analysis of phishing emails and the identification of key deceptive characteristics, the project seeks to develop effective educational interventions to enhance security practices. By leveraging a Design

Science Research Model and drawing insights from existing literature, the project aims to create artifacts that can aid in the recognition and prevention of phishing attacks within university settings.

Results

Through a literature analysis, the following key aspects of an effective phishing email have been identified:
Personalized greetings, such as "Dear [Recipient's Name]," make emails seem legitimate (Hook Security, 2023).
Matching the displayed link with the actual URL builds trust (Cyphere, 2022).
Warnings like "respond within 24 hours" prompt hasty decisions (BlueVoyant, 2021).
Subtle domain changes, like adding "support," often go unnoticed (Panda Security, 2024).
Phishing is more effective if recipients lack security training (Information Security Office, 2024).
Requests for personal data, framed urgently, exploit fear (Hook Security, 2023).
Using these key aspects of an effective phishing email, we created our own artifact within an university context.



Subject: Urgent: Immediate Verification Required to Prevent Account Deactivation

From: IT Services <itservices@[university].at>

To: [Recipient's Name]

Dear [Recipient's Name],

We have noticed suspicious activity associated with your university email account. To safeguard your personal information and maintain uninterrupted access to university services, it is essential that you verify your account details.

Please click on the following link to verify your account:

[Click here to verify your account]

Failure to complete this verification within the next 24 hours will result in the deactivation of your account for security purposes.

We appreciate your prompt attention to this matter.

Thank you for your cooperation and understanding.

Best regards,

The IT Security Team [University Name]

Figure 1: Univerisitized Artifact

Conclusion

Based on our results, we conducted interviews with IT security experts who remain anonymous due to data protection. In Interview 1, we validated our findings, confirming they are current and understandable. Key security measures identified include awareness training courses, multifactor authentication, and AI-based supportive systems (Interview 1, 2024).
Interview 2 revealed that Large Language Models (LLMs) enhance spear phishing by automating target research and email personalization, making detection harder (Interview 2, 2024). Historically, spear phishing required manual research (Rajivan & Gonzalez, 2018), but LLMs streamline this, increasing the threat level (Interview 2, 2024).

Bibliography

Interview 2, 2024. IT-Admin Expert

Interview 1, 2024. IT-Security Experts

BlueVoyant. (2021). *8 Devastating Phishing Attack Examples (and Prevention Tips)*. https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips

Hook Security. (2023). *Common Phishing Email Examples*. https://www.hooksecurity.co/phishing-email-examples

Rajivan, P., & Gonzalez, C. (2018). Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00135

Panda Security. (2024, March 25). *11 Types of Phishing + Prevention Tips*. Retrieved from https://www.pandasecurity.com/en/mediacenter/types-of-phishing/

Cyphere. (2022, January 10). Real-life Examples of Phishing Emails. Retrieved from https://thecyphere.com/blog/examples-of-phishing-emails/

Information Security Office, University of California, Berkeley. (n.d.). Phishing Examples Archive. Retrieved from https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive