Cybersecurity and the Human Factor

Thesis Participants:

Bagge, Viqtor. viba4115

Delsinger, Jakob. jade9062

Study's Research Context/Introduction:

Cybersecurity is a crucial part of today's business operations, with organizations' digital footprint and thus their vulnerability to attacks constantly growing (European Union Agency for Cybersecurity (ENISA), 2024; Mishra & Gochhait, 2023). Despite advanced technical protection measures, the human factor remains a critical vulnerability. Phishing, a form of social engineering, is the most common and costly threat to cybersecurity, where attackers exploit human behavior to bypass technical defenses (Bassett et al., 2022; Naqvi et al., 2023). According to Cloudflare (2023), an estimated 90% of successful cyberattacks start with a phishing email. The consequences for affected businesses can be severe, including financial losses, data breaches and reputational damage (Kothamasu et al., 2023b; Naqvi et al., 2023).

The problem is that despite significant technological advances in cybersecurity, the human factor remains a critical vulnerability. Over 74% of breaches in 2023 involved some form of human element (Verizon, 2023). Existing training programs, while helpful, are not yet sufficient to completely neutralize the human factor in phishing attacks, and improvements could be eroded within months if training is not reinforced (Wash & Cooper, 2018).

This study explores how targeted employee training can be modified to more effectively reduce organizations' susceptibility to phishing. Through a combination of quantitative analysis of simulated phishing data and qualitative semi-structured interviews, we aim to understand where existing awareness measures are succeeding, where they fall short, and how they can be refined.

Research Question (tentative):

How can targeted employee education be altered to more effectively reduce organizational susceptibility to phishing?

Consent Form:

Cybersecurity and the Human Factor

Information about the Bachelor's Thesis

-Students:

Bagge, Viqtor. viba4115

Delsinger, Jakob. jade9062

-Focus of the study:
This study investigates how targeted employee education can be altered to more effectively reduce organizational susceptibility to phishing. We will use semi-structured interviews to gain a deeper understanding of employees' experiences and wishes regarding phishing training, as well as IT workers' thoughts and strategies concerning the design and implementation of such training.

-Why we are contacting the informant:
We are contacting you as either a general employee who will be exposed to phishing training, or an employee with extensive IT-background who may have relevant knowledge of social engineering and related training. Your unique experience and perspective are crucial for understanding the human factor's role in cybersecurity and how training can be improved to address current threats like phishing.

Consent for Personal Data Processing in the Group Work To collect information for the study, we need your signed consent on this form. If you agree now, you can still withdraw your participation at any time. You do not need to provide a reason for withdrawing.

While we conduct the study, your personal data will be protected and will not be disclosed to unauthorized persons. We will store recordings and other data securely. The information we collect using audio during the first phase will promptly be converted into anonymized texts, and other material will be destroyed so that no one can identify you as a participant in the study. The consent forms will be stored securely in paper format in a remote location from the rest of the report so that they cannot be linked to what we have recorded. These papers will be kept in a locked safe by one of the group members conducting the interview. The recorded interviews will be stored on an encrypted and locked USB stick, which will be kept in a remote location from the consent forms.

The results of the study will be presented in a bachelor's thesis written in such a way that it is not possible to identify the participants. The names of the interviewees will be anonymized using a randomly assigned letter. The study follows research ethical guidelines and general laws. You can read more about this below.

Please feel free to contact the responsible student if you have any questions.

Students'/Responsible Student's Contact Information:
Email: jakob.delsinger@gmail.com
Phone: +46733592242

Informant's Consent
I have read the information about the study and consent to participate as an interviewee in the group work.

□ Yes

□ No

Informant's date and signature (not required for recorded consent):

Signature: Date:

_____ _____

Printed Name:

_____

More about Guidelines and Laws for the Study
The information, or part of the information, that we collect during the thesis may be linked to you through the recording of the interview and the transcriptions of your answers. Data that can be linked to you in this way is considered personal data according to the EU General Data Protection Regulation 2016/679 (GDPR). The reason the thesis needs to process such personal data is that the study investigates how targeted employee education can be altered to more effectively reduce organizational susceptibility to phishing, which requires a deeper understanding of individual experiences and perceptions of cybersecurity and training.

The legal basis for the processing of personal data is public interest according to Art. 6 (1e) GDPR in conjunction with the Data Protection Act (2018:218) Chapter 2, Section 2, and Chapter 1, Section 2 and Sections 7-9 of the Higher Education Act (1992:1434).

According to the EU General Data Protection Regulation and national supplementary legislation, you have the right to:

- request access to your personal data
- have your personal data rectified
- have your personal data erased
- have the processing of your personal data restricted.

Under certain circumstances, the General Data Protection Regulation and supplementary national legislation allow for exceptions to these rights. For example, the right to access data may be limited by confidentiality requirements, and the right to have data erased may be limited by archiving rules. If you wish to invoke any of these rights, please contact the responsible student using the contact details provided above. If you have general questions about the university's processing of personal data, you can contact the data protection officer at Stockholm University (dso@su.se). If you are dissatisfied with how your personal data is processed, you have the right to lodge a complaint with the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten). Information on this can be found on the authority's website (imy.se).