Analysis of the Peculiarities of Phishing Attacks on Enterprise Employees

Roman Kapusta
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
roman.kapusta@nure.ua

Karyna Horiainova
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
karyna.horiainova@nure.ua

Oleksandra Yeremenko
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandra.yeremenko@nure.ua

ABSTRACT

This work is devoted to a study of the peculiarities of phishing attacks on different classes of employees occupying positions that do not overlap with the field of information security. Particular attention will be paid to the personal qualities of average employees, and the vulnerable points of age and gender characteristics of each class of employees will be considered. The study's results will help identify specific weaknesses of employees, which may be vulnerable to a potential attacker and can be used to conduct a phishing attack on a selected group of enterprise employees.

CCS CONCEPTS

• Security and privacy • Social and professional topics

KEYWORDS

Cybersecurity, Phishing Attacks, Cybersecurity Awareness

1 Introduction

Today, cyber security is essential in forming the quality of work of almost any institution that may use information resources. Each of us is unique in our peculiarities, strengths, and weaknesses. We also differ in age, sex, culture, and gender [1-4]. All these indicators form our principles of world perception, which affect our awareness and trust level in any information we receive every second. Therefore, we get entirely different people constantly in contact with other members of society or groups with whom the same idea or cause may unite. Based on this, people continuously exchange vast information, which can be helpful exclusively for a specific group of users, such as employees of the same institution.

Employees use their computers daily and receive dozens of messages of different natures and importance. However, not only valuable information can be found in these messages, but also a planned attack. It can be based on an individual's qualities and bring significant losses to the employee and the company.

2 Human Employee Factors Associated with Phishing Attacks Creation

Phishing attacks are pretty common among malefactors. Such attacks allow cybercriminals to get a wide range of opportunities from obtaining confidential information about the victim to access rights to the entire enterprise structure. The attacker must first learn about the person or group of people to whom malicious messages will be sent to carry out a phishing attack successfully. Based on the previously gathered information, the attacker can prepare the appropriate content of the message to conduct the attack, which would most likely reflect the authenticity of the recipient's intentions and the need to fulfill the attacker's conditions. The content of the phishing message will be based on the personal factors of the person or group of persons to whom this type of attack will be used.

Particular attention should be focused on five human factors that can be key to creating a phishing message: age, gender, education, university qualifications, and IT experience. More detailed information about the specifics of using each factor is given below.

Figure 1 demonstrates the human employee factors related to cybersecurity awareness that affect a person's susceptibility to phishing attacks [1-4]. During the study, our attention was paid to the following significant factors:

1. Age expresses similar values, beliefs, and attitudes towards the specified problem of people who lived and developed simultaneously.
2. Gender reflects gender differences that cause different perceptions of technology. Women show significantly lower overall levels of risk-taking behavior than men. Therefore, their attitude to a harmful link will be much more careful than men's.
3. Education reflects the general perception of the message received by a person. The more qualitative the education of the potential victim, the more competent and lexically correct the written phishing message should be.
4. The university qualification (field of study) reflects the reader's confidence in this letter from a professional point of

view. So, for example, a person with non-technical background may overlook the danger of a letter sent from a false email address.

5. Work experience in IT reflects the general skills of a person when working with information resources and the ability to check the received message with various instruments.

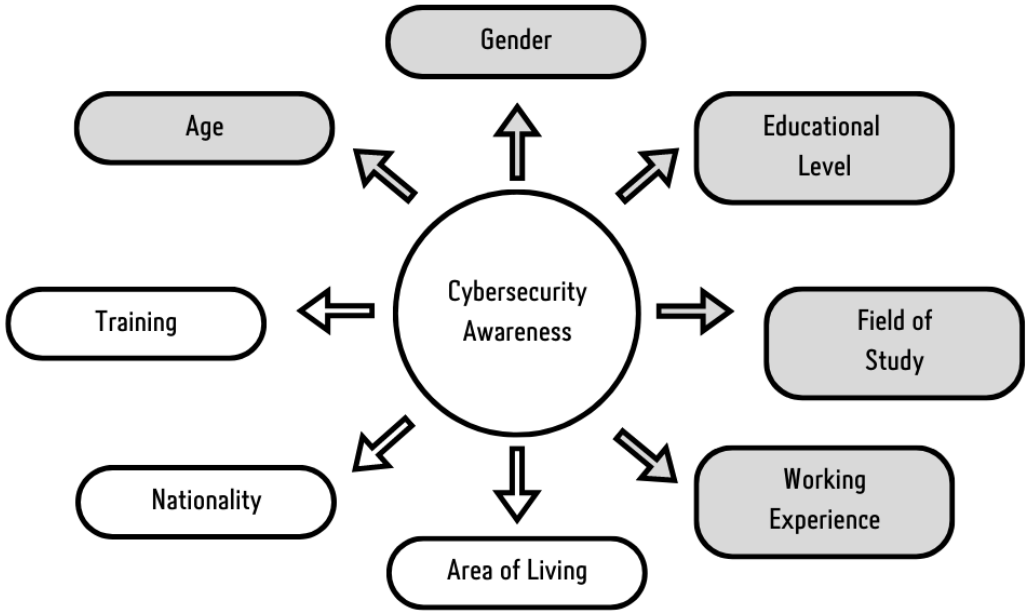

Figure 1: Employee Human Factors Associated with Phishing.

This way, we can identify the main human employee factors an attacker will consider to create a phishing message. The other indicators shown in the diagram also have a significant role in preparing a phishing attack. Still, they do not infuse the overall vector of the selection of the legend and expressions to create the message from the attacker so that they can be given less attention.

It can also be determined that the most vulnerable class of employees may be departments of an enterprise with predominantly male staff with no relationship to information resources. In addition, it should be noted that any employee, regardless of position and personal status, can become a victim of a phishing attack.

The success of an attack on trained and knowledgeable employees may depend on their psycho-emotional component, which will allow a potential attacker to choose the suitable composition of a message that will relate specifically to a person's private and personal values. An example of such a direction vector is the safety and well-being of children and everything related to them. Therefore, even experienced specialists with high cybersecurity awareness may be inclined to accept the terms of a phishing letter and fall for the attacker's hook.

Conclusion

Based on the data obtained, we can identify key recommendations that can be useful to improve information security and awareness of enterprise personnel to reduce the risks and damage from social engineering attacks:

- constantly reminding employees of the need to be more attentive when working with information resources;
- an individual interview with each employee who does not have a technical background and experience in IT;
- additional installation of special anti-phishing software and a link scanner;
- regular testing of staff to identify employees vulnerable to phishing attacks;
- staff training with a full-time psychologist to identify insiders and morally unstable employees of the institution;
- constant updating and modernization of enterprise security policies.

REFERENCES

[1] Christopher Hadnagy. 2021. *Social Engineering: The Science of Human Hacking 2nd Edition*. Gildan Audio and Blackstone Publishing.

[2] James W Williams. 2019. *Dark Psychology: The Practical Uses and Best Defenses of Psychological Warfare in Everyday Life*. Alakai Publishing LLC Paperback.

[3] Therdpong Daengsi, Phisit Pornpongtechavanich & Pongpisit Wuttidittachotti, 2022. Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Educ Inf Technol* 27 (2022), 4729-4752. DOI: https://doi.org/10.1007/s10639-021-10806-7.

[4] Ahmad Syukri Abdullah and Masnizah Mohd. Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. In *2019 International Conference on Cybersecurity (ICoCSec)*, pp. 26-31. IEEE, 2019. DOI: https://doi.org/10.1109/ICoCSec47621.2019.8970803.