

Analysis of a Phishing Experiment Article

Charles W. Pridgen

CYSE201S Cybersecurity & Social Science

Professor Matthew Umphlet

July 21, 2024

In the article, “Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality,” authors Remco Spithoven and Anthonie Drenth (2024) explain the results of their social scientific research obtained through an embedded, experimental approach on the topics of phishing attempts. They also explore the effects of voluntary e-learning to determine whether it does or does not reduce phishing victimization. For the experiment, the participants involved are unaware of it being conducted to preserve the accuracy of the data, if the participants were aware of the phishing attempts, it could result with them being on higher alert which might alter the data. Due to the nature of the experiment, ethical concerns rising from deception and a lack of consent, caused the researchers to take steps in evaluating the potential impact of the experiment as well as thoroughly debriefing each employee once it was complete (section, Ethical considerations). Conducted in the Netherlands on a Dutch municipal organization, they labeled as “Municipality X,” the goal was to answer the main question, “Which groups of employees at Municipality X run a high risk of falling victim to phishing based on an embedded experimental design and what is the learning effect of a voluntary e-learning” (section, Research questions). Along with the main question, the following 5 sub-questions were included:

1. What are the shared characteristics of Municipality X employees who clicked on the link or entered their credentials in the baseline measurement (T=1)?
2. What are the shared characteristics of Municipality X employees who clicked on the link or entered their credentials in the second measurement (T=2)?
3. Which employees at Municipality X appear to belong to the high-risk group of potential phishing victims?

4. What are the shared characteristics of employees at Municipality X have who did a voluntary microlearning on phishing?

5. What is the learning effect of the microlearning on phishing on employees at Municipality X? (section, Research Questions)

The overall experiment is comprised of two major parts, part one being two phishing emails; first email, measurement one labeled as, “t= 1,” and the second email, measurement two labeled, “t= 2.” Both emails were sent out to every employee of the municipality amounting to 1,437 accounts. Part one had no control group, therefore, the design was called a, “... *one-group-premeasurement-postmeasurement-design* [61]” (Section, Research design). According to the researchers, this part of the experiment will answer the first three sub-questions. Part one, along with the first three sub-questions, relate to the human factors of cybersecurity discussed in class, and will be further examined later in this essay. Part two was a smaller experiment where an invitation for a voluntary online microlearning was sent to a random sample group of employees. This experiment did have a control group, being the personnel who received the invitation, but did not take the online microlearning. The experimental group was the group that accepted the invitation and did take part in the online microlearning. The name for this experimental design was, “... *premeasurement-postmeasurement- control-group-design* [61],” (section, Research design).

In part one of the experiment, the baseline measurement of the first email that was sent out (t= 1) looked like the following; 64.4% (n= 926) non-clickers (people who didn’t click on the phishing link at all), 7.4% (n= 105) solely clicked (people who clicked on the phishing link, but didn’t fill in any credentials), and 28.3% (n= 406) of personnel clicked on the link, as well as filled in their credentials. Not only were the types of clickers tracked, the time of day was also accounted for. Characteristics of the employees that provide context of the victims were gender, age, number of service years, and type of employment contracts like part-time or full-time

workers (section, “Results of the baseline measurement (T= 1). As a result of the baseline test, researchers discovered that gender did not make a significant difference, whereas the other three factors of age, number of service years, and type of employment contracts did (section, Results of the baseline measurement (T= 1)).

The second measurement’s results ($t= 2$) were the following: 63.8% ($n= 917$) non-clickers, 15.5% ($n= 223$) solely clicked, and 20.7% ($n= 297$) clicked and filled in their credentials. Looking at the characteristics of the personnel for the second measurement, the researchers found that there were no significant differences, this time, between gender, age, and number of service years. What did have a significant difference in this measurement was the contract type, proving that full-timers clicked on the link and filled in their credentials more than average (section, Results of the second measurement (T= 2)).

Dissecting the overall results of part one of the experiment, sub-questions one through three can now be answered. Characteristics of age, number of service years to the Municipality, and the type of employment contracts were key characteristics of employees who either clicked on the link or filled in their credentials in the baseline measurement ($t= 1$), which answers sub-question one. Measurement two ($t= 2$) proved that the only significant shared characteristic between the employees who either clicked the link or filled in their credentials was the type of contract, or full-timers, answering sub-question two. The final answer given by the two measurements ($t= 1$ and $t= 2$) for sub-question three is, the shared characteristics of employees who run a high risk of phishing victimization are; age groups, particularly between 40-80 years old, and contract types, more specifically full-timers. Gender and service years did not have a significant difference.

As previously stated, part two of the experiment involved a small random group of employees that were sent an invitation for a voluntary e-learning on phishing. Employees who received the invite but did not take the online microlearning were considered the control group, while the employees who did take the online microlearning were the experimental group. The

idea was to see if the experimental group would demonstrate a visible learning effect due to the voluntary online microlearning. Employees who were at average or higher risk of becoming a victim of phishing mostly took the microlearning, while younger employees only employed for a short amount of time tended to ignore the microlearning, which answers sub-question 4.

Looking at the combined results of part one of the experiment ($t = 1$ and $t = 2$) and the e-learning, there was no significant difference between the control group and the experimental group. This means that the voluntary e-learning did not have a significant learning effect on the experimental group, and employees continued to be victimized, answering sub-question 5. (section, Learning effect of online microlearning).

Once the five sub-questions were answered, the researchers were able to use empirical evidence to answer the main question, “Which groups of employees at Municipality X run a high risk of falling victim to phishing based on an embedded experimental design and what is the learning effect of a voluntary e-learning?” (Remco Spithoven, Anthonie Drenth, 2024, section, Research questions). Their research shows that, “... senior and middle-aged employees run the biggest risk of becoming victims of phishing...” and are less open to doing an educational e-learning. The same goes for the young staff who have been employed with the Municipality for a short amount of time. All in all, the study indicates online microlearning is ineffective, and less voluntary educational efforts need to be implemented to make the organization more resilient to phishing attacks.

The study was tailored to this specific organization, and even though that may be the case, the results can be loosely and warily assumed for other organizations. The reason behind this is because every organization’s culture is different, thus, if you were to run this experiment on another organization the results may be quite different. With that being said, the information still holds value for society. It brings awareness to the different human factors that make people more susceptible to phishing attacks. Some human factors covered in the article include, demography, context factors, personality traits, digital literacy, and risk profiles. Age was a major

find in the study, older employees were not willing to take on a new online microlearning and were also susceptible to phishing. I believe the type of technology and learning habits developed because of the different times they were in contribute to older people becoming victims. It is important to note that another result of the experiment was younger participants with only 2-5 years of service were at higher risk of victimization as well. Another contribution that is relatively scarce in this subject, investigates context factors as an interesting and possibly significant human factor of phishing victimization. Lapses in judgement due to high stress and workloads could result in careless/accidental victimization of a phishing attempt.

Revisiting the culture of the organization, this experiment revealed that voluntary e-learning of social engineering is not effective. A more direct approach, implementing the importance of cybersecurity culture through empowering employees, and perhaps holding in-person physical trainings about the importance of cybersecurity may be more beneficial, especially for their senior to middle-management members and younger employees. As far as marginalized groups, like previously mentioned, the article covers human factors contributing to increased risk of victimization that these groups may be more susceptible too. People of lower socioeconomic class may not have the means to obtain technology, or even be exposed to e-learning designed to increase cybersecurity resiliency. Personality traits such as decreased emotional stability experienced by people of color in lower socioeconomic classes, harsh living environments, and exposed to trauma may also experience increased susceptibility to phishing or be less likely to partake in voluntary online microlearning. This may stem from the type of environment they grow up in, not having an emphasis on good cyber hygiene, and not being properly educated on the dangers of social engineering as well as the lack of emphasis on how important cybersecurity is.

Reference

Spithoven, R., & Drenth, A. (2024). Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality. *Journal of Cybersecurity*, 10(1). <https://academic.oup.com/cybersecurity/article/10/1/tyae010/7695673?searchresult=1>