DOI: 10.46793/STREAM25.259I
UDC: 159.953.5:004.832

A CASE STUDY ON STEM PROBLEM-BASED LEARNING APPROACH IN DEVELOPING COMPETENCIES FOR RECOGNIZING PHISHING EMAILS

Andrej Ignjatić*
Faculty of Organization and Informatics, University of Zagreb, Varaždin, Croatia

Diana Božić
Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia

Abstract: This research aims to explore if problem-based learning has an effect on employees' ability within an organization to detect phishing emails. Specifically, this paper tries to answer the following research question: Does the problem-based learning method in STEM affect the ability of an organization's employees to recognize potential phishing emails? The research was carried out through a case study involving a phishing simulation conducted within a Central European company. A total of 221 employees were targeted with phishing emails over two separate rounds, which lasted for four weeks. Between the rounds of the phishing campaign, problem-based learning education about phishing was provided to all employees. The research findings highlight several key points. Initially, there's been a reduction in the count of employees who clicked on links found in phishing emails. Second, there has been a decline in employees providing their user credentials to phishing websites. Lastly, the number of employees reporting suspected phishing emails to the IT department has also decreased. To our knowledge, this is the first paper that links STEM through problem-based learning with phishing.

Keywords: problem-based learning, PBL, phishing, STEM

INTRODUCTION

The STEM approach to education is designed not only to prepare learners (we use this term because it does not necessarily refer to pupils or students, it can be e.g. employees, as in this paper) for work but also to equip them with the necessary skills for living in the 21st century (Smith et al., 2022; Widya et al., 2019). The benefits of STEM education include connecting real-life problems with the content being learned (Elsayary et al., 2015). Some researchers believe that STEM education helps students develop the skills needed for

* anignjatic@student.foi.hr

problem-solving (Asghar et al., 2013; Capraro, Capraro, & Morgan, 2013; Casteldine & Chalmers, 2012; National Science Board, 2007, as cited in Elsayary et al., 2015). This can be achieved using the problem-based learning (PBL). PBL is a learner-centered education model that combines an investigative approach with the problem-solving process (Etherington, 2011, as cited in Elsayary et al., 2015), where the goal is not only to solve the problem but also to understand its origins, thereby developing students' thinking skills and integrating existing and new knowledge (Smith et al., 2022), as well as becoming an effective collaborator and increasing motivation for learning (Hmelo-Silver, 2004).

According to the Verizon Data Breach Report of 2023, 74% of all breaches in information systems involve a human element (Verizon, 2023). One of the initial activities of breaches is a phishing campaign. Phishing is the activity of faking internet websites or emails with the aim of tricking the victim into entering sensitive data for further criminal activities such as identity theft or financial crime by pretending to be another person or organization, often leaving open doors for subsequent attacks (Gavett et al., 2017; Iuga et al., 2016; Tomičić, 2023). The problem of phishing attacks is a known challenge within information security, especially since attacks are reported every year, and a decrease in the number of successful attacks in the near future is not anticipated (Iuga et al., 2016; Jampen et al., 2020), and attack vectors are becoming more sophisticated (Burda et al., 2020). Individuals, whether privately or as part of an organization, are an untapped resource for recognizing and timely responding to phishing attacks and are key to protecting the organization from potential threats. However, for individuals to successfully resist phishing attacks, they must be able to recognize potential phishing attacks, and to do so, education about them is necessary.

This paper tries to answer the following research question: Does the problem-based learning method in STEM affect the ability of an organization's employees to recognize potential phishing emails?

The rest of this paper is structured as follows. The second section presents a review of the literature and existing research. The third section shows the research methodology, including the research design and methods of data collection and analysis. The fourth section presents and comments on the obtained results. The final section summarizes the entire research.

LITERATURE REVIEW

When considering the relationship between employee information and cyber security education, there is no consensus among researchers on whether education (regardless of the form of education) has an effect on the ability of employees to recognize phishing attacks.

On one hand, it is believed that employee information and cyber security education cannot be linked to the ability to recognize phishing attacks (Broadhurst et al., 2020), partly because employees do not read the prepared materials (Caputo et al., 2014). Mandatory employee education programs do not lead to a reduction in the number of accesses to phishing websites (Gordon et al., 2019). Current methods of educating employees are not sufficient for recognizing sophisticated attacks (Burda et al., 2020). To achieve a better effect, it is necessary to educate employees several times to change their behavior (McElwee et al., 2018). However, one research has shown that conducting organized phishing campaigns in organizations, as well as educating employees about phishing, makes employees more susceptible to attacks (Lain et al., 2022).

On the other hand, researchers believe that employee education makes a difference in recognizing potential phishing messages (Carella et al., 2017; Heartfield et al., 2016). Employee education reduces the possibility of phishing messages affecting them (Alhaddad et al., 2023), thereby directly leading to a positive impact on the ability to recognize phishing email messages (Alwanain, 2021), as well as recognizing phishing websites (Alwanain, 2019), which leads to a reduction in the impact of potential phishing attacks. Also, researchers believe that targeted training on a conducted phishing campaign can be associated with a reduction in susceptibility to falling under the influence of phishing messages (McElwee et al., 2018).

After all that has been said, it is important to emphasize that in the search of relevant literature, not a single article was found that links STEM education, PBL, and phishing emails.

METHODOLOGY

The research was conducted in an organization in Central Europe that employs about 250 employees, most of whom communicate via email daily. The organization has established information and cyber security processes. The IT department regularly informs employees about phishing threats (regardless of whether they have occurred) and holds training sessions on information security at least once a year, where phishing is one of the sections covered. Each training also includes raising awareness of potential phishing attacks, given that phishing attacks are one of the frequent sources of attacks, and the employee (or user) is the most common attack vector (Burda et al., 2020). During training, IT employees explain examples of phishing messages on real cases and how to protect against them. Also, when phishing messages breach multiple email addresses within the organization, IT informs all email-using employees about the phishing attack, providing instructions on how to proceed. Additionally, when a new employee joins the organization, they undergo training to be alerted to possible information and cyber security, including phishing threats.

Furthermore, the organization has written standard operating procedures for responding to phishing attack detections. Employees can report a received phishing message, as well as information on whether they clicked on a link or filled out information, to the IT using the Helpdesk portal, email by phone, or directly to IT employees.

A case study was chosen for this research due to study employee behavior in their natural environment, i.e. without external influences (Mihelic et al., 2019).

An external contractor was engaged to conduct the campaign, with whom an NDA agreement was signed, in order to perform an information security check of the IT system using social engineering methods, i.e., phishing. Employees who do not use email and those who were informed about the campaign were excluded from the email addresses. The research design is shown in *Figure 1*.

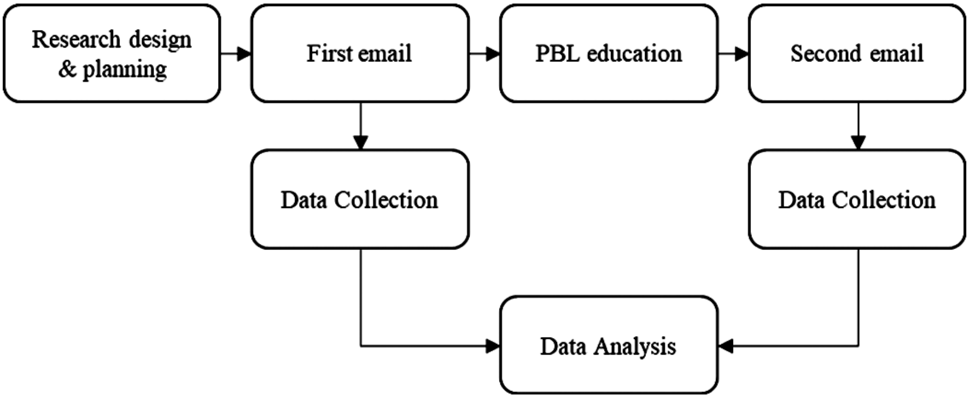

Figure 1. Research design scheme

The organization provided the external contractor with a list of 221 email addresses within the organization for the phishing campaign. From the phishing campaign, IT staff and employees who were aware that a phishing campaign would be conducted were excluded. The remaining users, apart from previously receiving training and email notifications, do not have an IT background and come from various other fields (e.g. law, economics, etc.).

Table 1. Users demographics

	Sex	*Frequency*	*Mean*	*St. Dev.*	*Min*	*Max*
Years	Female	173	43.47	8.7	25	65
	Male	48	41.48	10.25	26	64

The research and phishing campaign were divided into two rounds. The research and campaign were carried out over two working days separated by four weeks. On the first day, 120 minutes after the first notification of a phishing email was received, the IT sent a notification about potential phishing to everyone. On the second day when the second round of the phishing campaign took place, the IT sent a notification 70 minutes after receiving the first notification.

The first phishing email was sent to all employees within an hour to prevent security systems from recognizing it as phishing. The sender's address was: Notifications [Notification@organization.domain] MAILER-DAEMON@whytrustme.net, and the subject of the phishing message: "[IMPORTANT] Changes in entry rules at locations Location1 and Location2" (actual locations of the organization, which are publicly available were mentioned). The body of the phishing message stated that an unauthorized person was moving through the administrative area, even though the organization does not recognize this term, and therefore, it is necessary for all employees to be assigned PINs to enter the parking lot and organization's premises, stating a short deadline for accessing and filling out the information on the provided link.

A few days after the first round, IT organized an interactive PBL education, as a form of training, on phishing attacks. The education was not conducted *ex cathedra* but rather employees were encouraged to divide themselves into smaller groups and furthermore to identify whether a given set of emails were either phishing messages (not just in organized campaigns) or legitimate messages. Besides recognizing, employees were asked to identify clues that could determine whether the received email message was phishing or legitimate and how they could respond to such messages. The education concluded with a discussion among all employees. This education model was chosen to motivate employees to participate in the training (Elsayary et al., 2015).

The second phishing email was sent to all employees within an hour to prevent security systems from recognizing it as phishing. The sender's address of the phishing email for administrative staff was notification[notifications@eAdvertisement.hr] MAILER-DAEMON@whytrustme.net, and the subject of the phishing message: "New ergonomic chairs for Organization employees (EU-OSHA: Healthy Workplaces Good Practice Awards 2020-2022)". The body of the phishing message stated that the organization is purchasing new office chairs and it is necessary to access the link as soon as possible where the employee will choose the model of the office chair to be purchased for them.

After employees clicked on the links in both emails, a common interface opened. In the newly opened interface, employees were asked to enter their user's credentials (e.g. username and password for computer access). Users, after entering their user's credential, received a pop-up message stating that their username and password were incorrect.

According to the procedure for reporting phishing messages, employees should report any suspicious messages they received. An IT employee collected the data and updated it in a spreadsheet. After the campaign was completed, the external contractor provided the organization with relevant data in another spreadsheet. Both spreadsheets were merged into one using Microsoft Excel. Descriptive statistics were used for the statistical analysis of the data using the DATAtab software tool (DATAtab Team, 2024).

RESULTS AND DISCUSSION

The results of research will be shown in two parts. In the first part, the susceptibility of employees to phishing messages will be shown, specifically how many employees clicked and filled in the data in the requested forms. The second part will display the number of reported phishing email messages.

In the case of the first phishing email, the first employee of the organization clicked on the link two minutes after receiving the email, and the first data in the form were filled in three minutes after receiving the email. The last employee clicked on the link four days, 22 hours, and 10 minutes after receiving the email, and filled in the data four days, 22 hours, and 11 minutes after receiving the email. During this period, a total of 21 employees (9.5%) clicked on the link, and 14 of them filled in the data (6.3%). Before sending the email notification, 13 employees had clicked on the link, and 6 filled in the data; after sending the email notification, eight employees clicked on the link and filled in the data.

In the case of the second phishing email, the first employee of the organization clicked on the link seven minutes after receiving the email, and none of the employee filled out the form. The last employee clicked on the link 24 minutes after receiving the email. These are the only two employees (1.4%) who clicked on the link.

From the mentioned from above, it is evident that after attending PBL education, the number of employees who clicked on the link in the phishing email decreased, and none of the employee filled in the data on the page. However, it is important to emphasize here that users' specific credentials were not collected, only data about access and filled-in data were collected, so there is a probability that some employees filled in the form with false user credentials. This conclusion confirms the findings of previous studies (Alhaddad et al., 2023, Alwanain, 2019, Alwanain, 2021, Carella et al., 2017; Heartfield et al., 2016, McElwee et al., 2018), which highlighted the importance of employee education in recognizing phishing messages.

Table 2 shows the descriptive statistics of the time taken to recognize phishing emails before and after PBL education.

Table 2. Descriptive statistics results for reporting phishing email [in minutes]

	No.	*Mean*	*St. Dev.*	*Min*	*Q1*	*Q2*	*Q3*	*Max*
Before PBL	79	485.33	2494.79	2	4	13	43	15838
After PBL	52	253.02	1683.72	1	3	6	24.25	12158

Table 2 shows that the times needed for employees to report a potential phishing message have decreased. However, it was also observed that the number of employees who reported a potential phishing email decreased from 79 to 52, or by 34%. This can be interpreted as an increase in employee awareness and the belief that it is an obvious phishing email and that no further action is needed.

CONCLUSION

In this research, a phishing campaign was conducted targeting employees of a company. In the campaign, employees were sent two different emails in which they were asked to access phishing sites and fill in the requested data. Between the two rounds of the campaign, PBL education was conducted with employees. It concludes that PBL education has an impact on reducing the number of employees who will click on a phishing email, the number of employees who will enter the requested data, and also the number of employees who will report a potential phishing email.

This research has several limitations. Firstly, the research is geographically limited, i.e., it was conducted within one country and within one organization in that country, on a small sample size of 221 employees (users). Secondly, the research was conducted over a short period of time, meaning four weeks in total, and in only two rounds of phishing emails. Thirdly, the research did not perform a comparison between different traditional and STEM education methods. Future research is recommended to explore different STEM educational methods in comparison with traditional educational methods and their impact on developing employee competencies for recognizing phishing emails.

REFERENCES

Alhaddad, M., Mohd, M., Qamar, F., & Imam, M. (2023). Study of Student Personality Trait on Spear-Phishing Susceptibility Behavior. *International Journal of Advanced Computer Science and Applications*, 14(5): 667–678.

Alwanain, M. (2019). An Evaluation of User Awareness for the Detection of Phishing Emails. *International Journal of Advanced Computer Science and Applications*, 10(10): 323–328.

Alwanain, M. (2021). How Do Children Interact with Phishing Attacks? International Journal of Computer Science and Network Security, 21(3) : 127–133. Available at: https://doi.org/10.22937/IJCSNS.2021.21.3.17

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2020). Phishing risks in a university student community. *Trends and Issues in Crime and Criminal Justice*, 587.

Burda, P., Chotza, T., Allodi, L., & Zannone, N. (2020). Testing the effectiveness of tailored phishing techniques in industry and academia: A field experiment. *ACM International Conference Proceeding Series*. Available at: https://doi.org/10.1145/3407023.3409178

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, 12(1): 28–38. Available at: https://doi.org/10.1109/MSP.2013.106

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. In: Nie J.-Y., Obradovic Z., Suzumura T., Ghosh R., Nambiar R., Wang C., Zang H., Baeza-Yates R., Baeza-Yates R., Hu X., Kepner J., Cuzzocrea A., Tang J., & Toyoda M. (eds.), *Proc. - IEEE Int. Conf. Big Data, Big Data*. Institute of Electrical and Electronics Engineers Inc., 4458–4466. Available at: https://doi.org/10.1109/BigData.2017.8258485

DATAtab Team. (2024). DATAtab: Online Statistics Calculator. Available at: https://datatab.net/

Elsayary, A., Forawi, S., & Mansour, N. (2015). STEM education and problem-based learning. *The Routledge International Handbook of Research on Teaching Thinking*, 357–368.

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE*, 12(2). Available at: e0171620. https://doi.org/10.1371/journal.pone.0171620

Gordon, W., Wright, A., Glynn, R., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, 26(6): 547–552. Available at: https://doi.org/10.1093/jamia/ocz005

Heartfield, R., Loukas, G., & Gan, D. (2016). You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. *IEEE Access*, 4: 6910–6928. Available at: https://doi.org/10.1109/ACCESS.2016.2616285

Hmelo-Silver, C. E. (2004). Problem-Based Learning: What and How Do Students Learn? *Educational Psychology Review*, 16(3): 235–266. Available at: https://doi.org/10.1023/B:EDPR.0000034022.16470.f3

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1), 8. Available at: https://doi.org/10.1186/s13673-016-0065-2

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10(1): 33. Available at: https://doi.org/10.1186/s13673-020-00237-7

Lain, D., Kostiainen, K., & Capkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. 2022-May, 842–859. Available at: https://doi.org/10.1109/SP46214.2022.9833766

McElwee, S., Murphy, G., & Shelton, P. (2018). Influencing Outcomes and Behaviors in Simulated Phishing Exercises. *Conf Proc IEEE SOUTHEASTCON*. Available at: https://doi.org/10.1109/SECON.2018.8479109

Mihelic, A., Jevscek, M., Vrhovec, S., & Bernik, I. (2019). Testing the Human Backdoor: Organizational Response to a Phishing Campaign. *Journal of Universal Computer Science*, 25(11): 1458–1477.

Smith, K., Maynard, N., Berry, A., Stephenson, T., Spiteri, T., Corrigan, D., Mansfield, J., Ellerton, P., & Smith, T. (2022). Principles of Problem-Based Learning (PBL) in STEM Education: Using Expert Wisdom and Research to Frame Educational Practice. *Education Sciences*, 12(10), 10. Available at: https://doi.org/10.3390/educsci12100728

Tomičić, I. (2023). Social Engineering Aspects of Email Phishing: An Overview and Taxonomy. *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, 1201–1207. Available at: https://doi.org/10.23919/MIPRO57284.2023.10159691

Verizon. (2023). *2023 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/Tec2/reports/2023-data-breach-investigations-report-dbir.pdf

Widya, Rifandi, R., & Rahmi, Y. L. (2019). STEM education to fulfill the 21st century demand: A literature review. *Journal of Physics: Conference Series*, 1317(1), 012208. Available at: https://doi.org/10.1088/1742-6596/1317/1/012208