Online-Journals.org

iJAC International Journal of Advanced Corporate Learning

iJAC | eISSN: 1867-5565 | Vol. 18 No. 1 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijac.v18i1.51671

PAPER

Phishing Susceptibility Among Healthcare Workers: The Impact of Awareness, Email Type, and Location

Darin J. Challacombe[1,2](✉), **Elizabeth N. McElhiney**[2]

[1]Fort Hays State University, Hays, Kansas, United States of America

[2]Verisma Systems, Alpharetta, Georgia, United States of America

djchallacombe@fhsu.edu

ABSTRACT

While attempts by malicious actors to compromise computer systems continue to increase, there have been limited success in educating corporate learners. Most corporations must rely upon firewalls, email filtering, and other tools to prevent compromises since their employees vary in prevention reliability. Recent studies have shown limited success of anti-phishing awareness corporate learning campaigns; however, these studies have mostly utilized students or individuals aware of their participation in an experiment. The current research utilized healthcare workers. Over the course of 18 months and three experiments, we evaluated if different anti-phishing awareness learning campaigns, simulated phishing email content, or the employee's work location (remote vs. on-site) factored into their susceptibility to phishing. We found that those participants who received anti-phishing awareness interacted with the simulated phishing email less than those who didn't receive training. Overall, an average of four percent of the workers in each experiment submitted their credentials on the fraudulent website. Our results suggest any type of anti-phishing training may provide optimal results, at least regarding anti-phishing training.

KEYWORDS

phishing, awareness, compromise, medical records, health information

1 INTRODUCTION

Phishing is a significant threat to healthcare organizations. In a recently released report, Black Kite reported nearly 35% of the 2022 cyber-attacks they tracked targeted the healthcare industry [1]. Phishing represented over 50% of attack vectors reported [2]. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently announced 80% of large breaches are the results of hacking, usually instigated through phishing scams [3]. The threat is real and continues to evolve daily.

As background, phishing is considered a type of social engineering [4], [5]. Phishing relies upon targeted computer users to click on a link or submit credentials to a

Challacombe, D.J., McElhiney, E.N. (2025). Phishing Susceptibility Among Healthcare Workers: The Impact of Awareness, Email Type, and Location. *International Journal of Advanced Corporate Learning (iJAC)*, 18(1), pp. 4–15. https://doi.org/10.3991/ijac.v18i1.51671

Article submitted 2024-08-09. Revision uploaded 2024-11-26. Final acceptance 2024-12-30.

fraudulent website [6]. Its success is partially dependent upon humans' propensity for trusting others, as Malcolm Gladwell suggests [7]. Phishing emails appear to come from legitimate sources and often are convincingly real [4], [5], [6]. The target, believing the email to be true, clicks on a link and enters sensitive credentials to a fraudulent website [3], [4], [5].

Numerous studies have attempted to create a method or approach that works the best to educate users about the dangers of phishing emails. Jampen and others conducted a literature review of various anti-phishing training programs [8]. They concluded that while most researchers agree anti-phishing education is a key element, there is not an agreed upon methodology.

Given the lack of a universal standard, researchers and others have explored multiple approaches in various research settings [9], [10], [11]. Most of these methods involved the use of simulated phishing attacks [12]. That is, the learner would unsuspectingly receive a phishing email often tailored to their job or employer. The learner's interaction with the email (e.g., delete it, report it, click on the link, etc.) would be the litmus test on how phishing aware they were.

Other researchers suggest the learning should be done more traditionally and frequently in order to best train users to be more phishing aware [13]. In one such study, users were provided with a physical list of seven questions they should use to evaluate emails. While interesting, this research primarily used college participants in lab-like environments vs. real life employees or situations. It is highly doubtful that users will consistently use a risk factor guide or list to evaluate their incoming emails. There is often an ocean of difference between lab testing and real life.

Sutter and colleagues believed the current methodology of testing will always have challenges, and the best approach is to utilize robust filtering and artificial intelligence (AI) to prevent suspicious messages from even reaching the inbox [12]. Yet, even as this technology evolves, others are seeing malicious actors utilize AI to make their phishing campaigns more effective and efficient [14]. AI-enhanced phishing attacks are best protected against by AI anti-phishing technology.

Ansari et al. suggested that AI-based cybersecurity awareness training may be another tool to be used for this endeavor [15]. This is described as educating employees on how AI anti-phishing technology works. The idea is that if a user understands the "enemy", they will be better equipped to respond appropriately. Several vendors like Jericho and Hoxhunt advertise how they use AI to create customized simulated phishing emails and bite-sized training for employees [16], [17].

The impact of phishing within healthcare organizations is something not fully understood. HHS OCR documented in 2020 there were 66,509 reported breaches of protected health information (PHI) under 500 patients (a 6% increase from 2019) and 656 reported breaches of PHI in 500+ patients (a 61% increase). It is believed many of these breaches stemmed from successful phishing attacks against healthcare organizations.

The healthcare field is in the crosshairs of malicious actors. However, many in the healthcare field are reticent to be candid or transparent in how these threats impact their day-to-day operations. It is necessary for healthcare agencies to continue to have a dialogue about the issues they are facing so that other agencies can learn and improve.

Purpose. Our research purpose was to evaluate what method of training worked best in helping real medical professionals detect simulated phishing methods. We wanted to provide education on how to spot and report potential phishing attempts.

Caveat. To the authors' knowledge, no protected health information (PHI) safeguarded by our company has ever been compromised by a phishing attack.

We work diligently to ensure all employees are trained to spot and report attempted attacks. Since late 2022, we have also been utilizing AI-based anti-phishing technology to further safeguard PHI.

Ethics. This study used employees of a private health information (HI) company. All the participants were made aware of policies and procedures to monitor activity. The President of the company authorized the experiments in consultation with the authors and the Vice Presidents of Human Resources and Data/Technology. All personal identifying information (PII) was kept confidential with only the primary author having access to it.

2 EXPERIMENT 1

Multiple studies have shown value in phishing awareness training. [6] [7] There are also many companies that offer this training. For example, the SANS Institute provides a suite of just-in-time learning management system (LMS)-based training, simulated phishing tests, and remedial courses for when an individual fails a simulated phishing test. [18] Other companies, like KnowBe4, offer multiple LMS-based courses that range from engaging, interactive games to detailed security training discussing spear-phishing (viz., a phishing subset where executive and C-suite leaders are targeted by specifically customized and convincing emails) [19].

While LMS-based courses can provide training and awareness, other companies and organizations suggest periodic email reminders may be beneficial. For example, the United States' Cybersecurity and Infrastructure Security Agency (CISA) provides several free resources companies can use, including a weekly email campaign [20]. Other companies like Phish Grid provide multiple email templates to encourage cybersecurity awareness [21].

For this initial study, we wanted to combine these two methodologies (e.g., LMS-based courses and email reminders) to establish a baseline on phishing awareness effectiveness.

2.1 Method

Participants. We identified all the HI employees (N = 711) and then randomly assigned these participants into four groups.

Materials and Procedure. The experiment was spread out over a period of 30 days to appear to be random and not purposeful. The four groups received different training/awareness materials as show in Table 1.

Table 1. Number of participants in each condition for Experiment 1

Group #	N	Condition
1	180	Phishing Awareness LMS Course
2	154	Phishing Awareness LMS Course AND weekly Phishing tips emails
3	191	Weekly Phishing tips emails
4	186	Control group—no emails nor LMS course

From our random groups, we further randomized 35 participants from each of the four groups (N = 140). Fake phishing emails were sent out to all 140 participants (see Figure 1 for an example of this email).

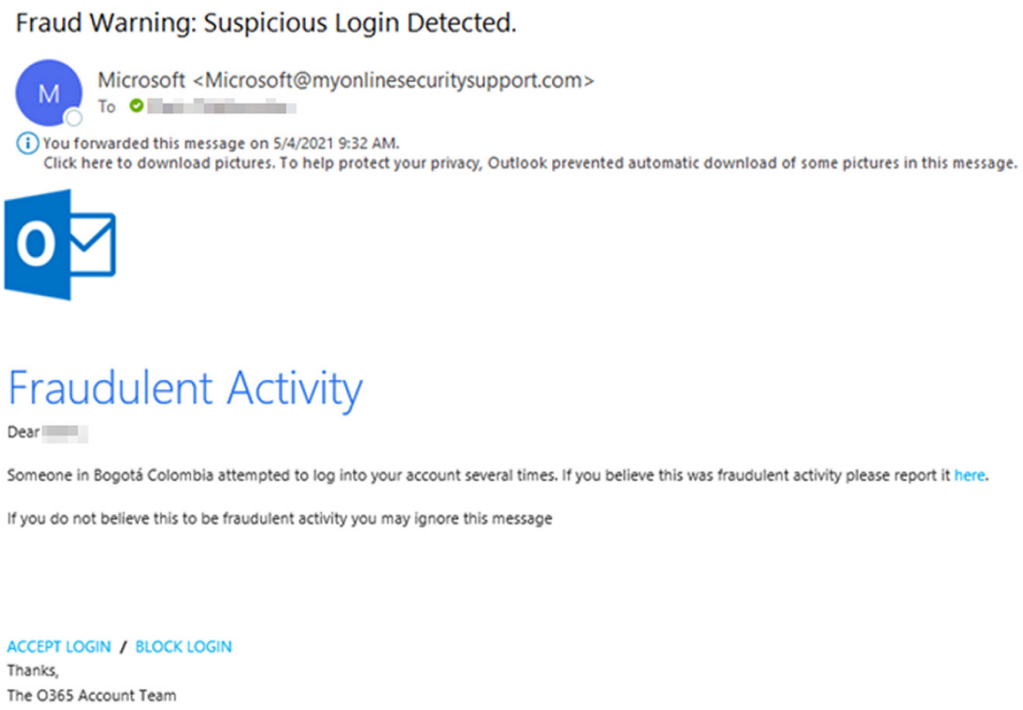

Fig. 1. Example of the fake phishing email sent out in May 2021 for Experiment 1

The phishing test system allowed us to record the participant's interaction with the email in one of four responses: Received, opened, clicked link, or submitted password data.

2.2 Results

Of the 140 individuals who received the phishing email, 18 reported it through the established processes for reporting Phishing emails (e.g., forwarding the email to the IT/Security department). Table 2 shows a breakdown of who opened the email, clicked on the link, or submitted data. A total of 5% of participants submitted data.

Table 2. Number and percentage of participant interactions for Experiment 1

Group	No Action		Email Opened		Link Clicked		Submitted Data	
	N	%	N	%	N	%	N	%
1	25	71.4	8	22.9	2	5.7	0	0
2	24	68.6	5	14.3	5	14.3	1	2.9
3	23	65.7	10	28.6	2	5.7	0	0
4	24	68.6	4	11.4	1	2.9	6	17.1

We conducted a χ^2 Test for Independence to investigate the association between the Experimental Group and Simulated Phishing Test Interaction. Results revealed a statistically significant association between these two variables, $\chi^2(9, N = 140) = 21.197$, $p = .012$. These results are most evident in the bar chart (see Figure 2).

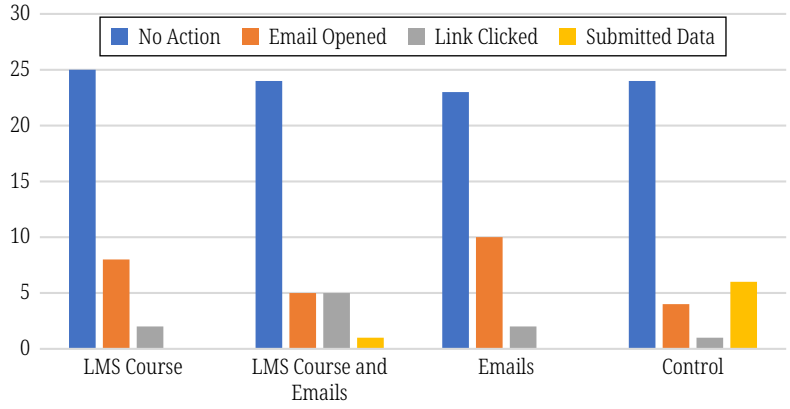

Fig. 2. Bar chart graphically showing the results of Experiment 1

2.3 Discussion

The Control Group (e.g., those who did not receive training or emails) interacted with the simulated phishing email more than the three other groups. That group also had the greatest number of people who submitted data onto the phishing form. The next worst group was the group that received both the LMS Phishing Awareness course AND the weekly emails. We found this result interesting as intuition would lead us to believe that more training would equal less susceptibility.

In the corporate learning environment, employees must balance their workload with all their other administrative requirements. The LMS Phishing Awareness course was designed to allow an employee to complete it within about fifteen minutes. However, this also required the employee to log into their Human Resources (HR) system to access the course. This often resulted in employees reaching out to have their credentials reset, which may have created a negative affect for the employee prior to them completing the course. It is possible all those factors may have reduced the LMS course's effectiveness.

This does not support that conclusion. Both the LMS Phishing Awareness course only and the weekly emails only groups did about the same.

3 EXPERIMENT 2

Roughly thirteen months following Experiment 1, we conducted a follow-up study. We turned on a feature within our email program (Microsoft Outlook) to tag emails that originated from outside the company with a notice. We believed this tag would be sufficient to prompt employees to be more aware of potential phishing emails. Together with our IT team, we wanted to test this theory by conducting a simulated phishing campaign.

3.1 Method

Participants. We identified all the HI employees (N = 826) and randomly assigned these participants into three groups.

Materials and Procedure. Like Experiment 1, we spread out the simulated phishing emails over the course of four weeks. No specific education was

provided before beginning the experiment. The participants received one of three simulated phishing emails (see Table 3).

Table 3. Number of participants in each condition for Experiment 2

Group #	N	Condition
1	349	Office 365 Suspension Notice campaign
2	348	Microsoft Teams Message Available campaign
3	129	OneDrive-Changes to OneDrive campaign

We decided to have Group 3 be the smallest since the usage of Microsoft OneDrive was relatively limited to management. As with Experiment 1, the phishing test system allowed us to record the participant's interaction with the email: Received, opened, clicked ink, or submitted password data.

3.2 Results

Both Groups 1 and 2 had similar percentages of participants coded as "no action". Group 1 saw an overall more interaction with the email along with more participants who submitted data. Table 4 shows a breakdown of the results. A total of 5% of participants submitted data.

Table 4. Number and percentage of participant interactions in Experiment 2

Group	No Action		Opened Email		Clicked Link		Submitted Data	
	N	%	N	%	N	%	N	%
1	266	76.2	53	15.2	10	2.9	20	5.7
2	269	77.3	40	11.5	34	9.8	5	1.4
3	104	80.6	16	12.4	4	3.1	5	3.9

As with Experiment 1, we conducted a χ^2 Test for Independence to investigate the association between the Email Type and Simulated Phishing Test Interaction. Results revealed a statistically significant association between these two variables, $\chi^2(6, N = 826) = 27.208, p < .001$. These results are most evident in the bar chart (see Figure 3).

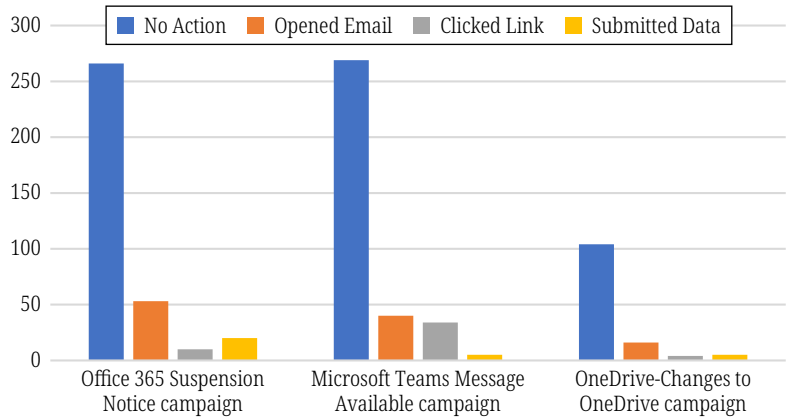

Fig. 3. Bar chart graphically showing the results of Experiment 2

We further wanted to examine the three email messages, four response types, and the participant location (e.g., remote vs. on-site). Therefore, we conducted a multinominal logistic regression analysis to examine the relationship between the email type and participant location and the interaction type (e.g., no action; opened email; etc.) with the category of "submitted data" as our reference category. The model was statistically significant, $\chi^2(9) = 28.034$, $p < .001$, suggesting the predictors contributed to the model. For instance, the email type "Microsoft Teams Message" was found to significantly increase the odds of being in the "clicked link" condition compared to the "submitted data" category, $B = 2.140$, $p = .009$, Exp(B) = 8.501.

3.3 Discussion

As we predicted, we did see a significant relationship between the email type and the interaction. We saw the email regarding the Office 365 Suspension (Group 1) had slightly more activity than the Microsoft Teams Message Available (Group 2). The email regarding OneDrive (Group 3) had the least activity, which is likelier since it had the smallest number of participants assigned to this condition. The multinominal logistic regression saw a significant interaction between those participants who received the Microsoft Teams email and those who clicked on the link. These results show the greater visibility of both the Office 365 and Teams vs. OneDrive.

This result is further interesting since, at the time, it had been several years since the company started using Microsoft Teams and Office 365 (circa mid-2019). What may explain this is that the company had acquired three other smaller companies a few months prior, and there was a big push within the organization to ensure we were all integrated on using both applications.

4 EXPERIMENT 3

The organization used for testing has a mix of employees located on-site at client facilities and others who are working remotely. The remote employees are provided with company-owned computers with special security settings for work usage only. For this testing, we decided to evaluate if an employee with a primarily on-site vs. remote status would interact with the results.

We hypothesized that employees working remotely would interact less with the phishing emails because they likely had less environmental stress and could thoroughly review the email before interacting with it. Conversely, those employees working on a client location were likely under time constraints with handling incoming phone calls, speaking with patients, processing requests, and other duties as assigned. This likely meant they would not be able to triage the email as thoroughly as the remote staff.

4.1 Method

Participants. As before, we identified all the HIM employees (N = 880). Of those, 507 worked all or most of their time remotely and 375 worked all or most of the time on-site. Using Excel's random number generator, we separated out both sets of participants (remote vs. on-site) into two groups: Control (N = 434) and Experimental (N = 440).

Materials and Procedure. For those in the Experimental group, we sent daily phishing reminder emails (see Figure 4) for the week preceding the actual phishing test. Those in the Experimental group did not receive any specific phishing reminder emails that week.

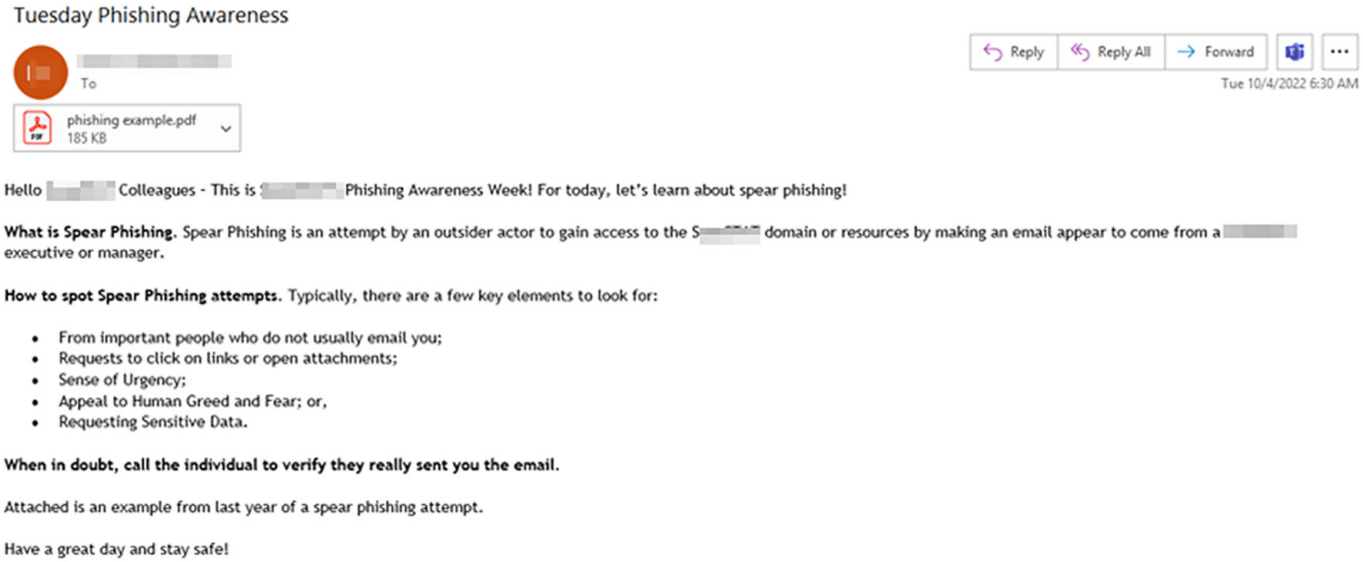

Fig. 4. Example of a phishing awareness email sent out to participants in the experimental group for Experiment 3

The follow-up week, we sent out a phishing email to all participants (see Figure 5). The phishing test system allowed us to record the participant's interaction with the email: Received, opened, clicked ink, or submitted password data. If the participant submitted password data, they were directed to a short (2 minute) video informing them that this was a test and that they need to be more careful in the future.

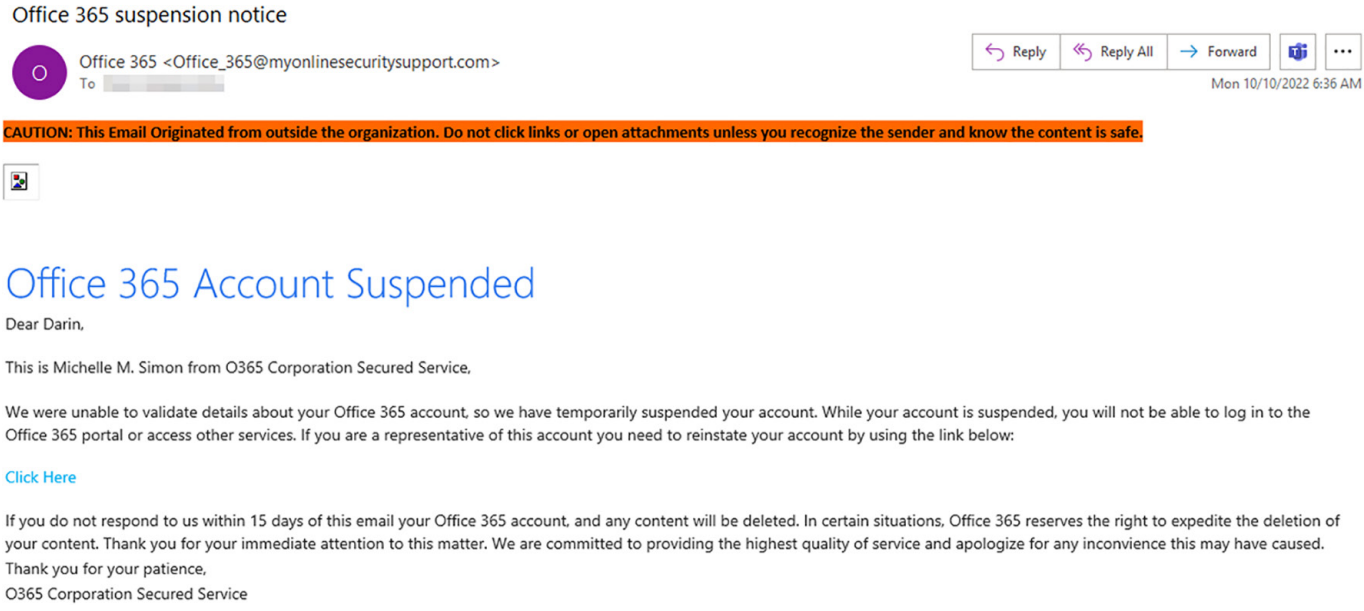

Fig. 5. Example of the simulated phishing email sent to Experiment 3 participants

4.2 Results

Among the two groups, 28 people interacted with email by clicking the link or submitting password data. Eighteen (18) of these were from remote participants and 10 were from on-site participants. See Table 5 for a breakdown of the data. A total of 2.1% of participants submitted data.

Table 5. Number and percentage of participant interactions for Experiment 3

	Location	Total	No Action		Opened Email		Clicked Link		Submitted Data	
			N	%	N	%	N	%	N	%
Control	Remote	251	202	80.5	36	14.3	4	1.6	9	3.6
	On-Site	183	148	80.9	30	16.4	2	1.1	3	1.6
Experimental	Remote	251	208	82.9	38	15.1	2	0.8	3	1.2
	On-Site	189	158	83.6	26	16.5	2	1.1	3	1.6
	Total	874	716	81.9	130	14.9	10	1.1	18	2.1

We started by evaluating the interaction between the group (e.g., control vs. experimental) and the interaction using a χ^2 Test for Independence. Results did not reveal a statistically significant association between these two variables, $\chi^2(3, N = 874) = 2.747$, $p = .432$. These results are most evident in the bar chart (see Figure 6). We also evaluated the interaction between location (e.g., remote vs. on-site) and the interaction using a χ^2 Test for Independence. Results did not reveal a statistically significant association between these two variables, $\chi^2(3, N = 874) = .677$, $p = .879$

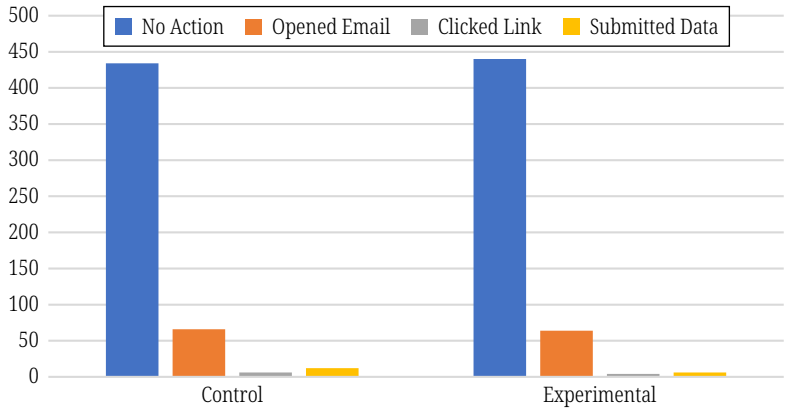

Fig. 6. Bar chart graphically showing the results of Experiment 3

We conducted a multinomial logistic regression to examine the relationship between the groups and location (e.g., remote vs. on-site) and the email interaction. The overall model was not statistically significant, $\chi^2(9) = 5.170$, $p = .819$, indicating that the predictors did not significantly improve the model compared to the null model.

Furthermore, the goodness-of-fit statistics, including the Pearson χ^2 and Deviance, suggested a poor fit of the model to the data, with values below 1 (e.g., .000 and .000, respectively), indicating that the model does not adequately explain the variance in the outcome categories. The pseudo R-squared values (viz., Cox & Snell: .006;

Nagelkerke: .009; McFadden: .005) also indicated that the model explained a minimal amount of variance in the outcome.

Because the predictors did not yield statistically significant coefficients, with all p-values exceeding the threshold of .05, it can be concluded that there is insufficient evidence to suggest that the predictors are associated with the outcome categories.

4.3 Discussion

Our results indicate that our hypothesis regarding remote vs. on-site participants was not supported. Participants in both locations interacted with the simulated phishing emails about the same. However, when evaluating the difference between the control and experimental groups, the latter had fewer potentially negative interactions (i.e., the experimental group clicked on the link or submitted data less than the control group), even though the result was not significant. Sending anti-phishing reminder emails did appear to have an impact on behavior.

5 OVERALL DISCUSSION

The healthcare field is a prime target for malicious actors. The goal of the current research was to evaluate how medical professionals would respond to phishing attacks after various vectors of education. We believe this is the first study to utilize actual medical professionals vs. students. In both Experiment 1 and 3, we provided anti-phishing awareness training in the forms of reminder emails or LMS courses. Both experimental results showed those who received any training interacted with the simulated phishing emails less than those in the control group. This study showed that any training resulted in less susceptibility.

Sadly, while most participants in all three conditions did not interact with the emails, an average of 4% of participants submitted data over the three studies. Any submission of data would represent a compromise of the participant's computer and likely the entire network. In our eyes, any submission of data constitutes a complete failure.

Humans are often programmed to believe others to a fault [7]. This study demonstrates this concept. Even medical professionals—individuals trained at least annually on security awareness—are susceptible to phishing attempts. While known already (based on all the reported breaches by other organizations), this study shows to what degree this potential is possible.

5.1 Limitations

While the simulated phishing tool is robust, there is a limitation on its reporting. For example, it will report "no interaction" if the participant does download the embedded graphic images that are part of the email. This means that it is possible more participants in all three experiments opened the email than was reported.

Another limitation is potential that participants may have become suspicious or been tipped off about the simulated phishing attacks. With any repeated measures study, there is an inherent conditioning that takes place. While there were changes in the employees over time, an estimated 600 participated in all three studies, whether they knew it or not.

5.2 Further Study

There are many companies that provide anti-phishing awareness training. The current methodology and approach could be useful in allowing these companies to test their training out on real healthcare professionals. We would recommend a comparative study (similar to Experiment 1) that uses materials from different companies to ascertain effectiveness.

Another suggestion would be to conduct a similar study using healthcare participants who are required to only work on-site. Coupling this with a stress measure may also yield interesting results.

6 REFERENCES

[1] Black Kite, "2023 Third Party Breach Report: Trends, Shifts, and Lessons Learned from 2022," 2023. [Online]. Available: https://blackkite.com/wp-content/uploads/2023/01/third-party-breach-report-2023.pdf

[2] CircleID Reporter, "Healthcare Industry Was the Most Common Victim of Third-Party Breaches in 2022." Accessed: Feb. 13, 2023. [Online]. Available: https://circleid.com/posts/20230208-healthcare-industry-was-the-most-common-victim-of-third-party-breaches-in-2022

[3] J. Baumann, "Health Industry Pressed to Protect Data as Cyberattacks Spread." Accessed: Oct. 30, 2024. [Online]. Available: https://news.bloomberglaw.com/pharma-and-life-sciences/health-industry-pressed-to-protect-data-as-cyberattacks-spread

[4] Federal Trade Commission, "Phishing Scams," Federal Trade Commission. Accessed: Oct. 30, 2024. [Online]. Available: https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams

[5] R. W. Gehl and S. T. Lawson, *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication*. Cambridge: The MIT Press, 2022. https://doi.org/10.7551/mitpress/12984.001.0001

[6] Check Point, "Social Engineering vs Phishing," Check Point Software. Accessed: Oct. 30, 2024. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/social-engineering-attacks/social-engineering-vs-phishing/

[7] O. C. Tanner, "Malcolm Gladwell on Trust in Life and Work." Accessed: Oct. 30, 2024. [Online]. Available: https://www.octanner.com/podcasts/trust-with-malcolm-gladwell

[8] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: Towards an effective anti-phishing training. A comparative literature review," *Hum. Cent. Comput. Inf. Sci.*, vol. 10, no. 1, p. 33, 2020. https://doi.org/10.1186/s13673-020-00237-7

[9] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Hum. Cent. Comput. Inf. Sci.*, vol. 6, no. 1, p. 8, 2016. https://doi.org/10.1186/s13673-016-0065-2

[10] P. Kumaraguru *et al.*, "School of phish: A real-word evaluation of anti-phishing training," in *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*, Association for Computing Machinery, New York, NY, USA, 2009, pp. 1–12. https://doi.org/10.1145/1572532.1572536

[11] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta Georgia USA: ACM, 2010, pp. 373–382. https://doi.org/10.1145/1753326.1753383

[12] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception," *IEEE Access*, vol. 10, pp. 100540–100565, 2022. https://doi.org/10.1109/ACCESS.2022.3207272

[13] D. M. Sarno, R. McPherson, and M. B. Neider, "Is the key to phishing training persistence?: Developing a novel persistent intervention," *Journal of Experimental Psychology: Applied*, vol. 28, no. 1, pp. 85–99, 2022. https://doi.org/10.1037/xap0000410.supp

[14] Benishti, "Prepare For The AI Phishing Onslaught." Accessed: Oct. 30, 2024. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2023/03/03/prepare-for-the-ai-phishing-onslaught/

[15] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of phishing attacks using AI-based cybersecurity awareness training," *International Journal of Smart Sensor and Adhoc Network*, pp. 61–72, 2022. https://doi.org/10.47893/IJSSAN.2022.1221

[16] Hoxhunt, "Reduce the Risk of Breaches with Phishing Training | Hoxhunt." Accessed: Oct. 31, 2024. [Online]. Available: https://hoxhunt.com/product/phishing-training

[17] Jericho Security, "Jericho Security | Anti-Phishing Training." Accessed: Oct. 31, 2024. [Online]. Available: https://www.jerichosecurity.com/solutions/anti-phishing-training

[18] SANS Institute, "Phishing Awareness Training | SANS Security Awareness." Accessed: Oct. 31, 2024. [Online]. Available: https://www.sans.org/security-awareness-training/products/security-awareness-solutions/phishing/

[19] KnowBe4, "KnowBe4 Security Awareness Training | KnowBe4." Accessed: Oct. 31, 2024. [Online]. Available: https://www.knowbe4.com/products/security-awareness-training

[20] CISA, "Teach Employees to Avoid Phishing | CISA." Accessed: Oct. 31, 2024. [Online]. Available: https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing

[21] Phish Grid, "8 Best Phishing Awareness Email To Employees – PhishGrid." Accessed: Oct. 31, 2024. [Online]. Available: https://phishgrid.com/blog/phishing-awareness-email-to-employees/

7 AUTHORS

Darin J. Challacombe is with the Fort Hays State University, Hays, Kansas, United States of America; Verisma Systems, Alpharetta, Georgia, United States of America (E-mail: djchallacombe@fhsu.edu).

Elizabeth N. McElhiney is with the Verisma Systems, Alpharetta, Georgia, United States of America.