ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1136

Strengthening Cybersecurity Awareness: The Role of Knowbe4's Automated Phishing Contests in Employee Training

Prity Choudhary[1]
University of Tampa, Florida, USA

Shanmuka Garaga[2]
Visvesvaraya Technological University, India

Vikas Jalan[3]
University of Pune, Pune, India

Rahul Choudhary[4]
University of Pune, Pune, India

Abstract Phishing attacks remain one of the most pervasive cybersecurity threats facing organizations today, often resulting in data breaches and significant financial losses due to human error. This study investigates the effectiveness of using automated phishing contests, facilitated through the KnowBe4 platform, to enhance cybersecurity awareness among employees within a small organization. The research was conducted in two phases: an initial phishing simulation where employees were not forewarned or trained and targeted cybersecurity training focused on identifying phishing emails. A second phishing contest, after a five-month interval, was utilized to measure the effectiveness of the training intervention.

The data from both challenges were analyzed to measure changes in employee behavior, concentrating on detection rates and response patterns. Results indicated a noticeable improvement in employees' ability to recognize phishing emails after training, though some gaps persisted, particularly with more sophisticated phishing templates. The study also explored which phishing emails were most challenging to detect and examined factors influencing employee engagement in these simulations. These findings highlight the value of structured phishing awareness training in strengthening an organization's cybersecurity defenses and provide actionable insights for designing more effective cybersecurity education programs.

Keywords: *Cybersecurity Awareness, Phishing Attacks, Employee Training, Knowbe4, Simulation, Cyber Threat Prevention, Security.*

I. INTRODUCTION

In today's digital world, phishing has emerged as one of the most continuing cybersecurity threats, targeting individuals and organizations. This is a malicious practice where tactics are executed to fool users into disclosing sensitive information, like passwords or financial information. Most of these types of attacks are carried out via emails or messages (He & Zhang, 2019). Major cyberattacks often remind us that vulnerabilities exist in our digital environment. The 2013 breach in Target data led to the loss of 40 million credit and debit card numbers, which amassed millions of customers to compensate for huge losses to the retailer financially and reputationally (De Bona & Paci, 2020). Similarly, the 2017 breach in Equifax exposed the personal details of approximately 147 million individuals, which had devastating consequences due to a lack of cybersecurity measures (Shahbaznezhad et al., 2021). More recently, the SolarWinds attack in 2020 has shown how such cyber-attacks can infiltrate major corporations and government agencies, affecting security at a national level (Alshaikh & Adamson, 2021).

These incidents define the need for corporations to instill a culture of cybersecurity awareness. As phishing attacks become more realistic, employees often find themselves at the frontline of defense against such threats. By enhancing cybersecurity awareness, organizations can better protect themselves against cyberattacks and safeguard their sensitive information. Much of that defense involves training employees since human error is still among the weakest links in cybersecurity attacks. Educating employees about the dangers of phishing and training them to recognize and respond to threats is critical to keeping organization assets and data safe (Pouraimis et al., 2019).

In the context of spreading cybersecurity awareness amongst employees, KnowBe4 is one of the leading players. It offers automated phishing contests and comprehensive training modules, which can be used to enhance employees' vigilance against phishing attempts. With its innovativeness, KnowBe4 is the linchpin in helping an organization fortify its cybersecurity posture and contribute to making the digital world a safer place. The company was founded in 2010 by Stu Sjouwerman and has since emerged as a leader in helping organizations fight against the continuously evolving threat of cybercrime. With a mission to educate and empower employees, KnowBe4 focuses on transforming the human element of security into a strong defense against phishing and other cyber threats (Daengsi et al., 2021).

KnowBe4's platform is designed to provide organizations with comprehensive tools for training employees and simulating phishing attacks. The platform is very easy to use and designed for administrators to manage training programs and track employee progress with ease. With this platform, an organization can conduct realistic phishing simulations to test employee awareness and readiness. These customizable simulations allow companies to tailor the scenarios to their specific needs (Grassegger & Nedbal, 2021). KnowBe4 provides training content in volumes hosted on interactive modules, videos, and quizzes about various topics related to cybersecurity awareness. It provides them with interesting insights into the work and reinforces their knowledge of potential threats. Reporting and analytics within the platform are available to show the employee performance of simulations and training. Administrators can easily identify areas where employees may need additional support or training. Aside from awareness, KnowBe4 provides them with the capability to respond appropriately in instances of phishing, such as reporting suspicious emails and identifying certain red flags. The platform is designed to continuously update its database with state-of-the-art phishing trends and tactics. It thus keeps employees informed about relevant and timely information needed to protect against emerging threats (Chatchalermpun & Daengsi, 2021). Automation of scheduling phishing simulations and training sessions contributes to less need for constant manual intervention by administrators. To take it to the next level, KnowBe4 has designed its training to include gamification through leaderboards and rewards for the most cybersecurity-aware employees.

In a nutshell, KnowBe4 is an incredibly powerful solution for organizations that properly train employees and use real-world phishing scenarios. KnowBe4 is instrumental in establishing a knowledgeable and alert culture that will likely reduce the risks of phishing and other cyber threats (Hijji & Alam, 2022).

➢ *Purpose of Study*

This study evaluates the effectiveness of automated phishing contests facilitated through KnowBe4's cybersecurity training platform in enhancing employee awareness and reducing susceptibility to phishing attacks within an organizational setting. The present study instead investigates how employee performance in correctly identifying phishing emails has changed following targeted training and seeks to contribute to an understanding of how structured cybersecurity training programs may shape employee behavior. The findings of this research would make the best practices for comprehensive cybersecurity awareness initiatives in organizational defense against phishing threats possible.

➢ *Key Questions Answered by this Study:*

- To what extent does targeted cybersecurity training using automated phishing contests reduce employee susceptibility to attacks over time?
- Which specific type of phishing emails does the employee have the most difficult time identifying, even after training, and where is awareness lacking?
- In a bid to answer these questions, the study gives evidence-based recommendations that may be adopted by organizations to advance cybersecurity training effectively in reducing the risks of phishing-related data breaches.

➢ *Problem Statement*

Phishing attacks remain one of the most prevalent and damaging cyber threats organizations face today. Despite ongoing efforts to educate employees about cybersecurity, many organizations experience data breaches due to human error and a lack of awareness regarding phishing tactics. Employees are often the first line of defense against such attacks, yet they frequently fall victim to cleverly disguised phishing emails, leading to significant financial and reputational losses (Sabillon, 2020).

While automated phishing simulation platforms, like KnowBe4, offer organizations tools to test and train their workforce, there is limited empirical evidence on the effectiveness of these tools in changing employee behavior and reducing susceptibility to phishing over time. This study addresses this gap by investigating whether participation in automated phishing contests and targeted training can improve employees' ability to detect phishing attempts. By assessing the impact of these training interventions, this research seeks to provide actionable insights for organizations looking to enhance their cybersecurity posture through employee education and awareness.

II. METHODOLOGY

➢ *Data Collection*

The research study applied a quantitative approach to explore the effectiveness of automated phishing contests in enhancing cybersecurity awareness among organizational employees. The data was collected through controlled phishing simulations using KnowBe4's automated phishing contest platform. The study was conducted within a small organization with approximately 90 salaried employees.

- *The Data Collection Process Was Carried Out in Two Distinct Phases:*

Pre-Training Test: In the initial phase, employees went through a phishing competition without notice or training on the subject. The object of this assessment was to establish a baseline measure of employees' susceptibility to phishing attacks. KnowBe4's platform was used to send out 10 phishing emails to all participants, utilizing templates provided by the platform to mimic real-world phishing scenarios. Employees were monitored to see whether they would identify or fall victim to these phishing attempts. Of the 90 employees, 56.72% actively responded to all phishing emails, while 43.28% did not engage with all 10 emails. The results in this phase were downloaded as an Excel file for analysis.

Post-Training Test: Subsequent to the initial testing, employees received specific training in identifying phishing emails, with an emphasis on the main precursors, such as links, sender addresses, and odd requests.

After five months, the phishing contest was repeated on the same platform using exactly the same templates to compare pre-training versus post-training performances in support of the intervention's effectiveness. Again, data was extracted in Excel format from KnowBe4's platform for further analysis.

It included the collected data on employee response for each phishing email, whether it was identified as phishing or they fell victim to the simulated attack. Other than that, the non-participation of some employees would also be noted to ensure that the analysis is thorough.

➢ *Data Analysis*

The analytics of data were informed by the comparison of performance of employees before and after the training invention in identifying phishing emails. This involved structuring and analyzing the data from the KnowBe4 platform using Excel and reviewing the performance of the cybersecurity training program.

- *Descriptive Statistics:*

The raw data from both rounds of phishing contests were imported into Excel for analysis. Descriptive statistics were calculated for both the pre-training and post-training assessments, such as the number of successful phishing detections, click-through rates, and the percentage of employees who fell for each phishing attempt. The analysis focused on identifying trends and patterns in employee behavior regarding phishing awareness.

- *Comparison of Pre- and Post-Training Results:*

To evaluate the impact of cybersecurity training, a comparative analysis was conducted between the results of the first and second phishing contests. Key performance metrics were compared, such as the rate of phishing email detection and the reduction in the number of employees who fell for phishing attempts. The difference in performance metrics before and after the training intervention was used to measure the effectiveness of the training program.

- *Gap Analysis:*

This was part of the analysis that attempted to ascertain very specific areas where employees continued to fail in recognizing phishing attempts even after training. This entailed an examination of the types of phishing emails that resulted in the highest failure rates in both rounds. The results of this analysis were used to refine and enhance future training sessions to address these specific knowledge gaps.

- *Participation Analysis:*

Special attention was given to the participation rates, particularly among the 8 employees who did not engage with all the phishing emails. This allowed the understanding of the impact of non-participation in training on the overall effectiveness of the training and whether there was an association between non-participation and cybersecurity awareness levels.

This study provided insight into automated phishing contests and their role in strengthening cybersecurity awareness by the employees through comparisons between pre-and post-training data. The results of this analysis were used to develop recommendations for optimizing cybersecurity training programs in similar organizational contexts.

III. RESULTS/FINDINGS

It was observed that the employees paid more attention to phishing emails after the training than before. Also, the participation rate increased from pre-training to post-training rounds. Furthermore, the rate of reporting phishing emails also increased as employees became more aware of the importance of reporting phishing emails.

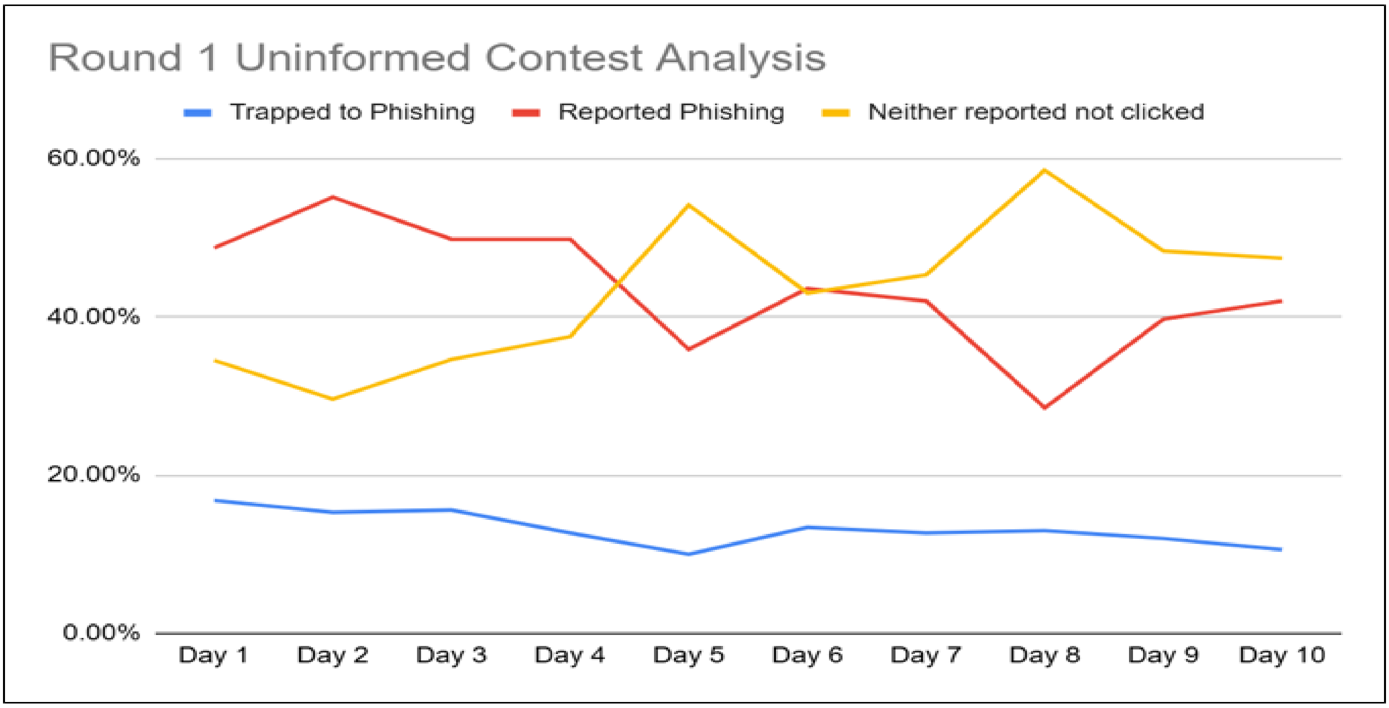


Fig 1 The Illustration Shows the Results of An Uninformed Phishing Contest

As illustrated in Figure 1, the average participation rate among employees was 56.72%. Within this group, 13.21% of participants were "trapped" by the phishing emails, indicating they clicked on the malicious links embedded in the messages. In contrast, 43.51% of the employees correctly detected and reported the phishing emails using the "Phish Alert" button. A significant portion of 43.28%, however, did not respond at all to the email, neither reporting nor clicking any link from the phishing emails. No response happened, though, which creates some gaps in engagement or awareness that may need further attention.

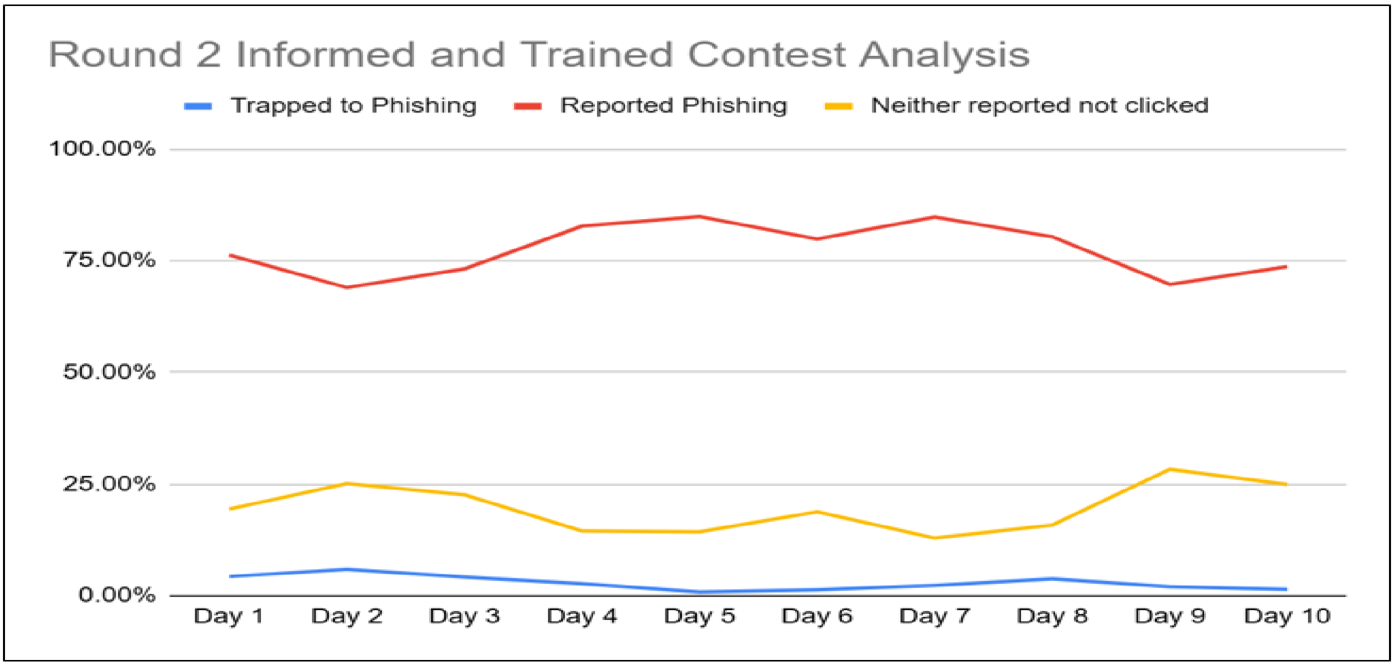
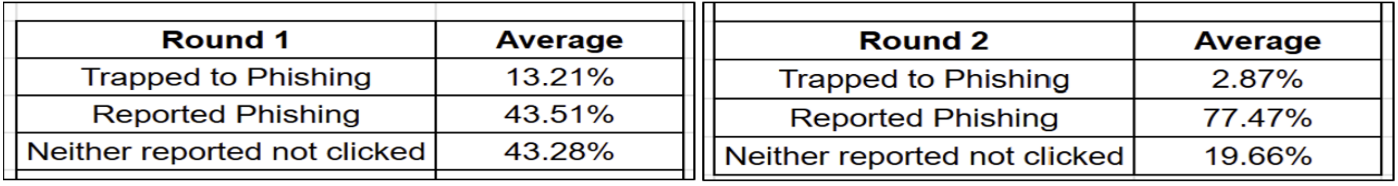


Fig 2 The Illustration Shows the Results of An Informed Phishing Contest

Round 2 of the phishing contests was conducted after analyzing the results from Round 1 and providing targeted training to employees. Figure 2 shows a significant decrease in the number of employees who fell for phishing attempts, with the "trapped" rate dropping to just 2.87%. Besides, the response rate increased sharply to 80.34%, indicating that participation was better after the training. A minority of the respondents did not respond (19.66%), although this was far below the rate from the first round.

Table 1 The Illustration Shows the Average of the Results of Uninformed and Informed Phishing Contest



Round 1	Average
Trapped to Phishing	13.21%
Reported Phishing	43.51%
Neither reported not clicked	43.28%

Round 2	Average
Trapped to Phishing	2.87%
Reported Phishing	77.47%
Neither reported not clicked	19.66%

The results from the two rounds of phishing challenges showcase how targeted cybersecurity training decreases the susceptibility of an employee to phishing attacks: Round 1, where no prior training was given to employees, had a participation rate of 56.72%, while 13.21% of participants clicked on phishing links, indicating their unawareness. However, a large number of the employees (43.28%) did not respond. By analyzing those results and by giving specific training and real perception, round 2 showed improvement in a significant manner: now participation increased to 77.47%, and the percent of those who fell for phishing attempts dropped to a very small number, that is, 2.87%. It also decreased the rate of non-participation to 19.66%, reflecting an improvement in the level of watchfulness and response. The evidence here will be that focused and structured training can improve employee detection and response to phishing attacks, hence securing an organization from cyber threats.

- ➢ *Limitations*

As this research was conducted in a small organization with about 90 employees, it cannot be generalized easily. The findings may not relate to much larger organizations or other industries that face different challenges in cybersecurity and demographics. The motivation of the employees or interest in topics related to cybersecurity could be some of the factors that influenced the rates of participation in the phishing simulations, thus potentially leading to biased results. Employees highly interested in cybersecurity issues could have participated more readily. The study did not explain why all employees did not participate in every phishing email. The reason for non-participation, for instance, time factor or ignorance, could form a good hypothesis that would shed light on how to modify future training programs. These constraints mean that though the study provided important insights, there was a need for more extensive and diverse samples, longer periods of follow-up, and extra control measures to aid in establishing a well-rounded understanding of the performance of automated phishing training programs.

IV. CONCLUSION

Thus, findings from this study have demonstrated the significance of automated phishing contests in improving cybersecurity awareness among employees. It has been established through the study, based on the KnowBe4 platform, that structured phishing simulations and targeted training enhance the capability of employees to recognize and respond to phishing attempts. The results showed a well-evident decrease in susceptibility to phishing attacks after training, which is another piece of evidence that supports regular cybersecurity education in improving organizational defenses.

This also tends to show that more sophisticated phishing emails remained an Achilles heel in this study, in which one-shot training is perhaps unlikely to completely close gaps in employee knowledge. The results point toward increasing demand for continuous adaptive training programs that would change with the dynamics of developing cyber threats. Investment in frequent, automated phishing simulations and bespoke training can assist organizations in developing their employees into the first line of defense against all different types of cyberattacks. The insights drawn from this study provide a substantial basis on which to improve cybersecurity training strategies, further helping to strengthen organizational security postures.

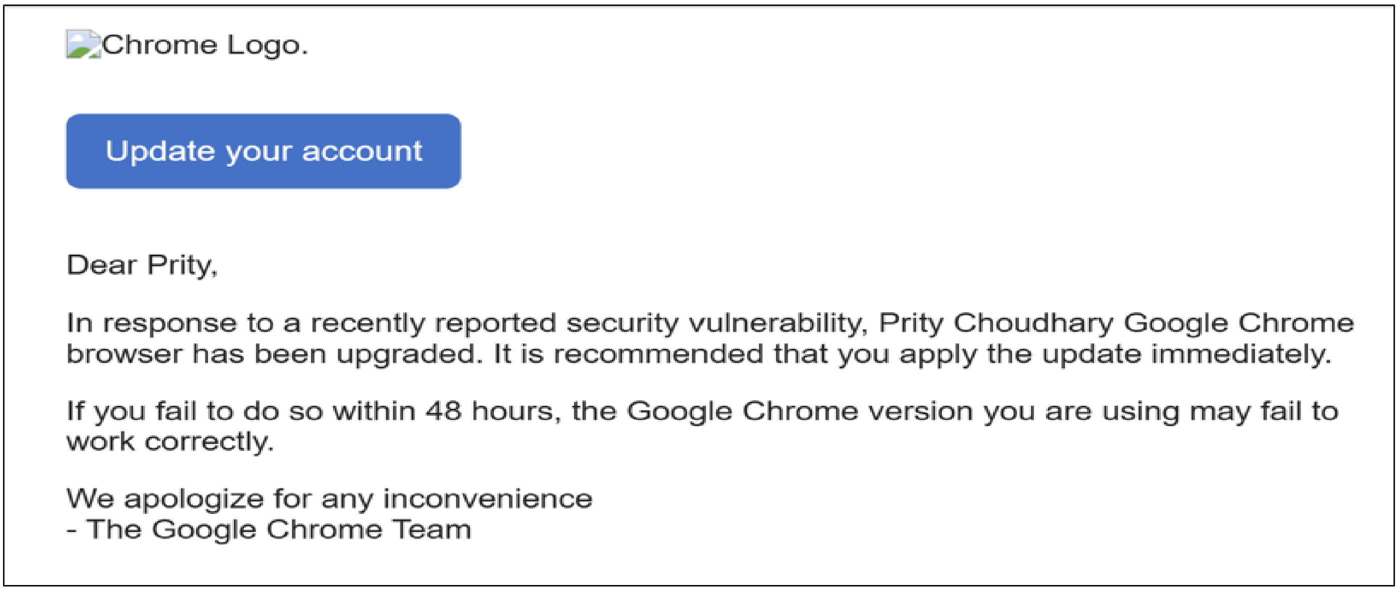
While this study demonstrated the effectiveness of automated phishing contests in enhancing cybersecurity awareness, several areas warrant further investigation, such as exploring the long-term impact of phishing simulations and training on employee behavior by conducting follow-up assessments over a more extended period (e.g., one to two years). This would provide insights into how well employees retain phishing detection skills over time and identify the optimal frequency of training refresher. Investigating the effectiveness of personalized phishing simulations based on an employee's role, level of access, or prior performance in phishing tests could reveal whether tailored training improves engagement and detection rates compared to one-size-fits-all approaches. Such a study conducted across different organizations in various industries and of various sizes may provide a better look at how organizational culture, industry-specific threats, and employee demographics influence the effectiveness of phishing awareness training. By addressing these, future studies could further refine how organizations go about influencing and developing their strategies in improving cybersecurity posture through employee education and awareness.

➢ *Ethical Consideration*

Participants were informed about the objectives and coverage scope of the study, the sequence that it would follow, and that their participation was entirely voluntary. Results of the contest that would be used in analyzing the knowledge gaps were kept confidential and stored on a password-protected laptop locked from accessibility by anyone except the authors of this research. KnowBe4 ensures that they are strict about their privacy policies, thus assuring that organization-wide data cannot be given away outside; employees have access to just their information. Any private or confidential data were destroyed through proper disposal after the study was completed. In addition, privacy directions for respondents, set by the Institutional Review Board, were followed throughout this research process.

APPENDIX

In order to protect the privacy of the participants some examples of email templates have been shared. Others were more personal in nature and contained either email addresses or the office address of the participant.



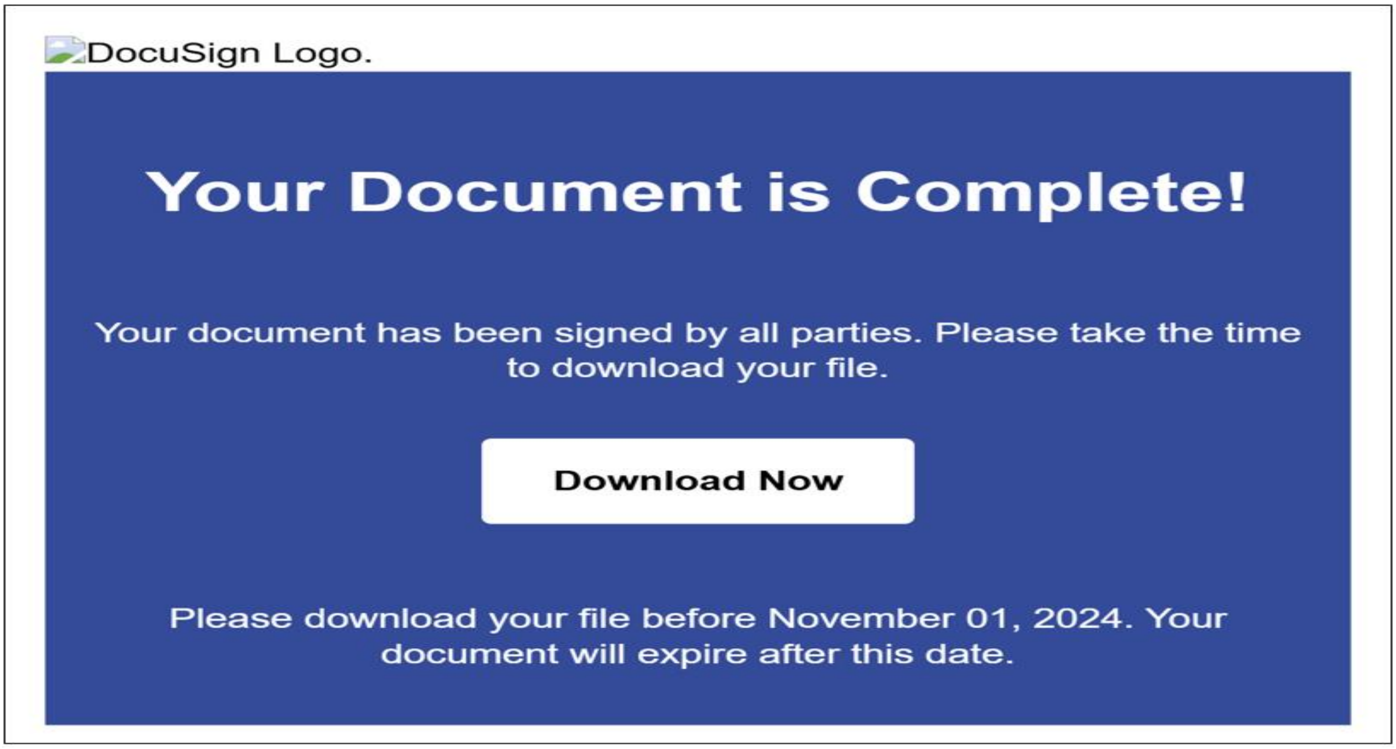
Dear Prity,

In response to a recently reported security vulnerability, Prity Choudhary Google Chrome browser has been upgraded. It is recommended that you apply the update immediately.

If you fail to do so within 48 hours, the Google Chrome version you are using may fail to work correctly.

We apologize for any inconvenience
- The Google Chrome Team

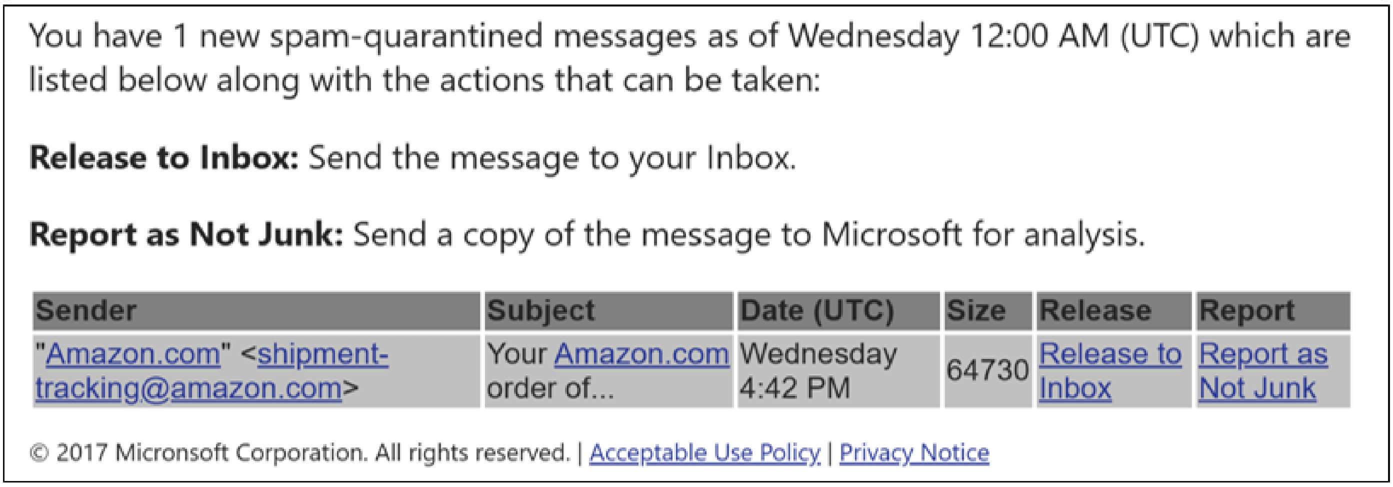
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1136



Your Document is Complete!

Your document has been signed by all parties. Please take the time to download your file.

Please download your file before November 01, 2024. Your document will expire after this date.



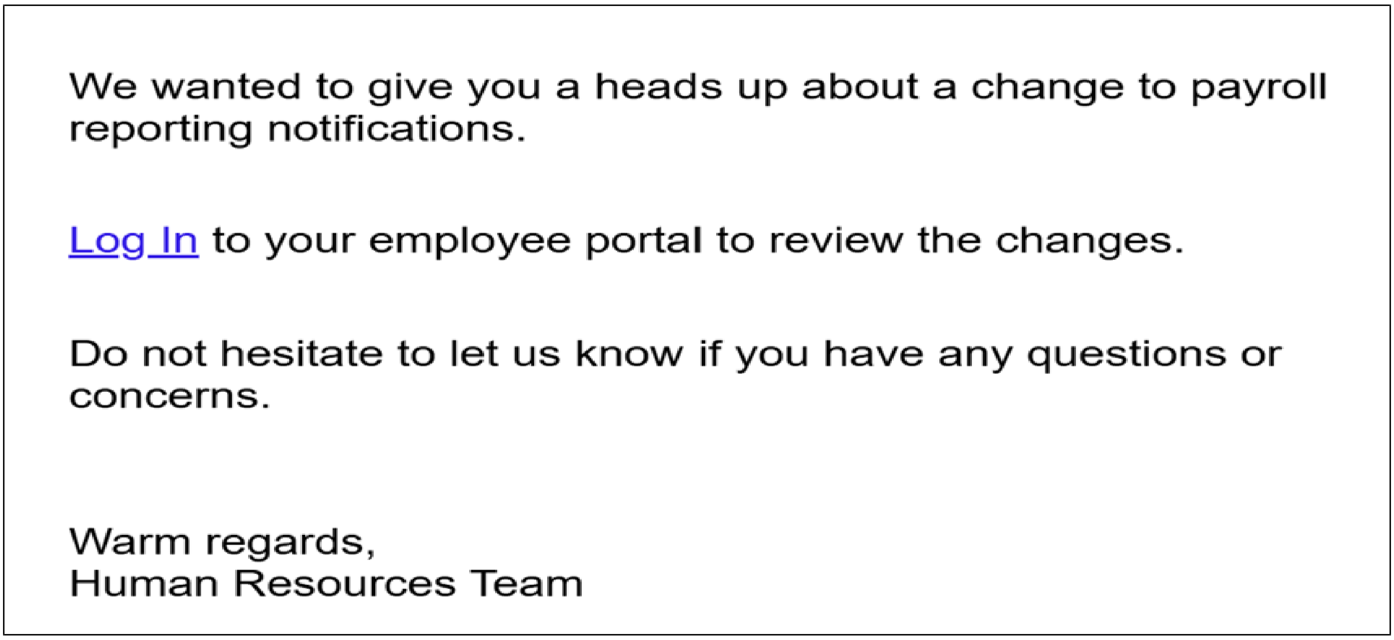
You have 1 new spam-quarantined messages as of Wednesday 12:00 AM (UTC) which are listed below along with the actions that can be taken:

Release to Inbox: Send the message to your Inbox.

Report as Not Junk: Send a copy of the message to Microsoft for analysis.

Sender	Subject	Date (UTC)	Size	Release	Report
"Amazon.com" <shipment-tracking@amazon.com>	Your Amazon.com order of...	Wednesday 4:42 PM	64730	Release to Inbox	Report as Not Junk

© 2017 Micronsoft Corporation. All rights reserved. | Acceptable Use Policy | Privacy Notice



We wanted to give you a heads up about a change to payroll reporting notifications.

Log In to your employee portal to review the changes.

Do not hesitate to let us know if you have any questions or concerns.

Warm regards,
Human Resources Team

REFERENCES

[1]. Sabillon, R. (2020). Delivering Effective Cybersecurity Awareness Training to Support the Organizational Information Security Function. https://doi.org/10.4018/978-1-7998-1879-3.CH012

[2]. He, W., & Zhang, Z. J. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce. https://doi.org/10.1080/10919392.2019.1611528

[3]. De Bona, M., & Paci, F. (2020, August 25). A real world study on employees' susceptibility to phishing attacks. Availability, Reliability and Security. https://doi.org/10.1145/3407023.3409179

[4]. Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? Journal of Computer Information Systems. https://doi.org/10.1080/08874417.2020.1812134

[5]. Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. Personal and Ubiquitous Computing. https://doi.org/10.1007/S00779-021-01551-2

[6]. Pouraimis, G., Thanos, K.-G., Grigoriadis, A., & Thomopoulos, S. C. A. (2019, May 7). Long lasting effects of awareness training methods on reducing overall cyber security risk. https://doi.org/10.1117/12.2518934

[7]. Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021, June 15). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. https://doi.org/10.1109/ICSCEE50312.2021.9498208

[8]. Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. https://doi.org/10.1016/J.PROCS.2021.01.103

[9]. Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. https://doi.org/10.1088/1757-899X/1088/1/012015

[10]. Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors. https://doi.org/10.3390/s22228663v