โครงการ CO-OP SHOWCASE : ก้าวแรกสู่อาชีพ ประจำปี 2567

I-BIT CWIE DAY 2024

ผลงานสหกิจศึกษาดีเด่น
ประเภทโครงงาน/ผลงาน
วิทยาศาสตร์และเทคโนโลยี

CODE

PHISHING EMAIL TEST AWARENESS

Nathapat Kantahirun, Asst.Prof.Dr.Maleerat Maliyaem, Dr.Kanchana Viriyapant

[a]**Bangchak Corporation Public Company Limited**
2098 M Tower Building, 8th Floor, Sukhumvit Road, Phra Khanong Tai, Phra Khanong, Bangkok 10260 Thailand

Abstract

Cybersecurity is a critical strategy that organizations employ to protect their digital assets from cyber attacks and hacking attempts. This strategy encompasses a wide range of security technologies, procedures, and measures designed to safeguard both information and systems. A key component of this is cyber awareness testing, including social engineering assessments, which help organizations identify vulnerabilities and improve their security protocols. In today's digital age, cybersecurity is vital for every organization, regardless of size or industry, as the risk of cyber threats continues to grow. Therefore, investing in robust cybersecurity measures and training skilled personnel is essential to safeguarding valuable assets and ensuring the long-term success of any organization

Introduction

In today’s digital environment, organizations face a growing number of cyber threats, with social engineering attacks like phishing among the most prevalent and damaging. Phishing is a type of fraudulent activity that uses social engineering techniques, often delivered through emails or misleading websites, to manipulate individuals into revealing sensitive information. Attackers commonly target details such as passwords, credit card information, or other confidential data, exploiting the trust of unsuspecting users to breach security defenses.

Methodology

Find and Present Phishing Examples:

Find and Present Phishing Examples The first thing to do when creating a phishing email is to study the sources of phishing patterns that will be used to trick employees.

Employee List Information:

Gather the employee list by requesting the list from the CBS administrator (Cybersecurity Team) and adjust format to meet the requirements and convert the file to CSV.

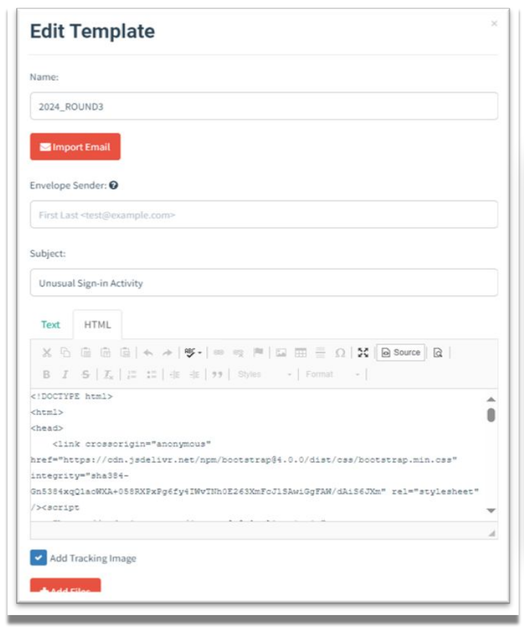
Gophish platform

Import User: Upload user file .csv on Gophish to prepare users into groups if needed. This can help target specific teams or departments and allow for more customized campaigns

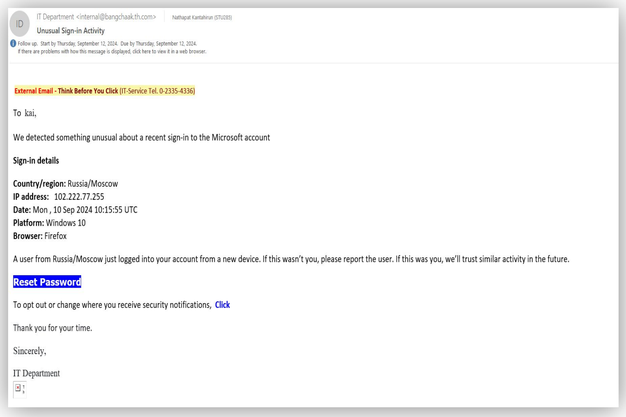
Create Email: Create a phishing email to test

Create Landing Page: When user click link url to continue next process

Launch Campaign: Start a phishing campaign by selecting a target group within the company to be targeted.



How do edit template



Subject Line: Change the email’s subject to suit the new campaign’s tone or purpose.
Email Body: In the email editor, you can modify the text, add new elements, or use dynamic fields (e.g., {{First Name}}) to personalize the email.
HTML Code: If you need advanced customization, you can switch to the HTML editor to adjust the email’s code directly.

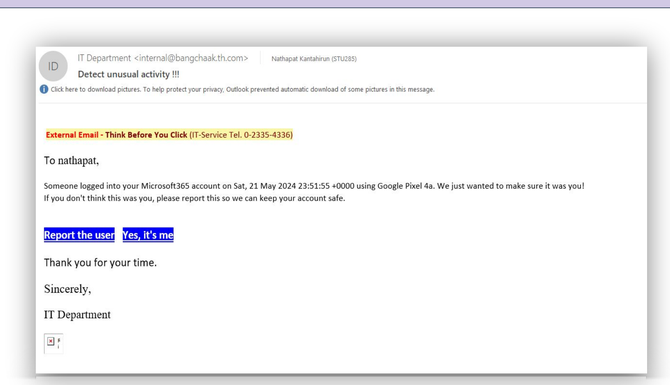
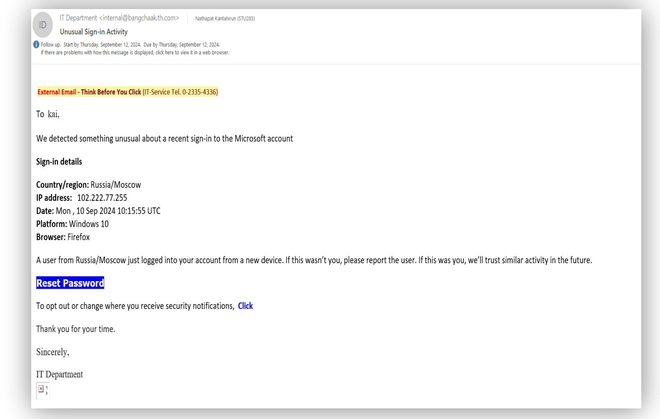


Figure 1 : Phishing Test #2 #3 /2024



Results

This image below shows the 2024 Energy Industry Cybersecurity Test results, with a test score of 1.69%, based on test results from KnowBe4

KnowBe4 is the world's largest data processing platform for attack intent training combined with attack simulation, attack intelligence, and attack simulating. With over 65,000 customers, KnowBe4 addresses the persistent problem of social engineering.

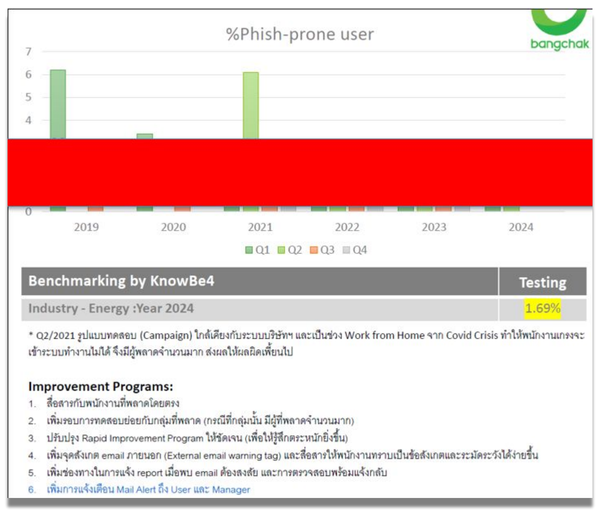


Figure 2: Benchmarking by KnowBe4 (Result)

Conclusion

Implementing phishing tests enhances cybersecurity awareness among employees, helping them recognize and exercise caution with suspicious emails or messages. This initiative fosters a security-conscious culture, ensuring that every employee understands their role in protecting the organization’s data and mitigating potential risks. Additionally, the results from these tests provide valuable insights into the effectiveness of existing training programs, enabling organizations to identify weaknesses and make necessary improvements. As a result, a well-prepared workforce not only strengthens the organization’s security posture but also boosts its credibility with clients and business partners, demonstrating a proactive approach to safeguarding sensitive information and resources.

References

[1] Gophish User Guide (Tools)

Introduction | Gophish User Guide (getgophish.com)

[2] Team CBS Bangchak Corporation

[3] Recommendation for cooperative in google classroom

https://classroom.google.com/c/NTE5OTMwNDgwOTcx

[4] platform Microsoft O365 to communication in team and working

Login | Microsoft 365 (office.com)S

[5] KnowBe4 Benchmark Phishing Result

Security Awareness Training | KnowBe4

Acknowledgements

I would like to express my sincere gratitude to everyone who made my internship experience enriching and valuable. The opportunity allowed me to enhance my ability to collaborate with individuals from diverse backgrounds, which significantly improved my teamwork and communication skills. Through hands-on experience, I was able to apply theoretical knowledge to real-world situations, deepening my understanding of the subject matter.

I also developed strong problem-solving skills by addressing practical challenges during the internship. The experience of living and working alongside others taught me adaptability and patience, qualities that are essential for both personal and professional growth.

Overall, this internship has made a substantial contribution to my academic, professional, and interpersonal development, equipping me with skills and experiences that will serve me in future endeavors.

.