ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 1, pp: (1-2), Month: January - March 2023, Available at: www.researchpublish.com

Effective Information Security Awareness Emails

Bayan Almulhim[1], Rami Alghamdi[2]

[1,2]Saudi Aramco, Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7505534

Published Date: 05-January-2023

Abstract: **What are the factors that affect the awareness emails? How do I know if my emails have been read by the employees or not? How can a department protect critical information resources through efficient awareness? What types of procedures work best for an organization? These types of questions are commonly heard nowadays. Strong security awareness programs are the first line of defence against cybersecurity attacks. Because no matter how many tools an organization uses, there is always room for development. In this paper, we will discuss some of the crucial security awareness aspects that could influence behavioural shifts for the better.**

Keywords: **Information security, Human factor, Cybersecurity, Analysis.**

I. INTRODUCTION

As the number and frequency of cyber-attacks designed to take advantage of unsuspecting personnel increase, the significance of the human factor in information security management cannot be understated. We can control the human factor by designing appropriate awareness; this could be accomplished by implementing a few guidelines that I will be sharing in my article.

II. BODY

Awareness emails are a mixture of words, pictures, and attachments. A quick analysis survey could help an organization improve its employees' effectiveness by getting them to open, read, and implement its awareness emails. Every organization must conduct this analysis to set the baseline and build clear and understandable awareness materials. One of the most critical results that I used to face during my seven years of experience in the cybersecurity field is the relationship between the timing and the context. Usually, people send their emails once they are ready, not once the employees are ready to read them. The quantity of words is another important factor. To control the awareness methodology and raise awareness, every organization must have a well-defined plan based on an annual analysis survey. Timing and the email body are major factors. If your employees are energized in the morning, you can take advantage of this and create lengthy emails with lots of descriptions and information, but during the afternoon, normally, the employees are less energized, so adding pictures and videos and fewer words will be an attraction for them. Furthermore, as information security analysts, we should not underestimate the importance of a cybersecurity awareness and education training program to educate his or her employees on the latest cybersecurity trends.

III. CONCLUSION

Every type of organization, regardless of how big or little, is susceptible to cybercrime. However, they do share one thing in common: human error is more than likely to be the source of them. According to Cybint, this is how about 95% of cybersecurity breaches have happened. This indicates that when it comes to preventing cybercrime and protecting the data

of your business, your employees are one of the weakest links in the chain. So, we should understand that communication is critical in the fight against cybercrime, and email is the most common method used, so our emails should be always effective and efficient.

REFERENCES

[1] Caroline Duncan. (2021)“ Cyber Security Awareness Email To Employees,” Retrieved from DeskAlerts: https://www.alert-software.com/blog/cyber-security-awareness-email-to-employees-sample

[2] CnSight. (2021). Cybersecurity on a Budget: 8 Pratical Steps to Lower Cyber Risk. Retrieved from CnSight: https://cnsight.io/2021/04/29/cybersecurity-on-a-budget-8-practical-steps-to-lower-cyber-risk/