Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 9, Issue 2, pp: (27), Month: May - August 2022, Available at: www.noveltyjournals.com

The Future of Cybersecurity Training

Johara Abdulrahman Al Jarri

Saudi Aramco, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.6638368

Published Date: 13-June-2022

Abstract: **The field of cybersecurity is evolving with emerging threats. It's crucial to keep up with new attack strategies through intensive training. For numerous professionals, taking courses or going through books is no longer enough, because most people will not pay full attention. Gamification is the way to improve cybersecurity skillsets in the future. Taking a creative and resourceful approach to training can make a significant difference in an organization's cybersecurity.**

Keywords: **gamification, cybersecurity training, upskilling.**

1. INTRODUCTION

The world of cybersecurity is consistently evolving as hackers learn new and more sophisticated approaches. Maintaining with new attack approaches through intensive training is key. Giving lectures or endless PowerPoint presentations doesn't cut it anymore for several employees, since more often than not your audience members won't keep their attention throughout the entire thing. The key isn't to demonstrate samples of phishing attacks or kinds of malware, but to possess your attention while making the full exercise creative: that's where gamification comes in.

The definition of gamification would be adding game principles, game thinking or game logic to a task to encourage participation – long story short, make training objectives into a game. By making learning more interactive and fun, you motivate the participants to have interaction more with the learning objectives and practical training Since the participants will get a hands-on experience on the material, they'll learn faster and retain information quickly.

A gamified cybersecurity training works on the same idea of gamified training. The organization gets to find out its participants' cybersecurity skillset level. By supporting its results, it can then analyze the areas where its policies and skills were lacking and improve them. First and foremost, it's an academic exercise – but since it mimics real-life scenarios, it's easier to comprehend simulated cyberattacks once an employee experience them than simply reading about them.

The importance of innovative learning techniques in cybersecurity is imperative as the world struggles to fill thousands of open cybersecurity positions and effectively fight cybercrime. For people and organizations looking to enhance their cybersecurity awareness and skills, understanding cyber theory may be beneficial. Yet, the foremost profound and effective thanks to learn is through doing, which is why gamification is so effective.

The future of cybersecurity skillset elevation is through gamification. Having a resourceful and innovative approach to training can make a large difference in organization's cybersecurity – not only will it's engaging for participants, but it's more likely they'll be enhanced in identifying cyber threats.

REFERENCES

[1] Scholefield, Sam & Shepherd, Lynsay. (2019). Gamification Techniques for Raising Cyber Security Awareness.