**AWARENESS ABOUT CYBER-SECURITY**

# Introduction

Cyber threats are growing every day as a result of digitalization in every industry and weaknesses in any organization's system or network. The main goal of cyber attackers is to hack sensitive company data in order to get financial gain or damage the firm's network. Cybersecurity refers to the employment of a variety of approaches to safeguard sensitive information belonging to any firm.

According Deloitte, 91% of all cybersecurity attacks begin with a phishing email to an unsuspecting victim. On top of that, 32% of all successful breaches involve the use of phishing techniques.

It is important for all organizations to raise awareness with the employees of cybersecurity issues such as phishing email attacks, social engineering and potentially downloading malware from unsecure website.

**Recent examples of where things can go wrong without cyber security awareness:**

*FACC, an Austrian aerospace parts maker, lost $61 million (approximately €54 million) in a CEO fraud scam. A hacker posed as the CEO and sent a phishing email to an entry-level accounting employee who transferred funds to an account for a fake project. This kind of situation underscores the importance of having comprehensive and regular cyber security awareness training for employees.*

*Source: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/*

**User Case Scenario:**

The organizations' employees were tricked into clicking phishing email links as they were unaware of the difference between a legitimate email and a phishing email.

Because of this malware spread throughout most users’ devices throughout the organization. For assistance, the organization’s operations team referred the issue to Microsoft Professional Services. Microsoft cleaned up the malware from all devises and user accounts. After they performed logs audit, Microsoft discovered that the attack started by a user clicking on a phishing email link which in turn downloaded the malware.

Additionally, Microsoft advised the executives of the organization that this time they were because the malware was not severe and could be removed. The next time it could be much worse and might even result in a ransomware encryption of every system.

According to Microsoft, the best course of action for the company is to develop an awareness program for all of their employees, educating them on phishing emails, social engineering attacks, and the importance of being cautious with what they download and which websites they visit.

They organization spent a fortune on this with Microsoft, which was more than their not-for-profit organization could afford. Taking Microsoft’s advice, the board wants these issues fixed by creating a substantial awareness campaign with measured results of improvements. They don’t have the resources for this and don’t know who and how to approach the market for professional assistance to get this done. For a small not-for-profit organization the need help but they have limited fund to get the awareness campaign on the way and get the desired results of improvement.

***Where fortify can help*:**

Fortify is a not-for-profit organization with cybersecurity expertise, resourced by volunteer professionals. We provided Cybersecurity advisory services at minimal, or at no cost, to assist organizations such as yours that have limited resources.

The volunteers of Fortify company help industries to protect from this kind of malware, phishing, and social engineering attacks in the following ways: -

* Using sophisticated tools, fortify will launch a phishing simulation attack to see how many people will click on the email in order to establish a baseline of phishing awareness.
* Fortify will use that data to determine the type of awareness training that should be offered throughout the organization.
* Fortify will create a “report
* After that, fortify will create a training course that will cover a variety of topics, such as social engineering, phishing emails attacks malicious website awareness.
* Fortify will create a “report phishing email” process and create a button in outlook to make it easy for the users to report/
* Following all of the training, Fortify will retest to see if there have been any improvements in "click rate" and how employees deal with an identified attack including “repot a phishing email process
* Volunteers with Fortify look for any other related flaws in internal business processes and create a road-map for the organization to follow toward cybersecurity awareness improvements.

***How to engage fortify services:***

There are a few simple steps to follow in engaging our services

* Go to the website: fortify.com.au
* Register your organization
* Read the guidelines and start to complete the self-assessment questionnaire. Please allow 50 minutes to complete the questionnaire as some areas may be complicated and require some careful thought.
* If you required assistance to complete the questionnaire, please submit a request via the “require assistance” button or go to fortify.com.au/assistance.