# Research and Development Department

The creation of a market analysis form for JPC-Defense has as its main purpose to gather relevant information about the market, potential opportunities, target audience, competitors, threats, SWOT analysis and to understand the customer needs. (Coursera, 2023)

The form was developed through Google Forms and it is available through the link: <https://docs.google.com/forms/d/e/1FAIpQLSdx0EV8nIXDRRQqZOLnmLNZMIMM6m1AyJ_lPCMwIFmdIDQRrQ/viewform>

## Software and Application needed for the project

Developing a training program requires a combination of steps such as instructional design, content creation and technology implementation.

The distribution and organization of the training content will be made through the Moodle platform which offers access not only through computers but also through its App on the mobile phone for Android and IOS. Using the platform we will be able to track and manage the learner's progress.

Focused on e-learning JPC-Defense involves the best technologies available on the market to develop online content that is creative and engages the learner. The use of Adobe Photoshop and Canva will help us to deliver content to high standards.

During the training, it will be available live sessions through the Zoom platform, chosen due to its easy usability which allows simple access from the user.

Collecting feedback from our customers is one of the main tools we have to improve the business, Google Forms will allow us to conduct surveys and make the possible improvements.

Measuring the impact of our training program ensures a good position in the market and keeps us one step ahead of our competitors. To analyse and develop actions to enhance our performance we will be using Power BI to generate all the reports we need. (Continu, 2023)

Simulation of real cyber attacks engages the learners to see the real application of the training. The platform Range force will allow us to simulate real-world attacks.

Storing the material and sharing it securely is of great importance not only for the company but for the users, with Google Drive we ensure the safety and availability of the materials and documents.

## Security Awareness Training Prototype

## Introduction

The Security Awareness Training Program from JPC-Defense is focused on phishing attacks and prevention methods.

Phishing attacks have increased drastically over the years, the latest phishing report from Zscaler ThreatLabs showed that it was an increase of 47.2% in 2022 compared with 2021. (Desai, et al., 2023) Sophisticated methods are being used by cybercriminals which concerns how people are unprepared to deal with the problem.

## User Registration

The user registration will be through our partner platform Moodle, which will secure safe access by the company’s email. Each user will have their own email that is going to be managed by the company and our team.

## Training Overview

Our Security Awareness Training will be divided into 2 modules: Phishing Attacks and Prevention Methods. These modules are separated into 2 topics of 30 minutes each, Spear Phishing Techniques, Business Email Compromise being part of phishing attacks and Employee Training, Multi-Factor Authentication (MFA) being part of prevention methods. There will be an extra free class on phishing simulation as a present for joining JPC-Defense.

## Phishing Attack Modules

**Spear Phishing Techniques** – Understand what is spear techniques and how cybercriminals use intelligence and personalised content to succeed in their attempts against big and small companies.

**Business Email Compromise** – The main methods used to compromise business email accounts and how social engineering can reveal and give access to sensitive information.

## Prevention Methods

**Employee Training** – Development of tools to identify possible attempts and how to respond effectively. Creation of a culture of protection in and out of the company, keeping a safe environment.

**Multi-Factor Authentification (MFA)** – The benefits of multi-factor authentication and how the implementations have impacts against phishing attacks.

## Extra Module – Phishing Simulation

**Phishing Simulation –** Exercises to estimate the real practice, simulating phishing attacks in different approaches on our partner platform Range Force.

## Help and Support

Our support team will be available 24 hours 7 a week, available for the user to contact us any time for any questions they may have. Also on Moodle it will be available a range of frequently asked questions about each module of the training.

## Conclusion

The Security Awareness Training ensures that all students are able to identify and respond to any attempt of phishing attacks. Total understanding of how to prevent cyberattacks and keep sensitive information secure avoiding any attacks that may happen through social engineering.

# Bibliography

Continu, 2023. *How to Create Effective Online Training Programs (6 Steps) - Continu.* [Online]   
Available at: https://www.continu.com/blog/create-online-training-programs  
[Accessed 25 November 2023].

Coursera, 2023. *Market Analysis: What It Is and How to Conduct One.* [Online]   
Available at: https://www.coursera.org/articles/market-analysis  
[Accessed 25 November 2023].

Desai, D., Hegde, R., Laufer, E. & Wang, J., 2023. *2023 Phishing Report Reveals.* [Online]   
Available at: https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year?\_bt=677493654214&\_bk=&\_bm=&\_bn=g&\_bg=154576188893&utm\_source=google&utm\_medium=cpc&utm\_campaign=google-ads-na&gad\_source=1&gclid=CjwKCAiAmZG  
[Accessed 26 November 2023].

Ramos, J., 2023. *Market Analisys Form.* [Online]   
Available at: https://docs.google.com/forms/d/e/1FAIpQLSdx0EV8nIXDRRQqZOLnmLNZMIMM6m1AyJ\_lPCMwIFmdIDQRrQ/viewform  
[Accessed 25 November 2023].

## 