

Ελληνικό Μεσογειακό Πανεπιστήμιο

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πρόγραμμα Σπουδών Μηχανικών Πληροφορικής ΤΕ

Τίτλος:

ΑΝΑΛΥΣΗ ΥΛΟΠΟΙΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΥΠΟΔΟΜΗΣ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗΣ ΔΙΕΡΓΑΣΙΩΝ ΑΣΦΑΛΕΙΑΣ

Title:

ANALYSIS IMPLEMENTATION AND EVALUATION OF CYBERSECURITY PROCESS AUTOMATION INFRASTRUCTURE

Καπουράνης Δημήτριος

Επιβλέπων εκπαιδευτικός : Ευάγγελος Μαρκάκης

Επιτροπή Αξιολόγησης :

-
-
-

Ημερομηνία παρουσίασης:

Ευχαριστίες

Firstly, I extend my sincere thanks to Prof. Markakis Evangelos, for his mentorship and invaluable feedback. His keen eye for detail, constructive criticism, and unwavering support have been instrumental in the development of this thesis.

I would also like to express my deepest appreciation to Ms. Dimitra Papacharoucha whose decided guidance, encouragement, and support throughout the process have been invaluable. Her expertise, dedication, and insights have not only refined my research, but also provided me with a wealth of knowledge that will undoubtedly shape my future endeavors.

I am also indebted to Mr. Nikolaos Astyrakakis for his invaluable support and guidance in the implementation process. His expertise, insight, and enthusiasm have been a source of inspiration and motivation.

I would also like to extend my gratitude to Nikos Papachatzakis for his invaluable contribution in developing the RPA Framework that served as the host for the implementation of my thesis. His exceptional skills and commitment to excellence have not only benefited me but the entire team as well.

Additionally, I would like to extend my sincere thanks to the members of Pasiphae Lab for their contributions to this thesis. Their insightful comments and constructive feedback have been fundamental in bringing this thesis to fruition.

Finally, I would like to express my heartfelt gratitude and love to my family for their support, love, and encouragement throughout this journey. I am also deeply grateful to my loving girlfriend, whose patience, understanding, and support have been invaluable in making this thesis a reality.

Abstract

The rise of social engineering attacks continues to pose a significant threat to individuals and organizations. The past few years, research has focused not only on developing effective cybersecurity defense strategies and mitigation approaches but also on the assessment of an individual's awareness of such attack scenarios. Several approaches have been used, ranging from traditional methods, such as questionnaires designed to assess cybersecurity risky behavior, susceptibility to persuasion, and so on, to more modern practices, such as simulated social engineering campaigns, which include Phishing Campaigns, among others. More often than not, Simulated Phishing Campaigns require human intervention, which can be time and cost consuming as well as prone to error. This thesis proposes the use of Robotic Process Automation (RPA) technology to automate Simulated Phishing Campaigns and, thus, enhance the efficiency and effectiveness of cybersecurity defense strategies. The proposed system includes a user interface and back-end logic that automates the process of sending phishing emails and enumerating interactions, with the goal to assess phishing awareness of a group of individuals that may be the personnel of an organization. Furthermore, the proposed system takes as an input the result of an initial persuasion susceptibility assessment and employs persuasion principles, commonly used as phishing techniques, with the aim to target specific aspects of the human personality and provide an enhanced assessment of one's phishing susceptibility by considering both the initial persuasion susceptibility assessment and the actual susceptibility recorded through the campaign. To evaluate the system, a realistic use case scenario was employed to conduct an experiment in lab environment and evaluate phishing awareness of a group of individuals using the proposed solution. The results of this thesis demonstrate the potential offered by RPA technology in automating Simulated Phishing Campaigns and thus, enhancing phishing awareness assessment strategies.

Περίληψη

Η άνοδος των επιθέσεων Social Engineering συνεχίζει να αποτελεί σημαντική απειλή τόσο για μεμονωμένους χρήστες του διαδικτύου όσο και για οργανισμούς. Τα τελευταία χρόνια, η έρευνα επικεντρώνεται όχι μόνο στην ανάπτυξη αποτελεσματικών αμυντικών στρατηγικών στον κυβερνοχώρο, αλλά και στην αξιολόγηση της γνώσης ενός ατόμου για τέτοια σενάρια επίθεσης. Μέχρι σήμερα έχουν χρησιμοποιηθεί διάφορες προσεγγίσεις, που κυμαίνονται από παραδοσιακές μεθόδους, όπως ερωτηματολόγια, που έχουν σχεδιαστεί για την αξιολόγηση επικίνδυνων συμπεριφορών στον κυβερνοχώρο, της ευαισθησίας σε τεχνικές πειθούς, έως πιο σύγχρονες πρακτικές, όπως προσομοιώσεις επιθέσεων Phishing. Τις περισσότερες φορές, αυτές οι προσομοιώσεις απαιτούν ανθρώπινη παρέμβαση, η οποία μπορεί να είναι χρονοβόρα και δαπανηρή καθώς και επιρρεπής σε σφάλματα. Αυτή η πτυχιακή προτείνει τη χρήση της τεχνολογίας Robotic Process Automation (RPA) για την αυτοματοποίηση τέτοιων προσομοιώσεων Phishing και, ως εκ τούτου, τη βελτίωση της αποτελεσματικότητας και της αξιοπιστίας τους. Το προτεινόμενο σύστημα περιλαμβάνει μια διεπαφή χρήστη και την λογική υποστήριξης που αυτοματοποιεί τη διαδικασία αποστολής Phishing email και απαρίθμησης αλληλεπιδράσεων, με στόχο την αξιολόγηση της κατάστασης μιας ομάδας ατόμων που μπορεί να αποτελεί το προσωπικό ενός οργανισμού. Επιπλέον, το προτεινόμενο σύστημα λαμβάνει το αποτέλεσμα μιας αρχικής αξιολόγησης πάνω σε πιθανή ευαισθησία σε συγκεκριμένες αρχές πειθούς. Έπειτα, χρησιμοποιεί αυτές τις αρχές, με σκοπό να στοχεύσει συγκεκριμένες πτυχές της ανθρώπινης προσωπικότητας και να παρέχει μια βελτιωμένη αξιολόγηση της ευαισθησίας κάποιου στο Phishing, λαμβάνοντας υπόψη τόσο την αρχική αξιολόγηση ευαισθησίας πειθούς όσο και την ευαισθησία που καταγράφηκε μέσω της προσομοίωσης. Για την αξιολόγηση του συστήματος, χρησιμοποιήθηκε ένα ρεαλιστικό σενάριο για τη διεξαγωγή πειράματος σε εργαστηριακό περιβάλλον και την αξιολόγηση κατάστασης μιας ομάδας ατόμων κάνοντας χρήση της προτεινόμενης λύσης. Τα αποτελέσματα αυτής της πτυχιακής καταδεικνύουν τις δυνατότητες που προσφέρει η τεχνολογία RPA στην αυτοματοποίηση προσομοιώσεων Phishing και, κατά συνέπεια, στην ενίσχυση των μεθόδων αξιολόγησης καταστάσεων επιρρέπειας σε Phishing επιθέσεις.

Table of Contents

Ευχαριστίες 2
Abstract 3
Περίληψη 4
Table of Contents 5
1. Introduction 7
Social Engineering Attacks 7
Persuasion Principles Exploitation 7
Emerging Issues and Proposed Mitigation 8
2. State of the Art 10
3. Technology Enablers 12
3.1 Protocols 12
3.1.1 Lightweight Data Access Protocol 12
3.1.2 Simple Mail Transfer Protocol 12
3.1.3 Transmission Control Protocol (TCP) 12
3.1.4 Secure Shell [SSH] 13
3.2 Programming Languages 13
3.2.1 Python3 13
3.2.2 C# 13
3.3 Frameworks 13
3.3.1 RPA Framework 13
3.3.2 Apache Directory Studio 14
3.3.3 MySQL 14
3.3.4 PhpMyAdmin 14
3.3.5 FastAPI 14
4. Implementation 15
4.1 Conceptual Diagram 15
4.2 Internal Architecture of the proposed solution 17
4.3 RPA automated Simulated Phishing Campaign Flow Diagram 19
4.4 RPA Automated Simulated Phishing Campaign Sequence Diagram 21
4.5 Phishing Email Templates 23
4.3 Translation of a Simulated Phishing Campaign in RPA tasks. 36
5. Evaluation 38

5.1 External dependencies deployment....38
5.2 Initiation of the Simulated Phishing Campaign....38
5.3 Results of the Simulated Phishing Campaign experiment....40
5.4 Discussion....44
6. Conclusion....45
7. References....46
8. Annex I....47

List of Figures

Figure 1: Conceptual Diagram....16
Figure 2: Simulated Phishing Campaign Adapter: Internal Architecture....17
Figure 3: Flow Diagram....20
Figure 4: Sequence Diagram....22
Figure 5: Example of phishing email based on Authority persuasion principle.. **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 6: Example of phishing email based on Liking persuasion principle ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 7: The process of a Simulated Phishing Campaign....39
Figure 8: Campaign start: pop-up....39
Figure 9: Connect to LDAP: pop-up....40
Figure 10: The post-campaign report....44
Figure 11: Phishing email based on the Scarcity principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 12: Phishing email based on the Reciprocation principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 13: Phishing email based on the Reciprocation principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 14: Phishing email based on the Liking principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 15: Phishing email based on the Liking principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 16: Phishing email based on the Consensus principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 17: Phishing email based on the Consensus principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 18: Phishing email based on the Commitment principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 19: Phishing email based on the Authority principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 20: Phishing email based on the Authority principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**

Figure 21: Phishing email based on the Authority principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
Figure 22: Phishing email based on the Authority principle. ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**

1. Introduction

Social Engineering Attacks

In the cybersecurity realm, many cyber-attacks are executed through social engineering practices [1]. The term "social engineering," as used by cyber security professionals, refers to the exploitation of the human element in an Information and Communications Technology (ICT) environment with malicious intentions. A very common social engineering practice is the exploitation of the human element in cyberspace through malicious emails, which is referred to as Phishing[1]. Phishing occurs when a user is prompted to download a file or provide sensitive information (e.g., credentials) through a faked link, giving the hackers the opportunity to exploit this information or implant malware onto the victim's machine. Phishing emails vary in terms of context, but several patterns have been identified. Phishing email senders utilize known persuasion principles to exploit human characteristics, commonly referred to as human weaknesses in the cyberspace.[8]

Persuasion Principles Exploitation

Similar to the way network penetration testers aim for vulnerable spots in a network, social engineers target human weaknesses, such as: trust, consensus, and fear of missing out [2]. According to Cialdini in [11], the six principles of persuasion are: Reciprocity; Scarcity; Authority; Commitment and Consistency; Liking; and Consensus.

The *reciprocity* persuasion technique refers to how humans value the balance of the things they receive from others and what they give back. To trigger this sense, malicious individuals try to pretend that they did something for the victim and then expect the victim to comply with their requests. An example of an attempt to exploit social obligation is the process of embedding a pop-up alert in a website informing the user that a “virus” has infected their system followed by a telephone number that the user may call to resolve the issue and corresponds to the attacker’s disposable telephone. The attacker then pretends to fix the user's issue and expects something in return. However, there never was an actual virus in the user’s system and the malicious individual pretends to have offered something to the victim in order to trigger the social obligation of returning the favor.

The *scarcity* or *fear-of-missing-out* persuasion principle refers to the shortage of availability of a product or a service and someone’s need of it. The lowest the availability of a product, the more people tend to think they need to purchase it. In phishing mails the principle of Scarcity is exploited by fake free trials or other fake offers that are in some way limited and urge the user to act in rush.

Moreover, people are more likely to follow instructions if they come from a well-known and respected authority. Identity-theft phishing emails commonly use the *authority* persuasion technique to exploit this weakness. Such emails may either originate from a well-known domain such as Facebook, Instagram, or LinkedIn, from a spoofed and compromised supervisor’s account, or from a fake account that resembles a legitimate account.

[1] Available: https://www.phishing.org/what-is-phishing

Research has revealed that people like to be consistent regarding both their beliefs and their actions, which makes them more likely to proceed with an action if they have already committed to do so. Therefore, malicious individuals employ the *commitment* persuasion technique by prompting someone to perform one small and insignificant action for them, which is followed by another also insignificant action. By repeating this process, the attacker can convince the victim to either reveal sensitive information or expose some point-of-entry for the attacker.

Regarding the *liking* persuasion principle, people tend to trust products or services recommended by people they like and trust, such as their friends. Moreover, people are more likely to buy products that are advertised to be used by people that are similar to them in terms of appearance, age, and behavior. For example, new employees are often targeted by phishing emails that supposedly come from the Human Resources department of the company, in which they work, in an attempt to exploit their liking instinct.

Finally, *consensus* refers to the urge for social acceptance, which is another human weakness that may be exploited by malicious actors in the cyber realm. Because of their inherently social character, humans are subject to the influence of others in the process of making decisions. People often observe their surroundings to discover what the norm is, and then they attempt to conform to what they observe. A phishing email including information such as "458 of our 600 employees have downloaded this update" will attempt to target this instinct with the aim of persuading someone to download malicious software in their system.

Emerging Issues and Proposed Mitigation

The issue that emerges from the frequency and impact of social engineering attacks is how an individual or an organization may be protected from this type of attacks. A common means of defense against social engineering attacks is awareness-raising campaigns [9]. These campaigns have the goal of educating individuals regarding known social engineering practices, aiding them in identifying and avoiding them in the future. Another way of familiarization with social engineering practices is through simulated social engineering attacks [10], which aims in educating individuals through the learn-through-experience methodology, while it reveals the susceptibility of an organization's workforce to phishing attacks.

For a Simulated Phishing Campaign to be carried out successfully several phishing email templates need to be developed and used for sending phishing emails to the targets of the campaign. These templates are based on the persuasion principles described above and are filled out with content relevant to the recipient, to achieve a more realistic experience. Finally, the interactions of the recipients with the phishing emails are recorded for generating a report that contains the overall susceptibility status of the individuals involved in the campaign. Nevertheless, the process of Simulated Phishing Campaigns is a rather complicated operation. The extensive nature of a manually conducted campaign, combined with the fact that such campaigns are often executed by third-party organizations, leads to an increased cost regarding its performance. The system administrator or an authorized individual needs to contact the initiator of the campaign to agree on several campaign parameters, such as duration, intensity, and information handling of the whole operation. As a result, simulated phishing campaigns are usually one-time operations that aim to momentarily assess the social engineering awareness of the personnel of an infrastructure.

In the process of investigating Simulated Phishing Campaigns and with the aim to automate such a procedure in order to mitigate its complexity and cost, this thesis proposes the use of the Robotic Process Automation (RPA) technology. According to the definition of IEEE [3], RPA is

the "*preconfigured software instance that uses business rules and predefined activity choreography to complete the autonomous execution of a combination of processes, activities, transactions, and tasks in one or more unrelated software systems to deliver a result or service with human exception management".* A piece of software that performs this predefined sum of tasks is often referred to as a *software robot*. Based on the literature review that was conducted regarding the use of persuasion principles in phishing emails and the automation of Simulated Phishing Campaigns through the RPA technology, this thesis presents a low-cost and high accuracy Simulated Phishing Campaign automation approach, while it investigates benefits and drawbacks that emerge from such an implementation.

The rest of this thesis is structured as follows: Chapter II reviews relevant state-of-the-art frameworks that either aim to automate cybersecurity operations, by utilizing the RPA technology, or attempt to automate phishing operations in general; Chapter III presents the technologies employed in this thesis towards automating Simulated Phishing Campaigns, such as data storage operations, User Interface design, etc.; Chapter IV provides a detailed description of the planning, design, and development of the proposed framework, while Chapter V refers to the framework's evaluation. Finally, Chapter VI includes the closing remarks of this thesis and the limitations of the proposed framework as well as the future steps that that could be followed towards the enhancement of the framework.

2. State of the Art

Automation in the cybersecurity sector is not a novel concept. Chen Zhong et al. in [4] established a system that considered the behavior of 29 expert cybersecurity analysts as they examined a set of alarms and firewall records. By automating the process and enabling the extraction of the path patterns for attack mitigation, the suggested framework reduced operational costs and time investment requirements.

RPA technology has also been utilized to aid in cybersecurity processes automation. Adhikari et al. [5] used RPA in conjunction with other technologies to help complex aerospace systems become immune to cyber-attacks. The findings demonstrated that, when compared to manually conducted Security Information and Event Management (SIEM) operations, RPA improved the process by enhancing the resilience of the systems.

To mitigate the financial and time expenses of manually conducted phishing campaigns, one of the earliest frameworks that was proposed for the automation of Phishing Campaigns was the Social Engineering Toolkit[2] (SET). Dave Kennedy, an experienced penetration tester, noticed a gap in the available cybersecurity tools and, as a result, he conceptualized and developed this open-source Python-based social engineering penetration testing application. Even though SET was first released twelve years ago, it is still a widely utilized tool for automating phishing campaigns. However, some of its drawbacks include its user interface that remains a command line environment and its ability to be deployed only on Linux operating systems. Therefore, SET is a platform-dependent framework and a more challenging experience when it comes to collecting, organizing, and presenting phishing campaigns' findings.

The most popular solution, as it has been utilized in scientific studies [6], [7], seems to be the GoPhish framework[3], which was developed by Jordan Wright in late 2013. GoPhish is currently an open-source platform that automates simulated phishing attacks and creates a report detailing the results of each campaign. Furthermore, GoPhish's well designed and implemented user interface makes it one of the most complete frameworks in terms of both automating a simulated phishing campaign and presenting each campaign's results.

KingPhisher[4] is another user-friendly framework that simulates real-world phishing attacks in order to test and raise user awareness. This framework can be used to run campaigns either for basic awareness training or for more complex scenarios, where phishing emails aim for credential harvesting.

Another simulated Phishing Campaign automation initiative worth mentioning is the Phishing Frenzy[5] framework. Brandon McCann[6], developed this framework to assist penetration testers in handling phishing attacks more effectively, while still providing realistic phishing campaigns. Compared with all the other frameworks discussed in this section, Phishing Frenzy is the least maintained framework, being last updated five (5) years ago.

Stemming from the literature review, automation in the context of cybersecurity is a concept that is constantly being revisited as new technologies emerge, such as RPA. To this day, there are several Phishing Campaign Frameworks that manage to automate processes such as:

[2] Available: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

[3] Available: https://github.com/gophish/gophish

[4] Available: https://github.com/rsmusllp/king-phisher

[5] Available: https://www.phishingfrenzy.com/about

[6] Available: https://www.phishingfrenzy.com/about

phishing email delivery, user interaction enumeration, and presentation of campaign findings. The common limitation identified throughout the analysis of the above listed frameworks is that, to the best of our knowledge, there is no framework that leverages RPA technology in order to achieve Phishing Campaign automation. In addition, besides the GoPhish framework, all the investigated phishing automation solutions lack an intuitive and user-friendly Graphical User Interface. These findings generated the notion to develop a framework for conducting Simulated Phishing Campaigns in an automated way, omitting the necessity for human interaction throughout the whole process, through the use of RPA technology. Complementary to the use of RPA technology, the front-end of the proposed solution provides a user-friendly interface and simplifies the utilization of the RPA technology for the end user. Thus, the contributions of the proposed framework include:

- The automation, through the RPA technology, of the Simulated Phishing Campaign cybersecurity process, with the aim to aid cybersecurity practitioners in testing the social engineering resilience of the personnel of an ICT environment.

- The development of an intuitive and easy-to-use User Environment that hides the complexity from the end-user, with the goal to be used by cybersecurity practitioners regardless of the level of experience and expertise.

- The evaluation of the proposed framework with the goal of identifying the emerging strengths and weaknesses of automating simulated phishing campaigns through RPA.

The following chapters describe in detail the technology enablers that were employed towards the development of the proposed RPA automated Simulated Phishing Campaign framework, the implementation process, as well as the evaluation of the proposed solution.

3. Technology Enablers

A variety of technological enablers had to be used in order to automate a Simulated Phishing Campaign using RPA. Technology enablers include programming languages that were leveraged for the development of this thesis' logic, protocols that made the dissemination of user input or component interoperability possible, and frameworks that complement the use of those protocols through a Graphical User Interface. Every tool and technology that was utilized for the implementation of the proposed framework is open-source and non-commercial. Additionally, the tool used for the initial persuasion susceptibility assessment is out of the scope of this thesis, and its output is directly used as an input to the Simulated Phishing Campaign.

3.1 Protocols

3.1.1 Lightweight Data Access Protocol

The Lightweight Data Access Protocol[7] (LDAP) is a software protocol that allows anybody, to whom has been granted permission, to locate data belonging to organizations or individuals. The software robots used in this thesis were able to function without human intervention, since they were granted permission to connect to the LDAP server that is running within the entity where the simulated phishing campaign was set to take place. The use of LDAP allows the robots to gather and store any sensitive information required for the successful execution of the simulated phishing campaign.

3.1.2 Simple Mail Transfer Protocol

The process of sending the phishing mails during the campaign was an important aspect of the implementation. Therefore, several different solutions were explored, including self-hosted Simple Mail Transfer Protocols servers (SMTP) as well as commercial SMTP server providers. Eventually, the Google SMTP server was selected for a number of reasons: firstly, due to the minimum number of requirements, as only a valid google account was necessary; secondly, because of the Google SMTP server's stability that was necessary for successfully conducting a simulated phishing campaign; and finally, owing to the seamless integration of the Google server with the code base of this thesis.

3.1.3 Transmission Control Protocol (TCP)

The Transmission Control Protocol[8] (TCP) is one of the major protocols of the Internet Protocol Suite. The TCP was selected as the main protocol that would be used to transfer information in the proposed implementation, due to the connection-driven functionality and the reliability that it proposes in contrary to the User Datagram Protocol[9] (UDP). Reliability was a more critical aspect than the speed of information transmission and the UDP solution, by-design, sacrifices reliability to gain speed in information transactions.

[7] Available: https://ldap.com
[8] Available: https://www.ietf.org/rfc/rfc793.txt
[9] Available: https://www.ietf.org/rfc/rfc768.txt

3.1.4 Secure Shell [SSH]

The Secure Shell Protocol[10] utilizes encryption to secure the interoperability between a client and a server. Being a well-established protocol used to manage more than half of the world's servers, it was chosen in the implementation of the proposed solution to validate and ensure the security of the communication between internal and external components and entities, respectively.

3.2 Programming Languages

3.2.1 Python3

Python3[11] is a programming language that supports a large number of external libraries, a feature that was leveraged in this thesis to deliver the maximum value in the minimum amount of required time. The Matplotlib library was one of the most significant libraries that were used, since it allowed the provision of insightful analytics in the form of bar graphs, which were included in the post-campaign report. Moreover, employee information had to be collected internally and in an automated way to ensure privacy and integrity of sensitive data and minimize the amount of human intervention, respectively. That was made feasible by using the Lightweight Data Access Protocol (LDAP) Python3 library[12]. Finally, the process of sending the customized and personalized phishing emails was handled by the SMTPlib[13] library, a Python module that provides a way of encapsulating an instance of SMTP connection in code level.

3.2.2 C#

C#[14] is a Microsoft programming language that works with the .NET Framework, which is a Microsoft-developed industrial framework that runs primarily on Windows. C# is an ideal option for designing apps customized precisely to the architecture of Microsoft's OS. Therefore, the visual components and Graphical User Interaction features of this implementation are mainly developed in C#. C# was chosen as the main User Interface development language due to the seamless compatibility with the Windows Operating System (OS), which is also developed by Microsoft, rendering the proposed framework to be more accessible and friendly to the end user.

3.3 Frameworks

3.3.1 RPA Framework

The implementation of this thesis regards the automation through RPA of the process of a Simulated Phishing Campaign. Thus, an already developed RPA Framework was employed to host the proposed implementation, providing the necessary User Interface (UI) as well as automation of point-and-click procedures for this thesis to build upon.

[10] Available: https://www.ssh.com/academy/ssh

[11] Available: https://www.python.org/download/releases/3.0/

[12] Available: https://www.python-ldap.org/en/python-ldap-3.4.0/index.html

[13] Available: https://docs.microsoft.com/en-us/dotnet/csharp/

[14] Available: https://docs.python.org/3/library/smtplib.html

3.3.2 Apache Directory Studio

Directory Studio by Apache is a powerful toolkit that can be used with any LDAP server. For this thesis, Apache's Directory Studio provided the Graphical User Interaction environment for the configuration, update, and maintenance operations of the LDAP server.

3.3.3 MySQL

MySQL[15] is a relational database management system that is based on Structured Query Language[16] (SQL) and is used in popular web applications such as WordPress[17], Drupal[18] and Joomla[19]. The data security feature that comes with the deployment of such technology was the key factor in choosing the MySQL framework for the data storage and management in the context of this thesis. Another reason for the selection of MySQL as a data storage solution is the type of the information that needs to be stored, because a technology like MySQL complements data storage and manipulation operations opposed to a graph-based database technology that emphasizes more to the relations between the entities and not the entities themselves.

3.3.4 PhpMyAdmin

The configuration, management and storage of Simulated Phishing Campaign data was enabled by the employment of a Graphical User Interface (GUI) management system. PhpMyAdmin[20] is an Open-Source solution for the management of a MySQL database and includes a graphical user interface for a more responsive and user-friendly environment. Similar to the GUI selection for the configuration of the LDAP server, PhpMyAdmin was selected for its user-friendliness, ease of configuration and ease of maintenance of this thesis database.

3.3.5 FastAPI

The interoperability between this thesis frontend and backend operation was achieved through the use of an Application Programming Interface (API), specifically the FastAPI framework. FastAPI is a state-of-the-art solution that focusses mainly on high performance and simplicity. These two characteristics fit the proposed framework since the high performance aided in the elimination of any possible bias, whereas the simplicity of FastAPI made the development of the framework's API fast and lightweight. Another advantage of the FastAPI is the automatic generation of Swagger, a documentation framework that assists both in the dissemination of the API's functionality and in testing operations.

[15] Available: https://www.mysql.com/
[16] Available: https://web.archive.org/web/20070926212100/http://www.almaden.ibm.com/cs/people/chamberlin/sequel-1974.pdf
[17] Available: https://wordpress.com/
[18] Available: https://www.drupal.org/
[19] Available: https://www.joomla.org/
[20] Available: https://www.phpmyadmin.net/support

4.Implementation

This chapter describes how the rationale of the proposed solution was structured as well as the way each technology enabler was used for the development of the proposed framework. Each sub-component of the proposed solution is described in this chapter regarding its structure and objectives. An initial overview of all the subcomponents, external dependencies, and personas is provided through a conceptual architecture diagram, which is then followed by an internal component diagram. Moreover, the way that each of the subcomponents interact with each other is showcased in a sequence diagram. Finally, the last part of this chapter presents the flow diagram of the operations of the proposed solution.

4.1 Conceptual Diagram

With the aim to achieve the goal of the proposed implementation, a number of main objectives were set for designing the architecture of the proposed solution. These objectives regarded the successful automation of the Simulated Phishing Campaigns, the employment of the RPA technology and, finally, the necessity of a user-friendly workspace environment:

1. Most of the operations are performed by the back-end operations of the software robots with the aim to provide a user-friendly experience that allows users to quickly and easily set up and run simulated phishing campaigns by interacting with the system and accessing its features without the need of expert's knowledge.

2. Minimum-to-no human involvement is needed is required in order to achieve efficient RPA automation of the Simulated Phishing Campaigns. The campaign configuration process requires input only from the Campaign Initiator for determining the necessary parameters. When this process is completed, no other human intervention is needed. The goal of this approach is to offload the manual management and running of Simulated Phishing Campaigns from the Campaign Initiator.

3. Robots' tasks are defined as clear and distinct steps to be executed on after another in a specific order. A key feature of RPA is that software robots can mimic human actions. By breaking down the process of a Simulated Phishing Campaign into smaller, distinct steps, the actions a human would take to complete the process can be described. With RPA these steps are carried out by software robots in sequence, automating the entire process. Additionally, since the robots follow the same steps every time, the proposed solution will be consistent and predictable, allowing for reliable and repeatable results.

Based on the objectives described above, the conceptual architecture of the proposed solution was designed and is presented in *Figure 1* below, including the internal components of the solution, the external dependencies, and the entities that either initiate the Simulated Phishing Campaign operation or directly refer to the process. The interoperability between the sub-components is also showcased. What is more, the two basic user roles participating in the proposed solution are showcased, namely the Campaign Initiator and the Targets of the campaign. The Campaign Initiator is the end-user that configures the campaign and will ultimately receive the post-campaign

report. On the other hand, the Targets refer to the phishing emails recipients which may be the personnel of an ICT ecosystem.

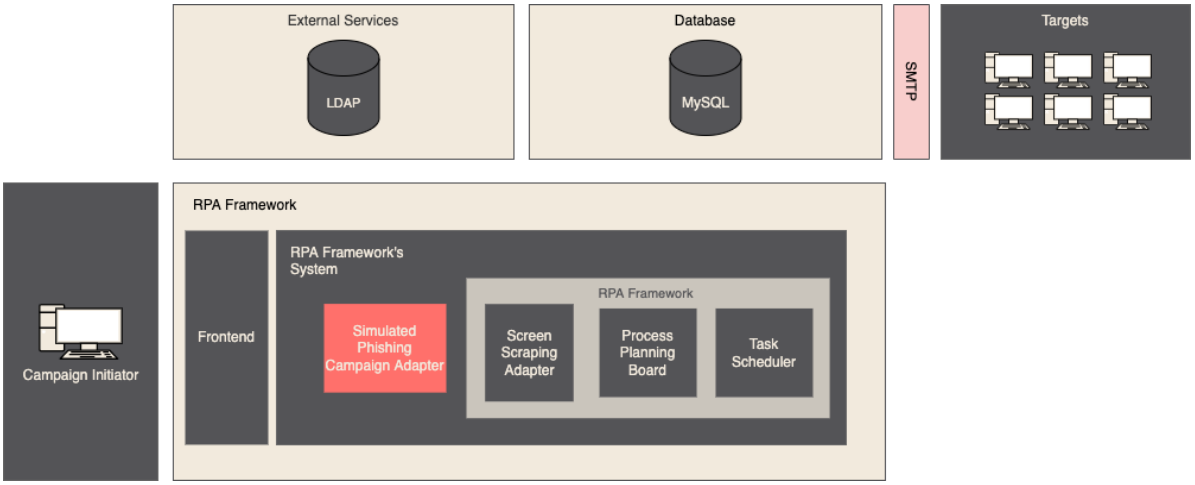


Figure 1: Conceptual Diagram

Starting from left to right, the Campaign Initiator is depicted as an external entity to the proposed framework. That is because, besides the initial campaign configuration, the rest of the proposed solution's operations function without the need for any human interaction. Thus, the Campaign Initiator's sole role is to configure and initiate the Simulated Phishing Campaign process. However, if a Campaign Initiator decides to interfere, either to prematurely terminate the campaign or to manually inspect the campaign's results, they can achieve this by interacting with the framework's User interface.

Moving to the central section of the diagram, the "RPA Framework" component represents the framework that hosts the proposed solution. By employing a "Plugin" architecture the proposed operations were added as a complementary component to the functionality of the RPA framework, rendering the proposed solution highly modular.

Inside the "RPA framework" two different components are depicted, namely: the "*Frontend*", which represents the component responsible for the user interaction with the RPA framework for collecting user input and safely transferring it to the proper back-end component while providing a user-friendly environment and a satisfying user experience; the "*RPA Framework's System*", which contains all the back-end operations of the RPA framework.

The Simulated Phishing Campaign Adapter module depicted inside the RPA Framework's System represents the solution proposed in this thesis, which complements the already existing RPA Framework. Therefore, the description of the implementation of the RPA Framework component is out of the scope of this thesis.

Moreover, the "*External Services*" and "*Database*" components located at the top of the diagram, both describe software services that interact with the RPA Framework. The former contains the user information storing directory that is accessed through the LDAP and the latter includes the MySQL database initialized with the templates of the phishing emails. Both components are located at the top of the architecture since both function regardless of the infrastructure that exists below.

The "Targets" of the Simulated Phishing Campaign is also an external entity of the system. This entity depicts the recipients of the phishing mails sent by the software robots; the interactions of these entities to the emails of the Simulated Phishing Campaign will eventually be recorded to produce the report of a campaign. In an ICT ecosystem, these recipients refer to the personnel whose phishing susceptibility will be assessed.

Finally, state-of-the-art communication and security protocols, such as TCP and UDP, are leveraged for the interoperability of the depicted components, improving the security of the information transactions.

4.2 Internal Architecture of the proposed solution

Moving to the implementation of the Simulated Phishing Campaign Adapter, the key entities of *Figure 1* are also visible in *Figure 2* below, due to the direct interaction with certain internal components of the adapter. Such entities are the *RPA Framework's Frontend*, the *Campaign Initiator* and the *Targets* of the campaign.

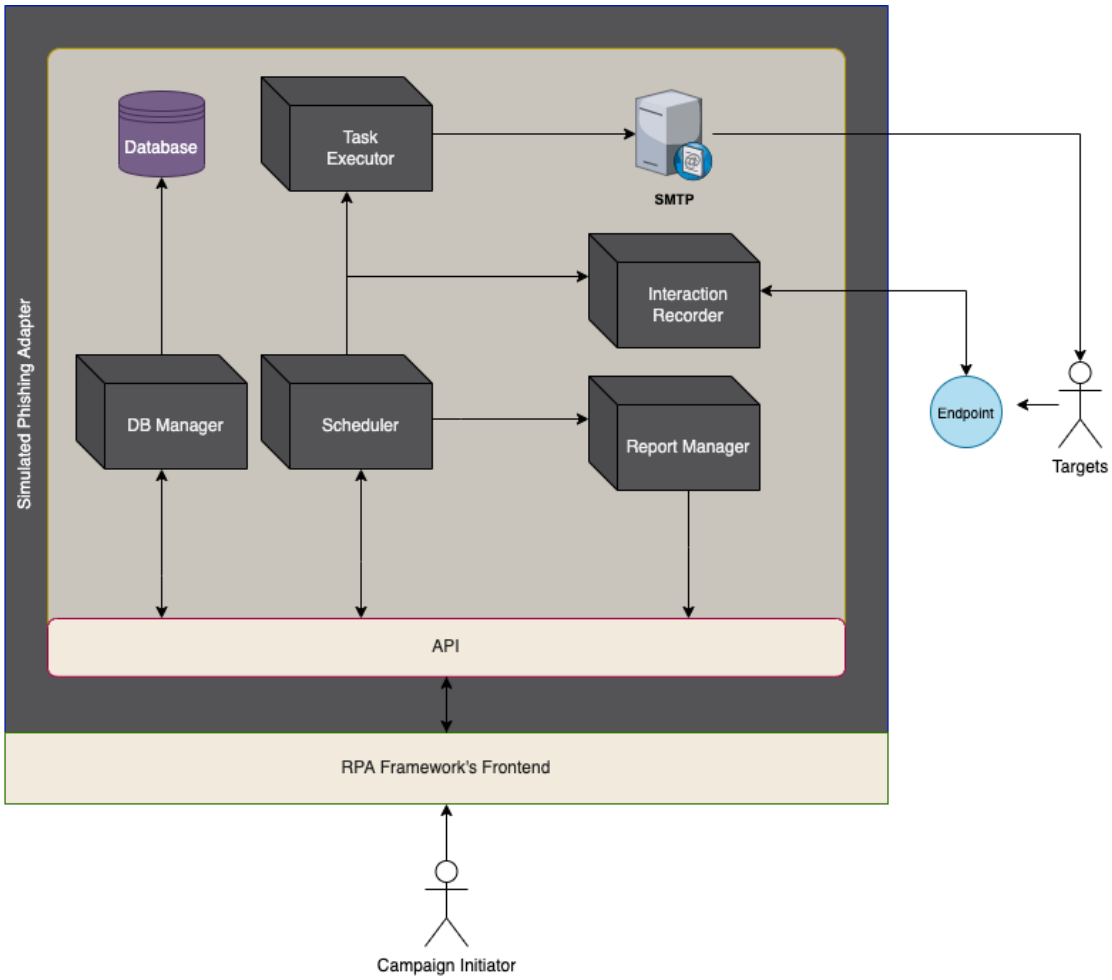


Figure 2: Simulated Phishing Campaign Adapter: Internal Architecture

The Frontend of the RPA Framework is the component responsible for interacting with the end user (Campaign Initiator) and, therefore, invokes the API of the proposed solution by translating the input received from the end user to its corresponding request.

Each request is being handled by the Simulated Phishing Campaign Adapter's API. The responsibilities of the API include the proper communication with each of the sub-components of the adapter, as well as the response back to the RPA Framework's Frontend, with the goal to inform the end user for the success status of each of the actions they requested to be performed.

The DB Manager sub-component handles database manipulation operations. Its objectives regard the creation of new campaigns, recipients, and departments as well as the process of updating the already existing ones according to the requests of the Campaign Initiator that are received through the API. Since each department belongs to at least one campaign and includes a number of individuals that will be considered the recipients of the emails of the campaign, there are also correlation processes that need to be handled by the DB Manager. Successful correlation is a necessity for the reliable campaign runtime. The API is constantly informed by the DB manager for the status of the database regarding updating operations to handle any errors that may occur or informing the Campaign Initiator that everything was set up correctly.

The Scheduler sub-component generates the schedule of the Simulated Phishing Campaign. This sub-component breaks down all the emails that need to be sent to all the recipients into timed tasks that span across the specified duration of the campaign. The duration of the campaign is indicated by the assigned starting and ending date. Another parameter that is considered by the Scheduler is the total number of recipients that the campaign regards. By following the approach that every phishing email template will be sent once to each of the campaign's recipients, each recipient adds a total of tasks to the schedule equal to the amount of the selected phishing emails that will be sent. Moreover, the campaign scheduler foresees leaving a two-day slack at the end of the campaign in order to capture any late responders to the phishing mails.

The generated schedule is sent to the Task Executor sub-component, which executes the included tasks; the successful execution of a task results in a successfully sent phishing email. The emails are sent through a server supporting the Simple Mail Transfer Protocol (SMTP). An important operation of the Task Executor is filling out the phishing emails with dynamic text and visual content to achieve a more realistic Simulated Phishing Campaign. Finally, a decision was made for the Task Executor to send the emails during the working hours (9a.m. to 5p.m.) since there have been identified higher traffic in emails in those hours with the goal, the phishing emails to be blended in with legit ones.

The interactions of the email recipients with the emails are monitored by the Interaction Recorder sub-component. Phishing emails contain images and hyperlinks. Both images and hyperlinks are not directly accessible, rather they are requested from the Interaction Recorder, which enumerates g what was requested. For example, an image request means that a recipient opened the mail, therefore, the image was loaded. On the other hand, a hyperlink request means that the recipient attempted to follow a link contained in the phishing email. Additional to the enumeration of the requests, Interaction Recorder also records the credential submission activities that take place on the landing pages to which several hyperlinks may lead. However, the actual values of the submitted credentials are not recorded in the proposed solution for preserving the security and privacy of the individuals involved in the Simulated Phishing Campaign as Targets.

Finally, the Report Manager sub-component is responsible for producing a report, in a human-readable form, to describe the overall susceptibility posture of the individuals who were

assessed. Valuable information for the creation of this report is the total number and type of interactions with the phishing emails performed throughout the duration of the campaign. These numbers are interpreted into insightful analytics and are depicted in charts to provide a more easily understandable overview of the overall phishing susceptibility of the targets.

Overall, by developing dedicated sub-components for each functionality, system-wide failures are mitigated. However, successful communication between sub-components is necessary to complete end-to-end operations.

4.3 RPA automated Simulated Phishing Campaign Flow Diagram

All the sub-components described above need to work together to achieve a successful automation of a Simulated Phishing Campaign. In the flow diagram presented in Figure 3 below, a successful creation and execution of Simulated Phishing Campaign is described.

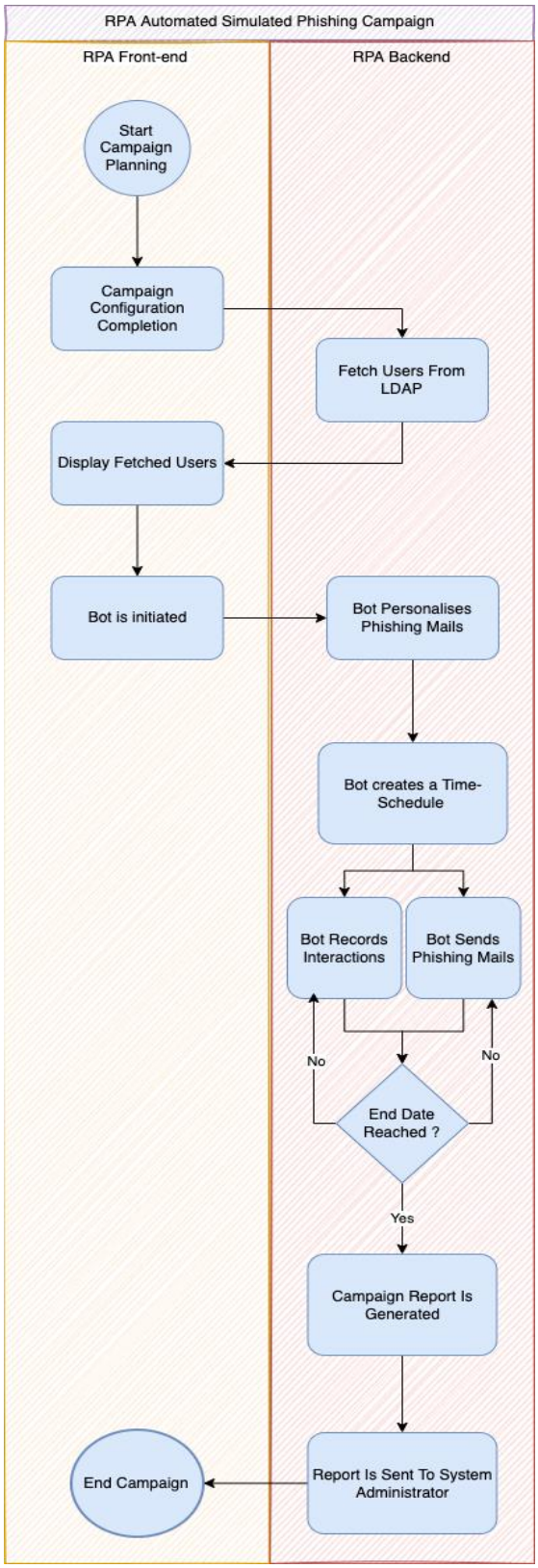


Figure 3: Flow Diagram

The process flow for the Simulated Phishing Campaign is initiated through the Frontend, when the Campaign Initiator sets up the necessary parameters, including the LDAP credentials, the start and end dates, and a descriptive name for the campaign.

Once the initial setup is completed, the framework's robot attempts to fetch the users from the LDAP system. This operation also serves as confirmation that the parameters were set up correctly. If the fetch operation is successful, the users are displayed to the Campaign Initiator to indicate that the LDAP was accessed successfully.

When the configuration of the Simulated Phishing Campaign has been completed the Campaign Initiator can execute the campaign and wait for the results of the assessment.

The execution of the campaign initiates the personalization of phishing emails. Each user will receive every phishing email type generated by using the phishing email templates, once to avoid bias and provide a clear view of the success rate for each email.

Once the phishing emails are generated, they are placed in a time schedule to be sent out at the appropriate times. The schedule is developed around the defined starting date and ends two days before the scheduled end date, allowing for late responses to be recorded.

Parallel to sending the phishing mails, the Interaction Recorder is monitoring the interaction of the targets with the received emails, by enumerating the requested URLs and the submitted credentials.

The process of sending the phishing emails and recording targets' interaction is an ongoing operation until the ending date of the Campaign. When the ending date has been reached, the report of the campaign is generated. The report includes an analysis of the findings of the assessment in percentages and absolute numbers as well as a visualization through bar charts, to help the Campaign Initiator understand the overall phishing susceptibility of the infrastructure.

4.4 RPA Automated Simulated Phishing Campaign Sequence Diagram

The flow of operations described above is achieved through successful internal communication. Figure 4 below presents the Sequence Diagram, which illustrates how information is parsed between the sub-components during the successful creation and execution of a Simulated Phishing Campaign.

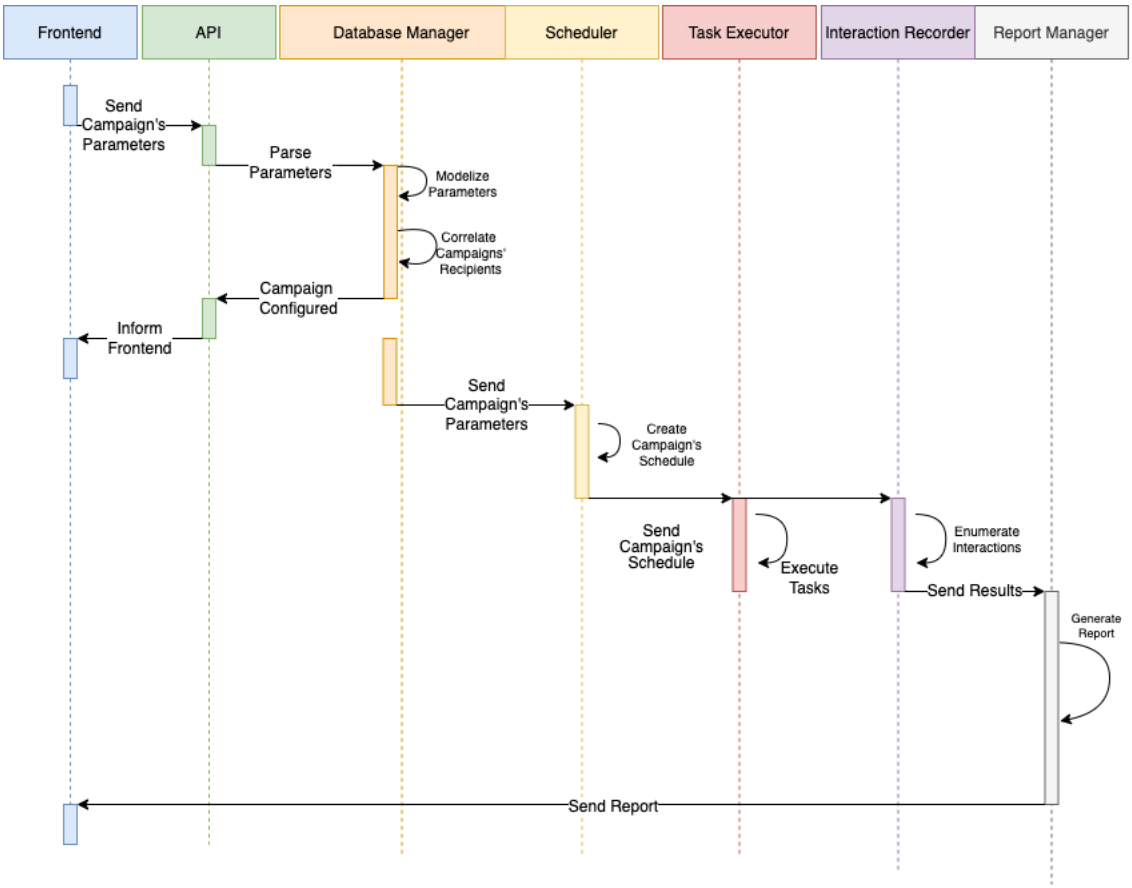


Figure 4: Sequence Diagram

The process begins when the Campaign parameters, submitted to the Frontend by the Campaign Initiator, are parsed to the adapter's API. The API, by having direct communication with the sub-components, is able to forward this information to the responsible sub-component. In this case, the sub-component that needs to receive the submitted information is the DB Manager.

The DB Manager saves the received information to the database and fills in additional necessary information, such as identifiers, for the successful correlation and reference of the saved parameters. The status of the DB Manager's operation is communicated to the Frontend to inform the end user for the successful creation of the Campaign. Furthermore, DB Manager dispatches the parameters of the new campaign to the Scheduler.

The scheduler handles the parameters of the new campaign and generates the schedule according to them before forwarding the campaign to the Task Executor.

The Task executor waits until the starting date of the Campaign. Once the starting date has been reached, and before sending the first phishing email, Task Executor initiates the Interaction Recorder to begin monitoring the interactions to the phishing emails that may be performed by the targets. The Task Executor and the Interaction Recorder work in parallel all throughout the duration of the campaign.

When the ending date of the campaign has been reached, both the Interaction Recorder and Task Executor seize to enumerate interaction and send mails, respectively. The Interaction Recorder, before stopping its operation, sends the enumerated interactions to the Report Manager,

which proceeds to generate the report. The generated report is finally sent back to the Frontend so the Campaign Initiator can inspect it.

4.5 Phishing Email Templates

The conduction of a Simulated Phishing Campaign required the creation of phishing email templates to specify the overall form and appearance of the emails. These templates contained variables in crucial parts of the email that would later be replaced with dynamically generated information. This allowed for the customization and personalization of the phishing emails to make them more convincing and effective.

To build the phishing email templates, the overall structure and layout of the emails was first defined. This included the font, color scheme, and formatting to make the emails look authentic and professional. Variables were then added in strategic locations to be later filled with information such as the recipient's name, to allow for dynamic customization.

This process was repeated to create a total of 12 templates. These included emails that appeared to come from well-known authorities, such as a national bank, as well as emails that seemed like friendly messages from a co-worker. This process ensured that the templates were versatile and leveraged all the persuasion principles identified in relevant literature, namely: scarcity, reciprocity, liking, authority, commitment, and consensus. Once the templates were developed, they were tested to verify that they worked as intended. This involved replacing the variables with sample data to see how the emails would look with real information. The templates were also tested with different data to ensure that they remained convincing and effective. The following sub-sections present in more detail the emails that were generated from each template type, for the scope of this thesis.

Announcement e-mail:

The e-mail depicted in Figure 5 was constructed to comply mainly with the persuasion principle of scarcity and liking. By informing the recipient about an unknown announcement aims to invoke the feeling of missing out and the consequences that may bare. Furthermore, this particular email was written in an informal way to resemble an email coming from a familiar individual.

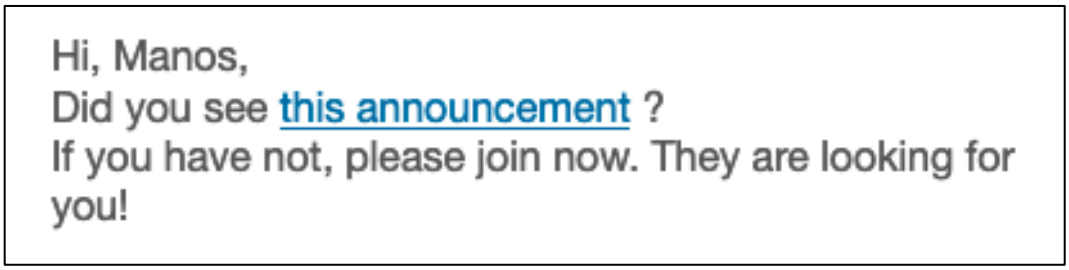


Figure 5: Announcement mail.

E-mail offering assistance

In a similar vein, the e-mail presented in Figure 6 seems to have been sent by a familiar individual. By including the email address of an individual that belongs in the same organization

as the recipient and by offering to conduct the books' closure on behalf of the recipient, the following email utilizes the reciprocity and liking persuasion principles to drive the e-mail recipient to download the embedded file.

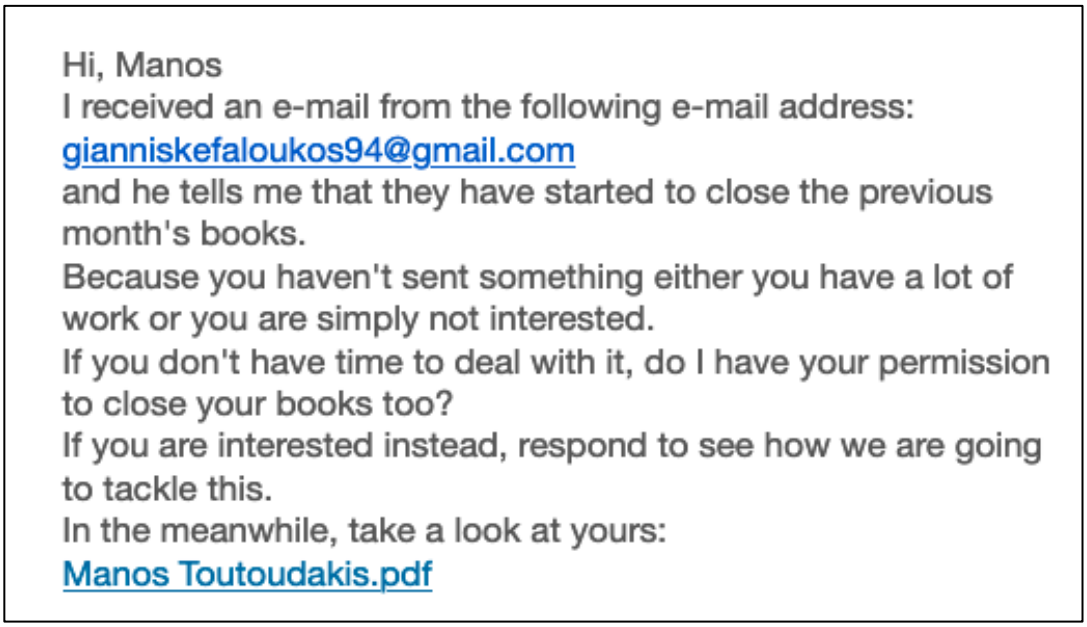

Hi, Manos
I received an e-mail from the following e-mail address:
gianniskefaloukos94@gmail.com
and he tells me that they have started to close the previous month's books.
Because you haven't sent something either you have a lot of work or you are simply not interested.
If you don't have time to deal with it, do I have your permission to close your books too?
If you are interested instead, respond to see how we are going to tackle this.
In the meanwhile, take a look at yours:
Manos Toutoudakis.pdf

Figure 6: Books' closure e-mail.

Calendar e-mail:

Following the same approach, the e-mail presented in Figure 7 was composed based on the liking and the scarcity persuasion principles. By informing the recipient about an upcoming event and prompting them to provide their availability, the scarcity persuasion principle is employed. Similar to the previous email, the disclosure of the e-mail address of a co-worker of the recipient employs the liking persuasion principle.

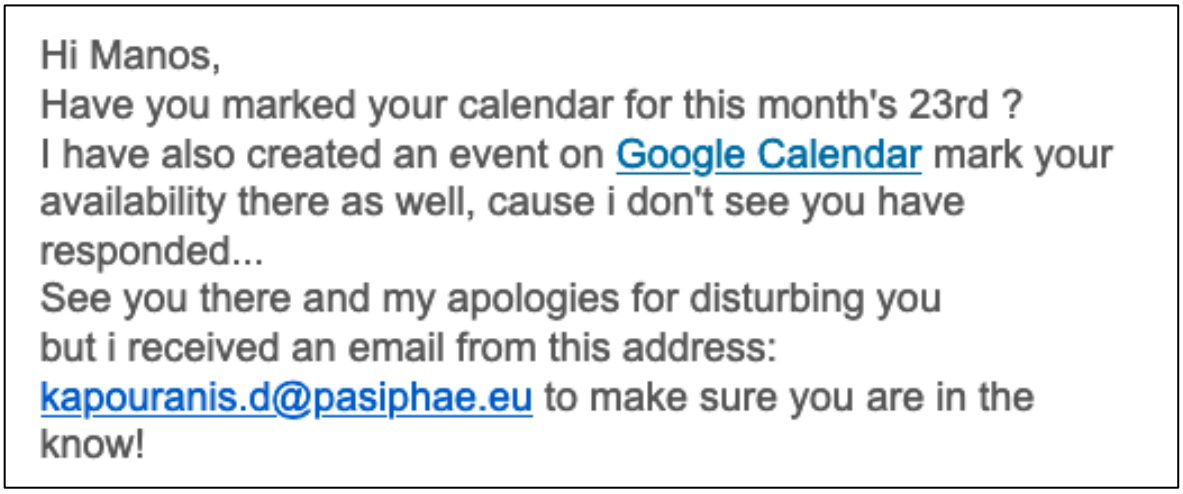

Hi Manos,
Have you marked your calendar for this month's 23rd ?
I have also created an event on Google Calendar mark your availability there as well, cause i don't see you have responded...
See you there and my apologies for disturbing you
but i received an email from this address:
kapouranis.d@pasiphae.eu to make sure you are in the know!

Figure 7: Event e-mail.

E-mail asking for assistance

The e-mail depicted in Figure 8 makes use solely of the liking persuasion principle. By disclosing an email address familiar to the recipient and asking assistance in opening a seemingly benign and harmless e-mail that does not load for the sender, susceptibility to the liking persuasion principle is targeted.

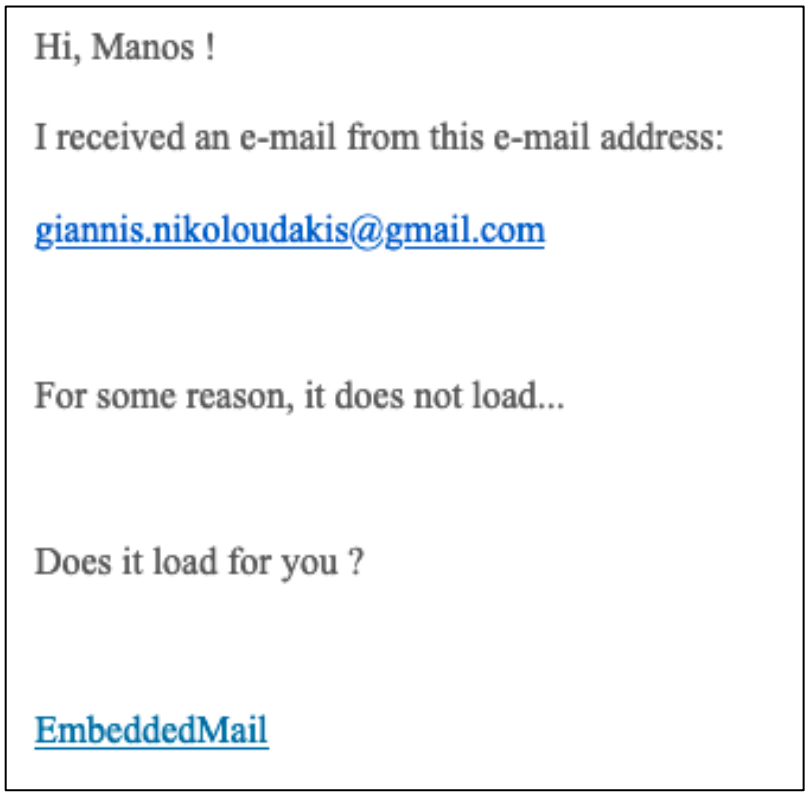


Figure 8: Email asking for assistance.

E-mail asking opinion in a serious matter

The e-mail depicted in Figure 9 is asking for the recipient's opinion in the reinstalment of the death penalty and aims to invoke the commitment persuasion principle. The sensitive nature of a matter like this attempts to harvest a response from the mail recipient. Furthermore, by including a file that supposedly includes the responses of other individuals in this request, the recipient is prompted to see what others have responded, aiming to invoke the consensus persuasion principle.

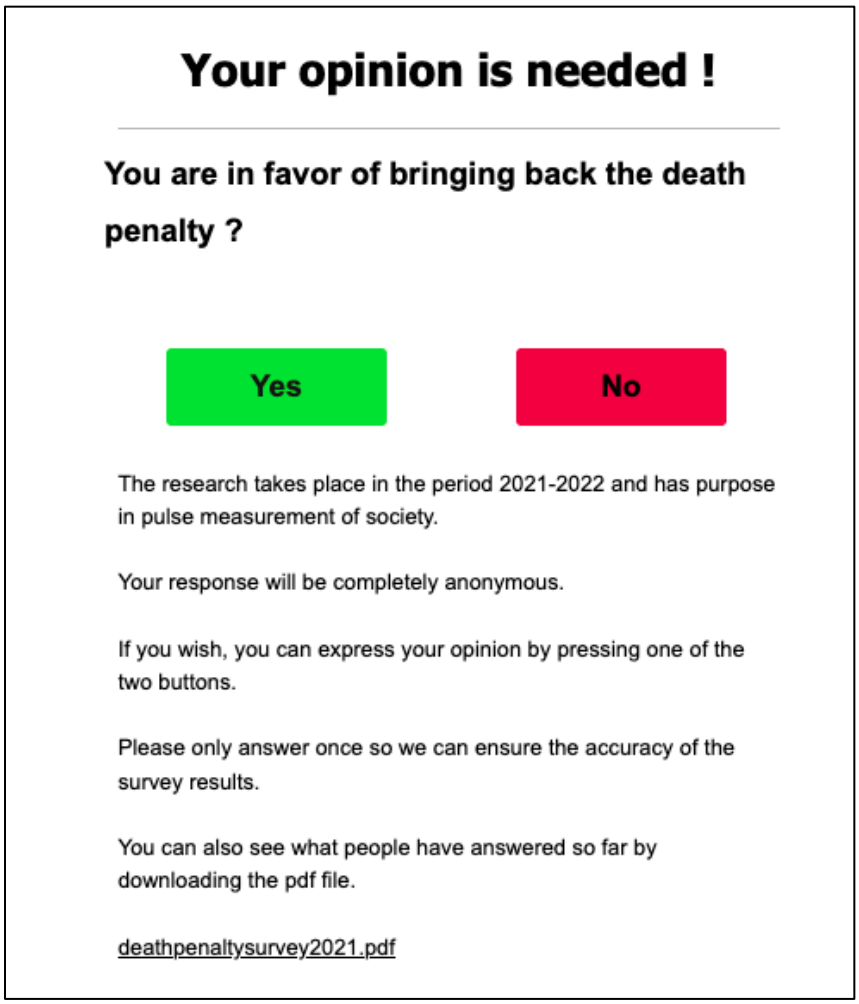


Figure 9: Opinion on death penalty e-mail.

Vaccine fine e-mail

Another attempt to invoke the commitment and consensus persuasion principles is the email presented in Figure 10 , composed to prompt the recipient to co-sign the petition to stop fining the unvaccinated elderly.



Figure 10: Vaccine petition e-mail.

Reforestation e-mail

Under the same approach and also targeting the commitment and consensus persuasion principles, the e-mail presented in Figure 11 prompts the recipient to co-sign the petition on the recent, at that time, topic of forest fires and the reforestation of the burned areas.

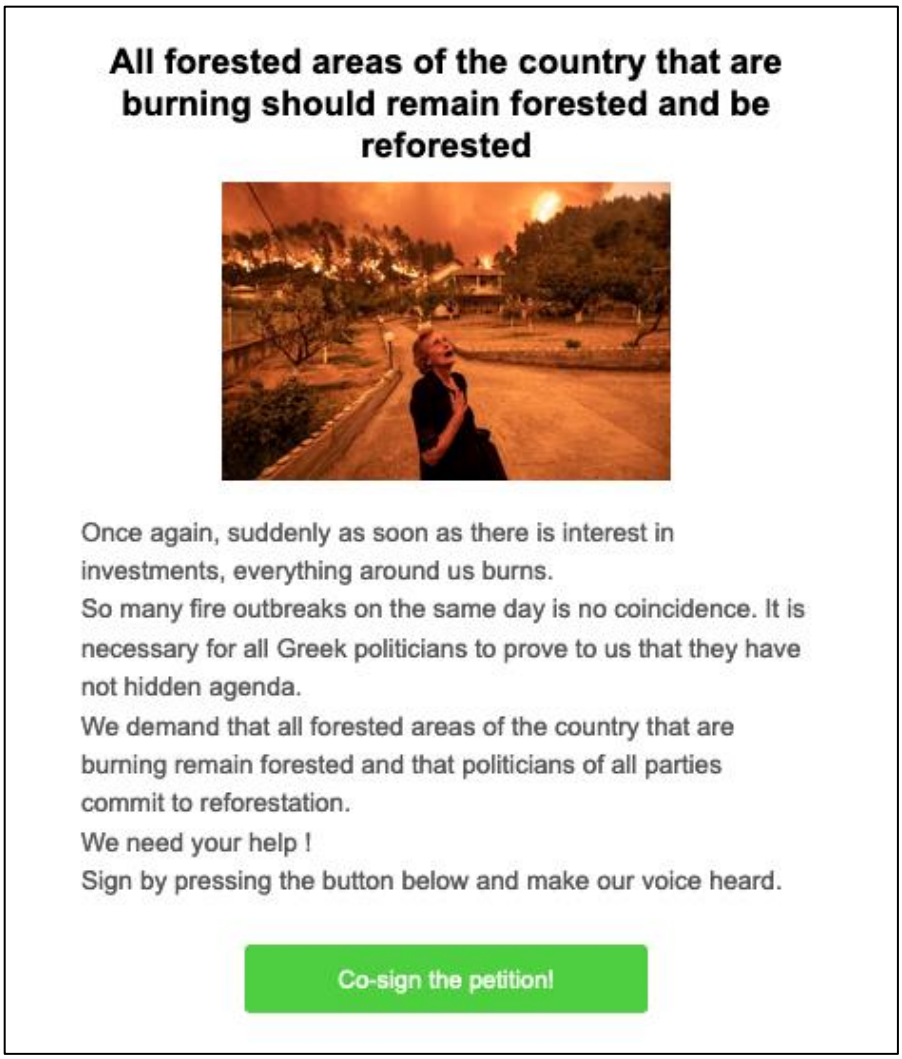


Figure 11: Reforestation e-mail.

Facebook e-mail

Facebook is a well-known and widely used social network and, therefore, resembles a figure of authority. By employing the authority of such an organization along with the content of the mail presented in Figure 12, which implies that an unsuccessful attempt was made to breach the recipients' Facebook account, the authority and scarcity persuasion principle are used.

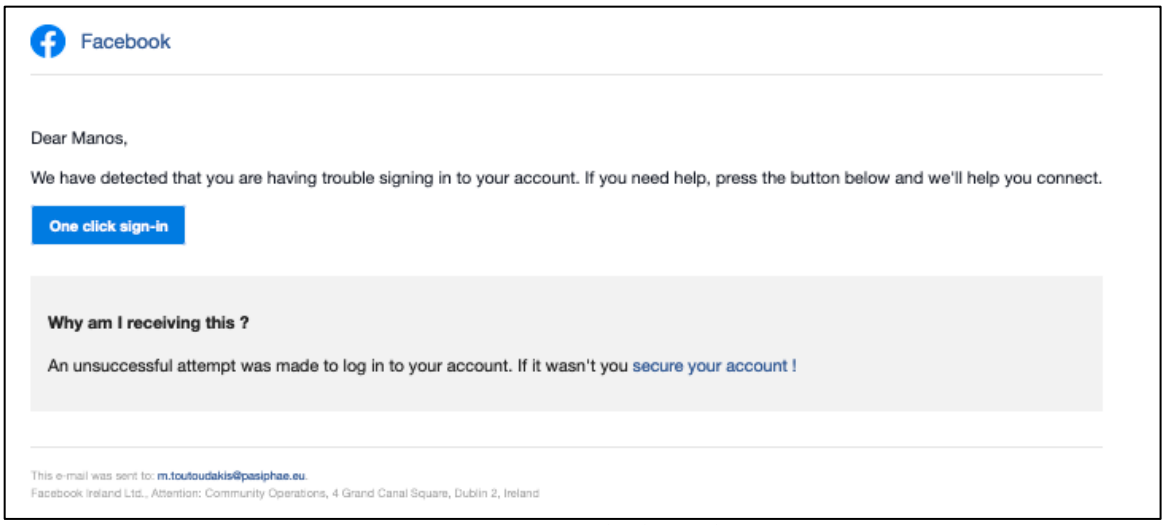


Figure 12: Facebook e-mail.

Instagram e-mail

Following the same approach with the Facebook email, the authority of the Instagram social network is used in the e-mail depicted in Figure 13, aiming to gain the trust and successfully invoke a response from the recipient.

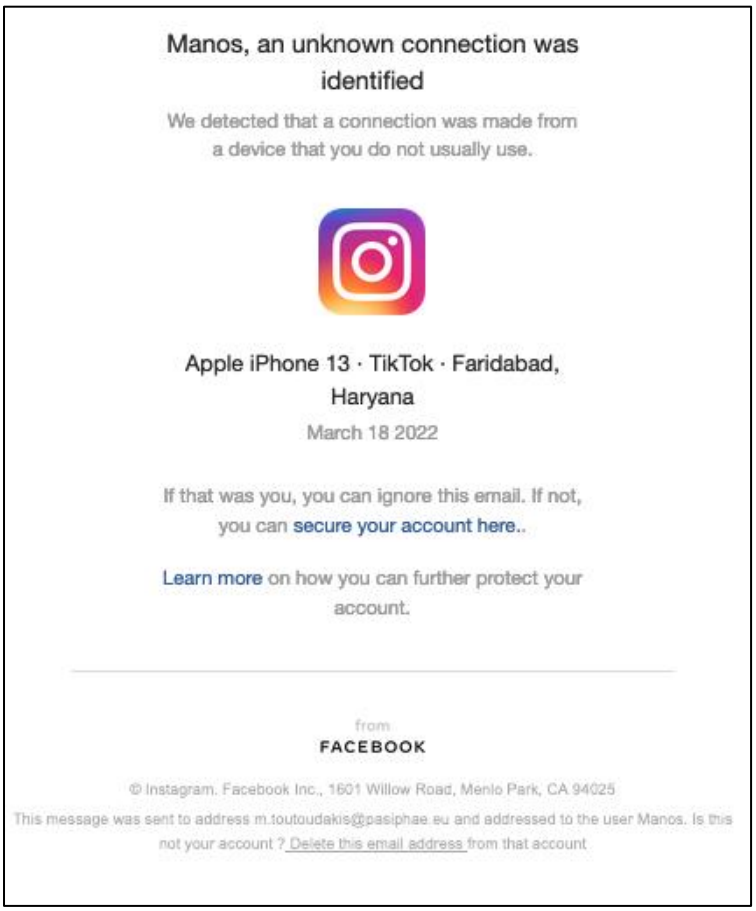


Figure 13: Instagram e-mail.

Revolut e-mail

The authority of a well-known bank organization is also employed in the e-mail presented in Figure 14. Revolut is a worldwide used virtual bank and the following email, by implying an unsuccessful breach attempt, aims to use the authority and scarcity persuasion principles.

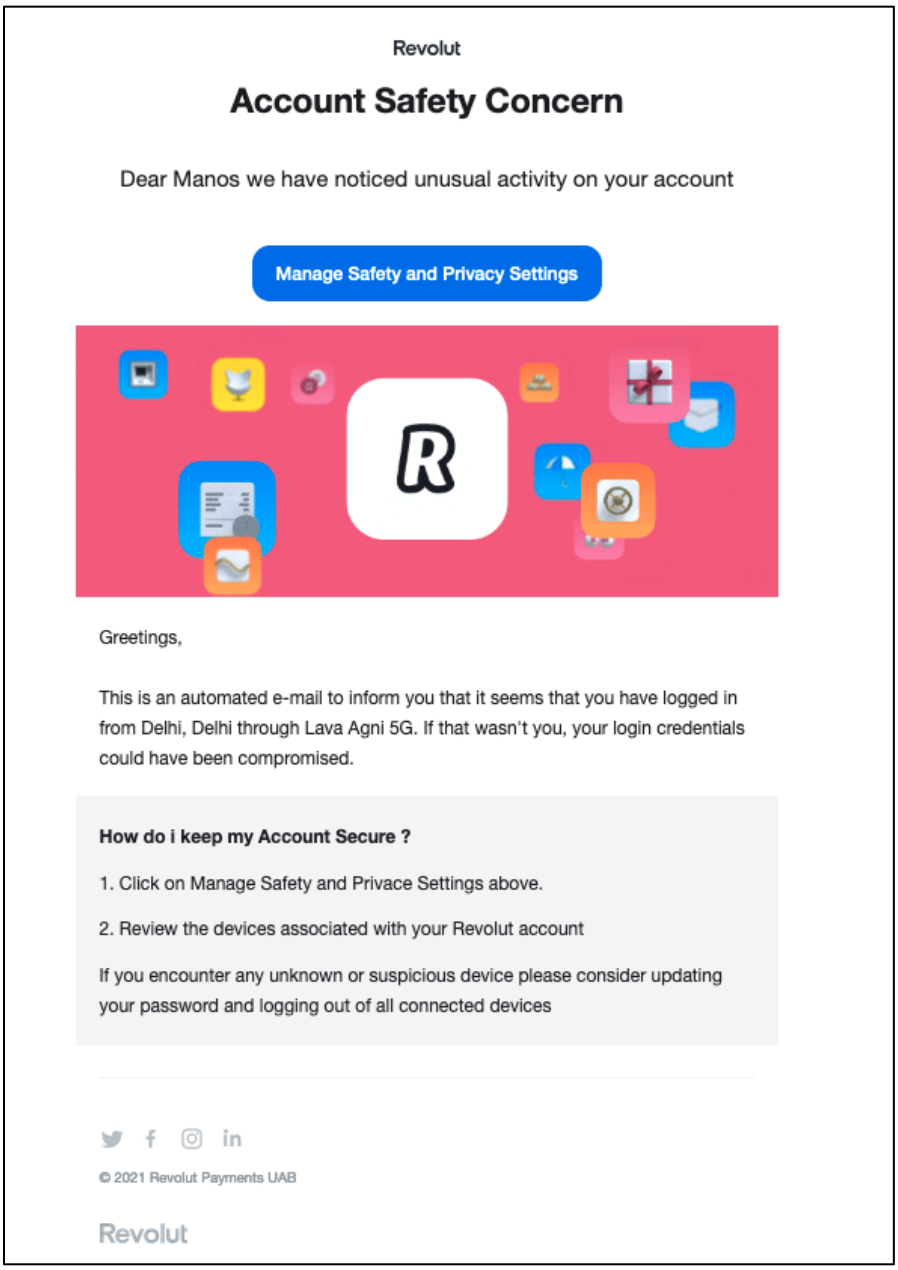


Figure 14: Revolut e-mail.

Win-Bank e-mail

Another well-known bank organization in Greece is Piraeus Bank. The email depicted in Figure 15 contains a fake transaction through Winbank, the electronic platform of Piraeus Bank, and aims to employ the scarcity and authority persuasion principles.

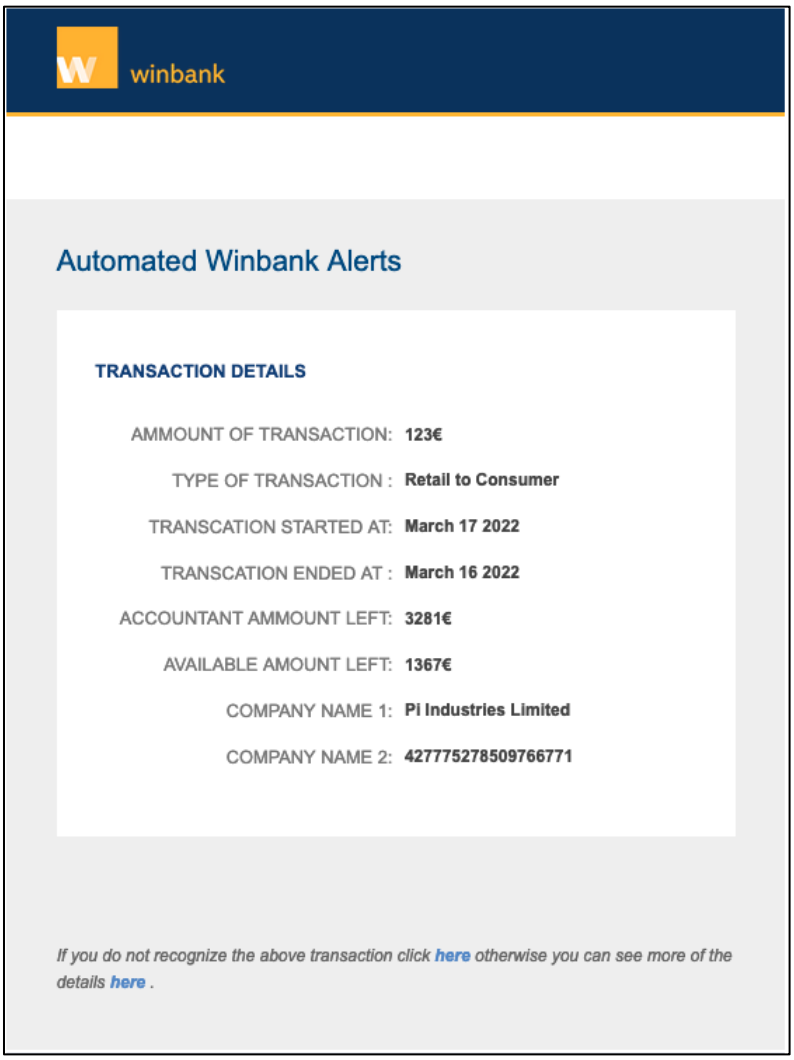
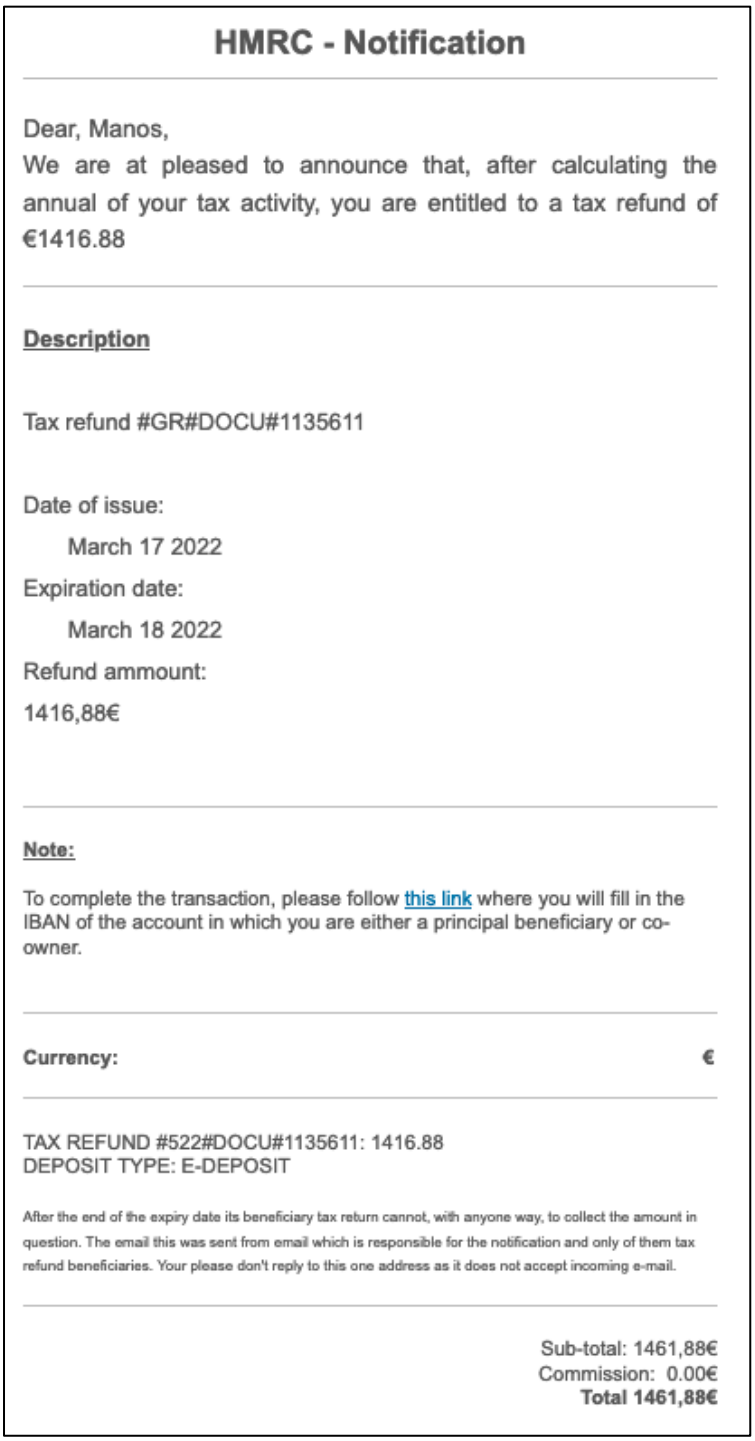


Figure 15: Winbank e-mail.

Tax refund e-mail

In an attempt to invoke the scarcity and reciprocity persuasion principles, the e-mail depicted in Figure 16 informs the recipient that is eligible for tax refund. The reciprocity persuasion principle is invoked by offering the recipient a specific amount of money without asking something in return. Furthermore, by pointing out that the recipient has one (1) day left to complete the transaction before it expires, the scarcity persuasion principle is also used.



HMRC - Notification

Dear, Manos,
We are at pleased to announce that, after calculating the annual of your tax activity, you are entitled to a tax refund of €1416.88

Description

Tax refund #GR#DOCU#1135611

Date of issue:
March 17 2022
Expiration date:
March 18 2022
Refund ammount:
1416,88€

Note:

To complete the transaction, please follow this link where you will fill in the IBAN of the account in which you are either a principal beneficiary or co-owner.

Currency: €

TAX REFUND #522#DOCU#1135611: 1416.88
DEPOSIT TYPE: E-DEPOSIT

After the end of the expiry date its beneficiary tax return cannot, with anyone way, to collect the amount in question. The email this was sent from email which is responsible for the notification and only of them tax refund beneficiaries. Your please don't reply to this one address as it does not accept incoming e-mail.

Sub-total: 1461,88€
Commission: 0.00€
Total 1461,88€

Figure 16: Tax refund e-mail.

Fashion newsletter

The e-mail presented in Figure 17, in an attempt to employ the reciprocity persuasion principle, offers a free subscription to a newsletter that the recipient otherwise would have to pay in order to subscribe to. Furthermore, by pointing out that over two hundred and fifty thousand

(250.000) individuals have already subscribed, susceptibility to the consensus persuasion principle is targeted.

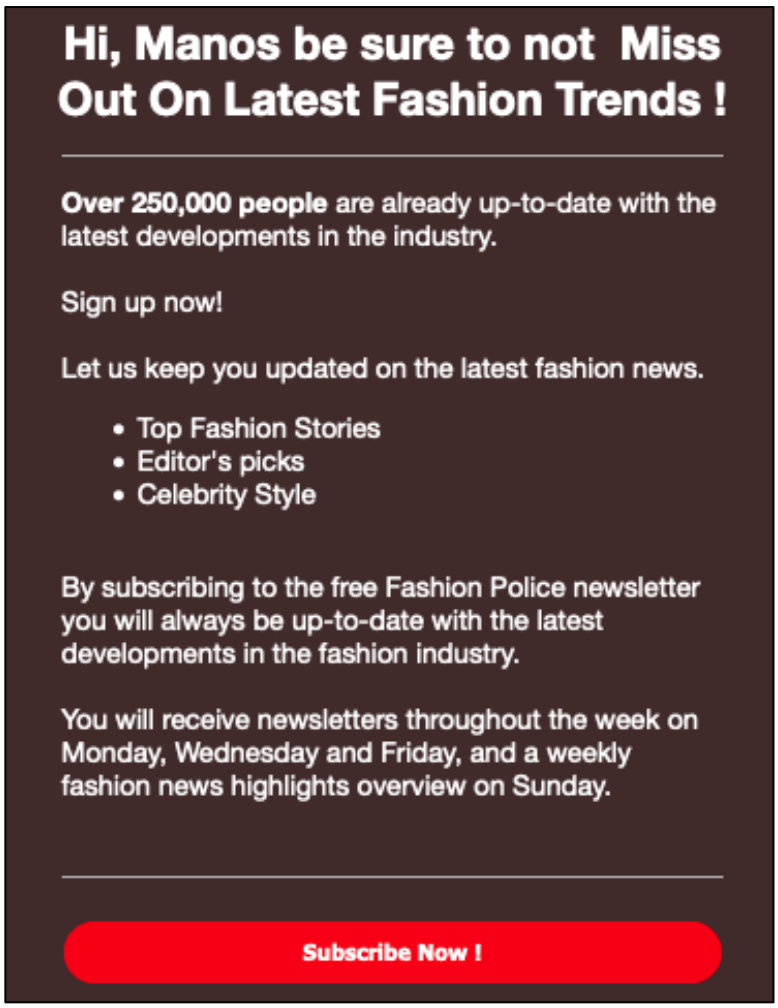


Figure 17: Fashion newsletter email.

Technology newsletter

Following the same approach, the e-mail in Figure 18 was also composed to invoke the feeling of reciprocity to the recipient. Similar to the Fashion newsletter e-mail, a free subscription to a technology themed newsletter is offered to the recipient.

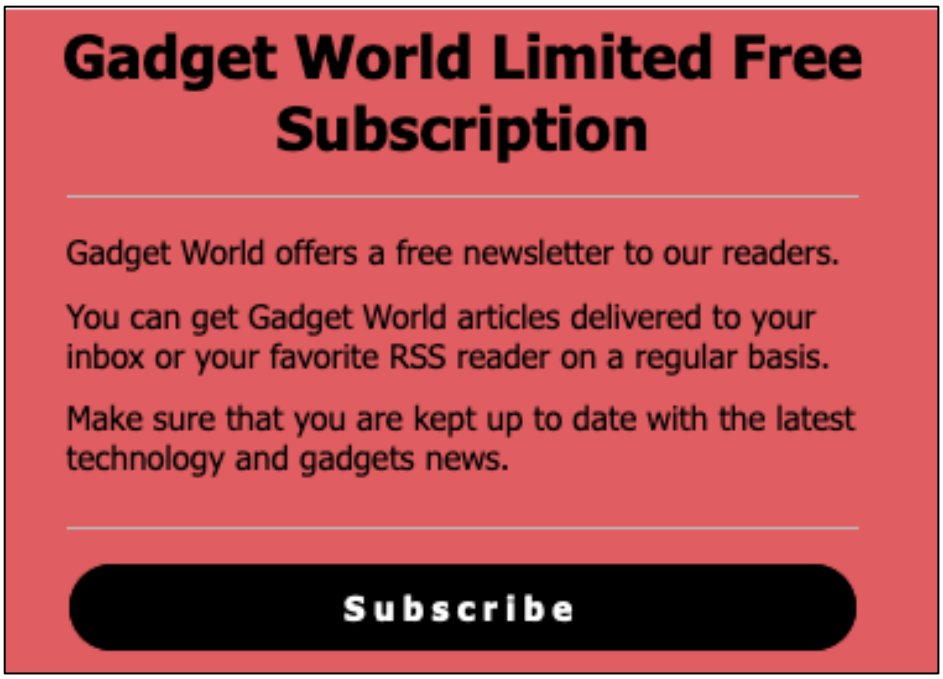


Figure 18: Technology newsletter e-mail.

Landing Pages

The links that were contained to each of the composed e-mails led to their corresponding landing pages. For example, the link contained in the Winbank e-mail presented in Figure 15, led to a clone of the webpage of Piraeus Bank depicted in Figure 19: Winbank website clone., through which the event of submitting credentials is enumerated. Other examples of such landing pages, clones of legitimate, can be found in Annex I.

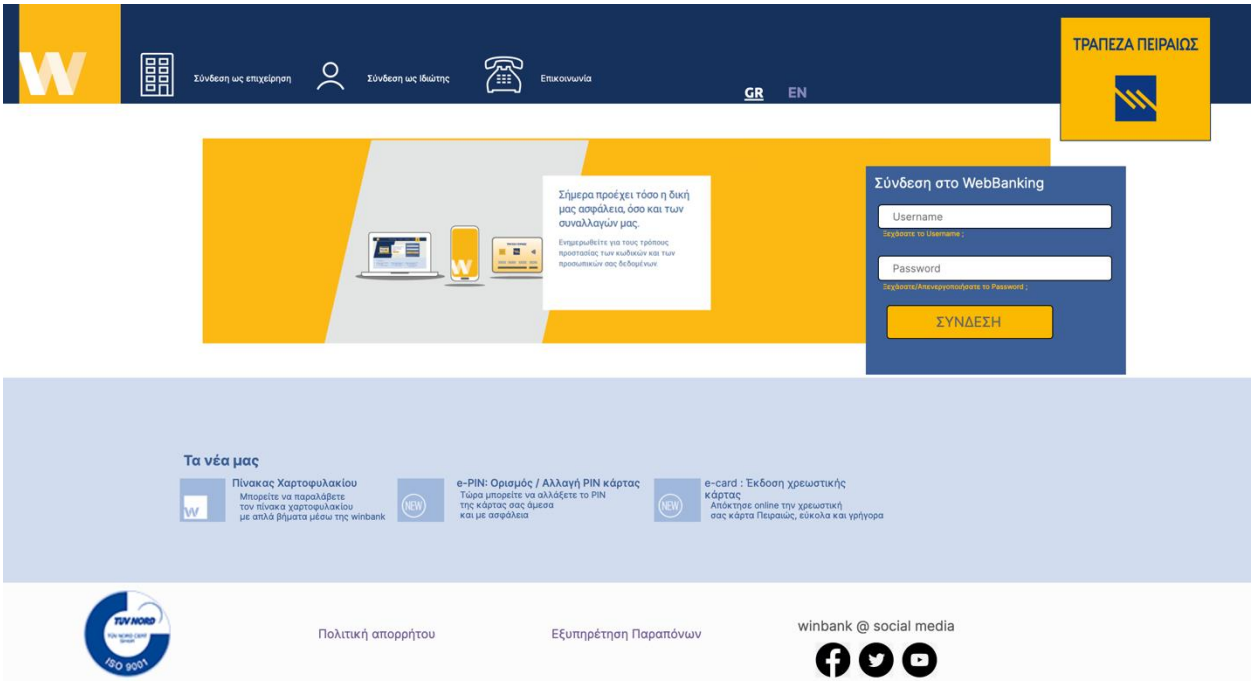


Figure 19: Winbank website clone.

4.3 Translation of a Simulated Phishing Campaign in RPA tasks.

The translation of the process in RPA tasks involves breaking down the Simulated Phishing Campaign into smaller, independent tasks that can be combined to form the entire process. These tasks were designed to be reusable in order to create additional RPA processes. To create these tasks, the same steps that a human operator would take to conduct the campaign were followed.

Specifically, before the conduction of the campaign, the first step a human operator would take would be to specify when the campaign will start and for how long it would last. For fulfilling these requirements, the first task of the RPA process asks the end-user the starting and ending dates of the campaign. Additionally, it requests the user to name the campaign, which is necessary due to the support of multiple and parallel campaigns.

For the next task of the process, after the duration of the campaign is defined, the human operator should know the mailing list of the targets of the campaign. For the mailing lists to be disseminated to external parties, a non-disclosure agreement would be required. In the case of the proposed solution this issue is avoided by accessing the already existing LDAP system of the infrastructure in which the campaign will be conducted. By logging in through the RPA framework, the Campaign Initiator does not need to share the mailing list of the personnel. Thus, the second task is the connection to the LDAP system.

Since the targets and the duration of the campaign are defined, the campaign is ready to start. However, an additional task was added for confirmation purposes. In this step the end-user can confirm that the mailing list is fetched properly from the LDAP system as well as review the parameters of the campaign, such as the name and duration. If everything is properly configured, then the campaign is initiated.

Finally, a task to present the results of the Simulated Phishing Campaign was included to represent the manual report a human operator would compose. In this step, the Campaign Initiator submits an email address to which the post-campaign report will be sent.

5. Evaluation

To evaluate the proposed solution of this thesis, an experiment was conducted where a Simulated Phishing Campaign ran over a period of one week, during which phishing emails were sent to a sample of colleagues. The results of the experiment will be used to determine the feasibility of automating simulated phishing campaigns through RPA in a real-world environment. This chapter documents the whole operation from the deployment of the system until the receival of the post-campaign report.

5.1 External dependencies deployment

The proposed system has two external dependencies, namely, an LDAP Server containing the details of the personnel and an SQL database that stores system-related information such as names and dates of the campaigns.

The LDAP Server was instantiated and filled with information from 10 colleagues. This information regarded their email address as well as their first and last name. The server was deployed at the internal part of the infrastructure (not exposed to the internet) before being accessible by external entities, due to security reasons.

Similar to the LDAP Server, an instance of an SQL database was also deployed infrastructure-internally since it was required for the proposed system to function. Since the tables and data are generated dynamically during the runtime of the proposed system, no initial configuration was necessary.

5.2 Initiation of the Simulated Phishing Campaign.

Once the external dependencies of the system are resolved, the Frontend of the RPA Framework is accessible. Through this frontend, the operation of the Simulated Phishing Campaign will be described as distinct RPA tasks. As displayed in Figure 20, the operation of Simulated Phishing Campaign is composed of 6 distinct steps. After the *"Start"* task, which defines the start of an RPA Framework process, the necessary steps for the automation of the Simulated Phishing Campaign are "*Campaign Start"*, "*LDAP Set Up"*, "*Send Mail"* and "*Generate Report".* The steps "*Connect to HV"* and *"Arsenal and Targets"* were added to complement the proposed system and for confirmation purposes, respectively, as it will be explained further below.

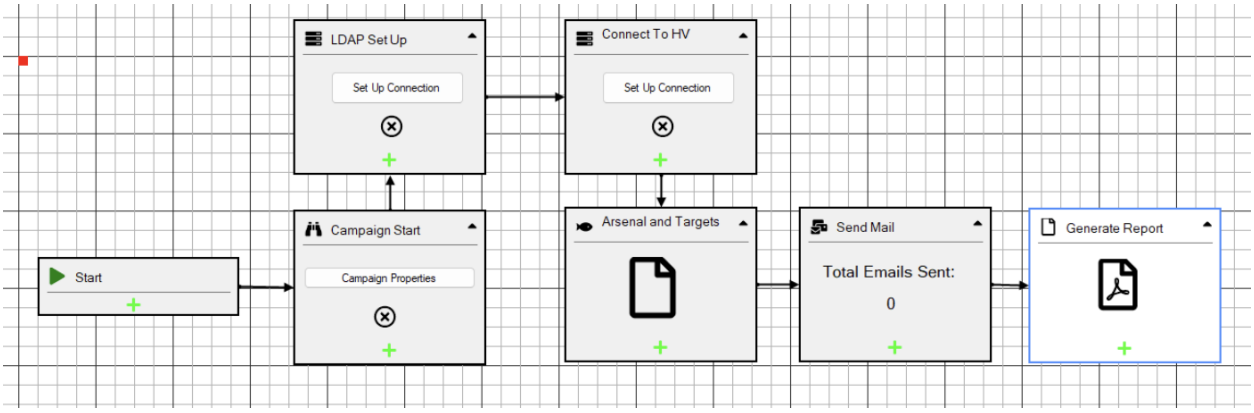


Figure 20: The process of a Simulated Phishing Campaign

Once the necessary as well as complementary tasks are placed in the correct order the next step is the configuration of the steps, where this is required. Tasks that require configuration contain a circled "X" in their body indicating that further actions are required. The first step in the order that requires input is the *"Campaign Start" task.*

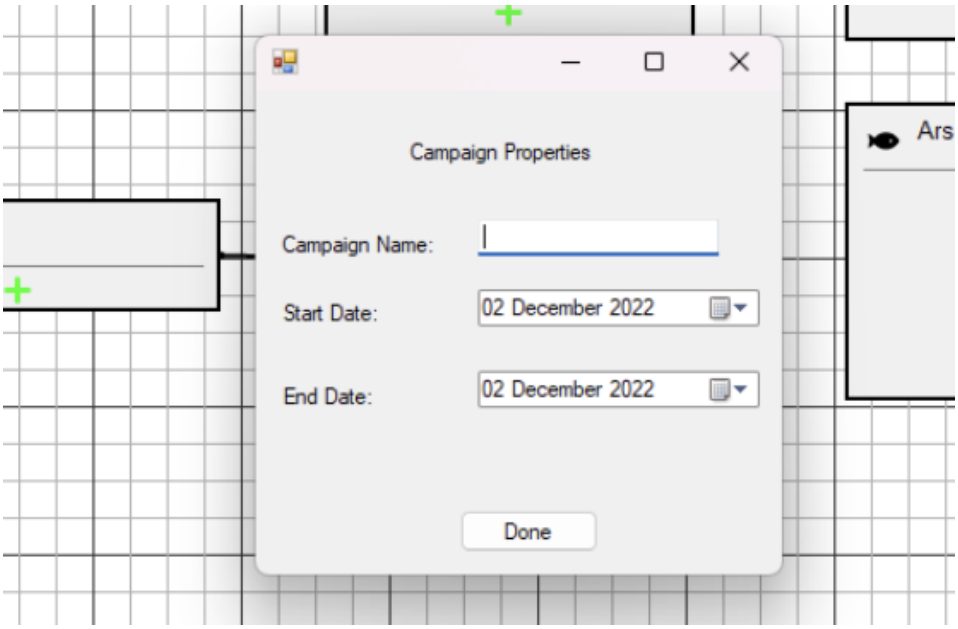


Figure 21: Campaign start: pop-up

The pop-up window depicted in Figure 21 appears when the *"Campaign properties"* option is clicked. Through this pop-up the Campaign Initiator submits the duration and name of the campaign. When the properties are defined, the circled "X" is replaced by a green checkmark indicating the successful configuration of the task.

Similar to the *"Campaign Start"*, as presented in Figure 22, the *"Connect to LDAP"*, "*Connect to HV"*, and *"Generate Report"* tasks gather their input through a dedicated pop-up window and when the configuration of each is successful the Campaign Initiator is also informed through a green checkmark on each tasks body. The successful configuration of all tasks of the RPA Process will display the available Targets in the *Arsenal and Targets* task. After reviewing that the Simulated Phishing Campaign contains the proper Targets the end user can initiate the operation.

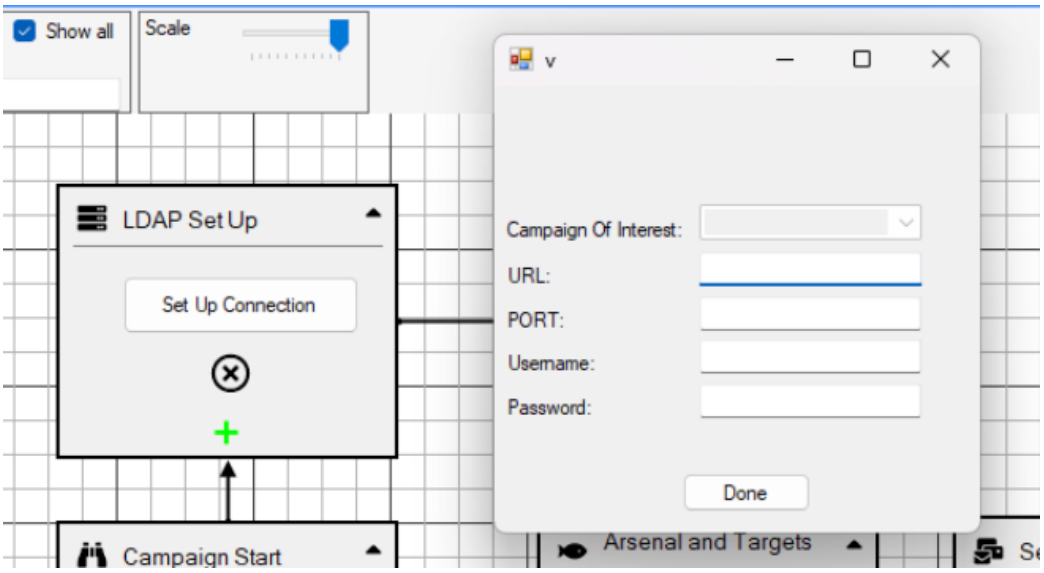


Figure 22: Connect to LDAP: pop-up

5.3 Results of the Simulated Phishing Campaign experiment

In the experiment conducted to evaluate the feasibility of the solution, the LDAP directory was instantiated with the details of 10 individuals, who became the targets of the campaign. While the campaign was active, a total of 140 phishing mails were sent, out of which 101 were opened. Inside these emails, two different types of links were included. Some emails contained a link that led to a phishing webpage that requested a credential submission, while the rest of the emails included a link that, when the recipient clicked on it, a malicious file was requested. A total of 76 clicks on the malicious webpage URLs was recorded. Out of these 76 visits, 46 times the targeted individuals submitted their credentials. Additionally, a total of 7 malicious file requests were recorded.

A post-campaign report was generated with the collected results, which is showcased in Figure 10 below. The findings of the Simulated Phishing Campaign are presented in the report including both the amount and the types of interactions of the recipients with the phishing emails. Furthermore, a comparison between the initial persuasion susceptibility assessment and the result of the campaign is included in the post-campaign report, showcased in the form of bar charts, providing valuable insights regarding susceptibility to persuasion as it stems from the initial assessment and the actual susceptibility recorded through the campaign. However, the

interpretation of this comparison as well as the reason of the differences identified between the results of the two assessments is out of the scope of this thesis.

The results of the experiment showed that the automated Simulated Phishing Campaign was effective in attracting interactions as well as enumerating them.

Automatically Generated Report for "PilotCampaign" Campaign:

Report Overview:

Total e-mails sent:	140
Total emails opened	101
Total malicious links clicked	76
Total credentials submitted	46
Total file downloads	7

Statistic Analysis:

72% of the phishing mails sent were opened.

54% of the malicious links was clicked

32% of the mails harvested credentials successfully.

5% of the malicious files were downloaded.

Campaign Description:

Campaign Named : PilotCampaign started at 17/3/2022 and the last email was sent at 23/3/2022 signaling the end of the campaign.

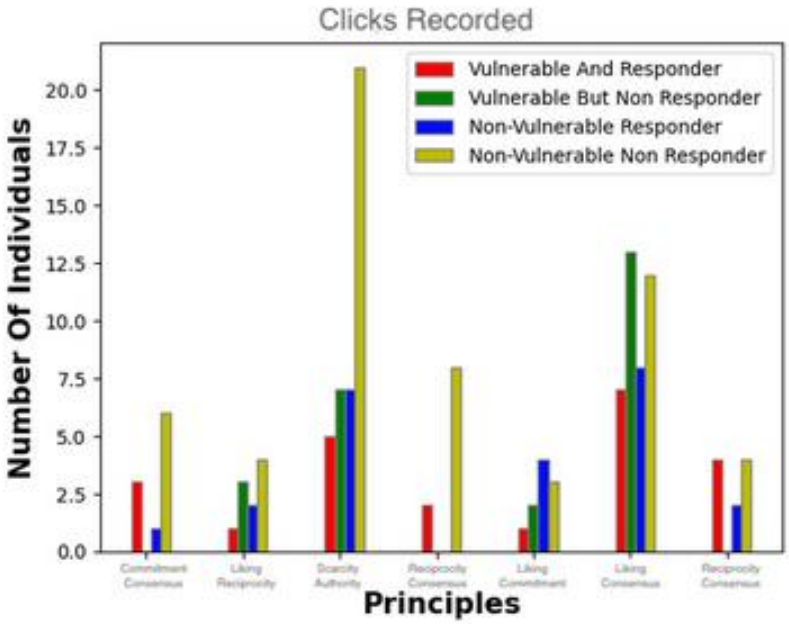
Throughout the campaign 10 individuals were tested with a total of 140 mails. All participants recieved exactly the same mails in order the test to be as objective as possible.

Findings:

While the campaign was active, a total of 101 phishing mails were opened out of the 140 that were originally sent. Inside those emails, two kinds of links could be included. One that led on a "malicious" webpage and one that requested an equally could-be-malicious file. We enumerated a total of 76 clicks on the malicious webpage URLs, of which 46 individuals went on to submit their credentials on the particular webpage. The malicious file requests were counted at a total of 7.

"malicious" webpage and one that requested an equally could-be-malicious file. We enumerated a total of 76 clicks on the malicious webpage URLs, of which 46 individuals went on to submit their credentials on the particular webpage. The malicious file requests were counted at a total of 7.

Interaction Figures:



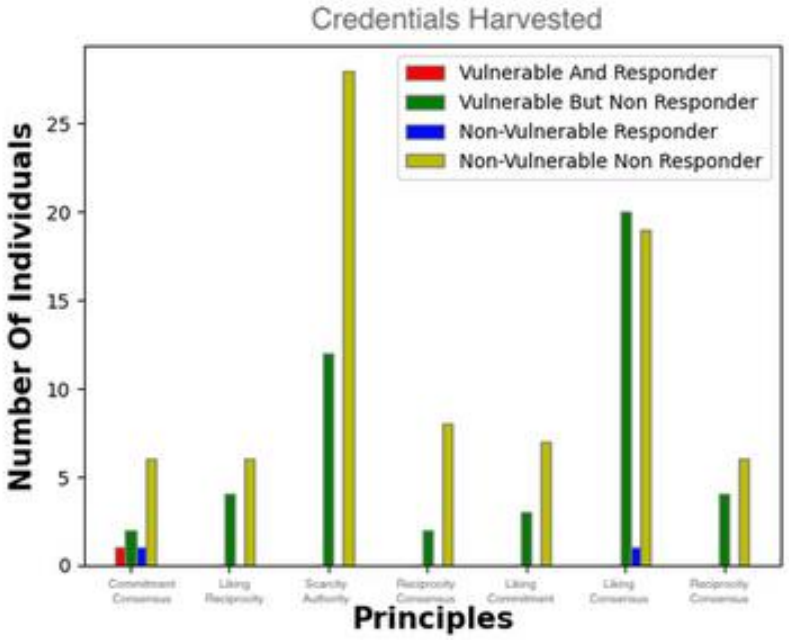


Figure 23: The post-campaign report

5.4 Discussion

Overall, the results of the experiment support the feasibility and potential effectiveness of automating through RPA the process of Simulated Phishing Campaigns. However, further research is needed to confirm these findings and to explore the potential limitations and risks of automating simulated social engineering attacks through RPA for cybersecurity awareness assessment.

The proposed solution does not come without some limitations, which should be considered when interpreting the results. Specifically, the sample size of the evaluation experiment was relatively small, and the same operation with a larger sample size may have yielded completely different results regarding target susceptibility rates. Additionally, the targets of the Simulated Phishing Campaign were individuals with knowledge in the cybersecurity domain, which may have affected their phishing email awareness and, thus, their behavior and response to the phishing emails of the campaign. A larger and more diverse sample may provide additional insights in light of the effectiveness of Simulated Phishing Campaigns as a phishing awareness assessment method as well as aid in unravelling the reason for the disparity in susceptibility results between the initial persuasion susceptibility assessment of the targeted individuals and the individuals' actual susceptibility to phishing emails employing such persuasion techniques.

6. Conclusion

This thesis explored further applications of the RPA technology in the realm of cybersecurity and proposed the automation of Simulated Phishing Campaigns through RPA.

By describing the process of a Simulated Phishing Campaign in distinct subsequent steps and developing the corresponding User Interface as well as the necessary backend functionality, a prototype system was presented. The proposed system is capable of attracting and enumerating the amount and types of interactions conducted by the personnel of an ICT infrastructure, who are the targets of the campaign. Furthermore, to evaluate the proposed modularity of an RPA automated operation, the results of an initial persuasion susceptibility assessment were parsed as input to the Simulated Phishing Campaign. The results of the campaign were compared with this initial assessment, providing a more realistic evaluation of the susceptibility of the targets of the campaign, since the actual behavior of the targets towards phishing emails was recorded.

Next steps towards the enhancement of the proposed system include further expansion to discover and evaluate additional automation of cybersecurity operations through RPA such as open-source intelligence (OSINT) operations concerning the Targets of the campaign as well as automation of the initial persuasion susceptibility assessment to result in a more comprehensive solution.

7. References

[1] N. Klimburg-Witjes and A. Wentland, "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," *Science Technology and Human Values*, vol. 46, no. 6, pp. 1316–1339, Nov. 2021, doi: 10.1177/0162243921992844.

[2] O. Zielinska, A. Welk, C. B. Mayhorn, and E. Murphy-Hill, "The persuasive phish," Apr. 2016, pp. 126–126. doi: 10.1145/2898375.2898382.

[3] *2755-2017 - IEEE Guide for Terms and Concepts in Intelligent Process Automation*. IEEE, 2017.

[4] V. K. Suri, M. D. Elia, P. Arora, and J. van Hillegersberg, "Automation of Knowledge-Based Shared Services and Centers of Expertise," 2019, pp. 56–75. doi: 10.1007/978-3-030-15850-7_4.

[5] S. Adhikari and C. Davis, "Reinforced learning and robotic automation based Cybersecurity," Jun. 2020. doi: 10.2514/6.2020-2929.

[6] E. B. Blancaflor *et al.*, "Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools."

[7] J. Dreese, "Phishing with a License: Measuring the Susceptibility of Students to Phishing Attacks by Developing a Phishing Simulation." [Online]. Available: http://www.ucl.ac.uk/cert/antiphishing/.

[8] A. Ferreira, L. Coventry, and G. Lenzini, "Principles of Persuasion in Social Engineering and Their Use in Phishing," Lecture Notes in Computer Science. Springer International Publishing, pp. 36–47, 2015. doi: 10.1007/978-3-319-20376-8_4.

[9] A. Karakasiliotis, S. M. Furnell, and M. Papadaki, "Assessing end-user awareness of social engineering and phishing," Proceedings of 7th Australian Information Warfare and Security Conference, 2006, doi: 10.4225/75/57A80E47AA0CB.

[10] W. Yeoh, H. Huang, W.-S. Lee, F. Al Jafari, and R. Mansson, "Simulated Phishing Attack and Embedded Training Campaign," Journal of Computer Information Systems, vol. 62, no. 4. Informa UK Limited, pp. 802–821, Aug. 30, 2021. doi: 10.1080/08874417.2021.1919941.

[11] R. B. Cialdini and B. J. Sagarin, 'Principles of Interpersonal Influence', 2005.

8. Annex I

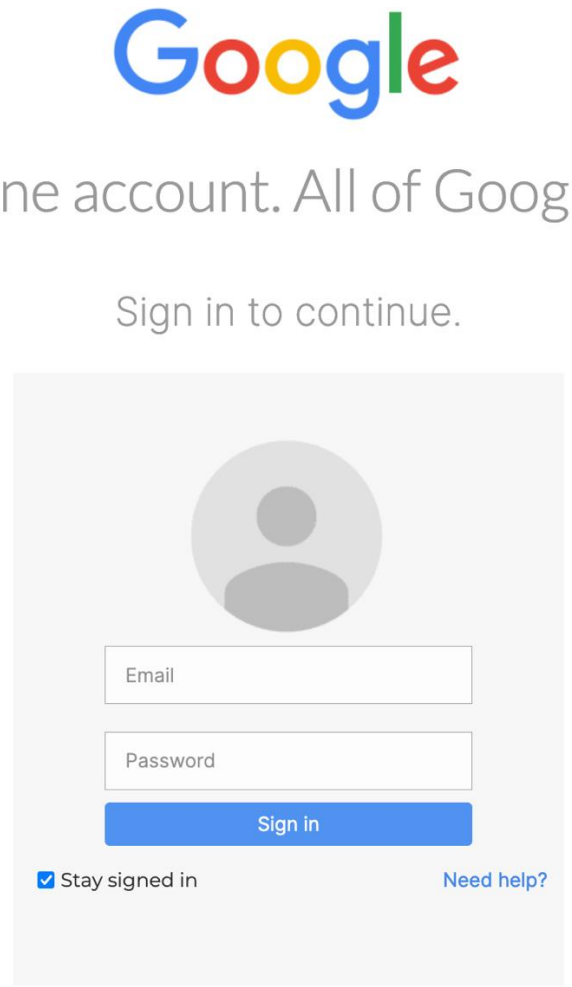


Figure 24: Google sign-in clone.

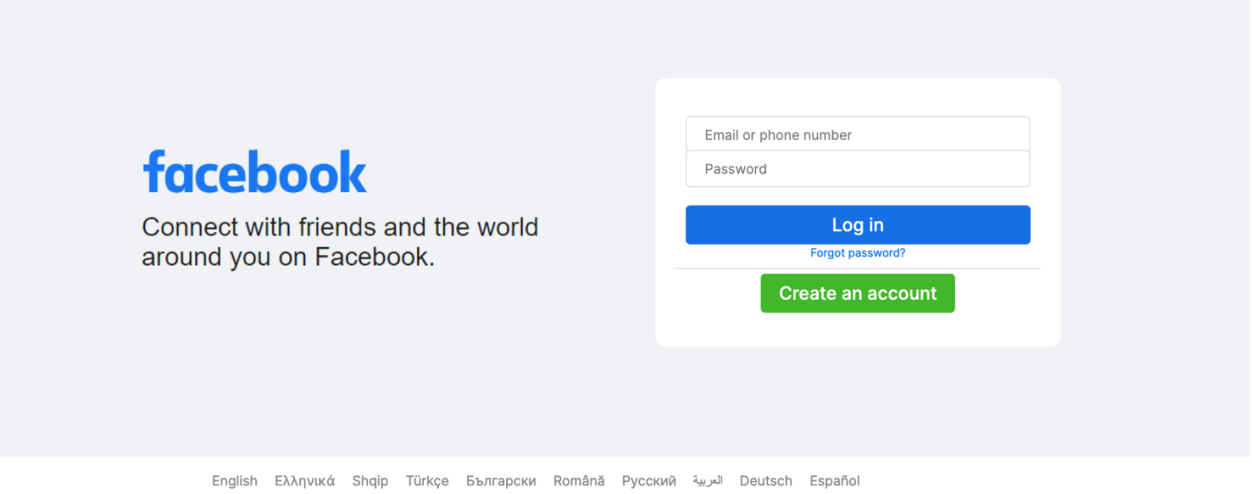


Figure 25: Facebook website clone.

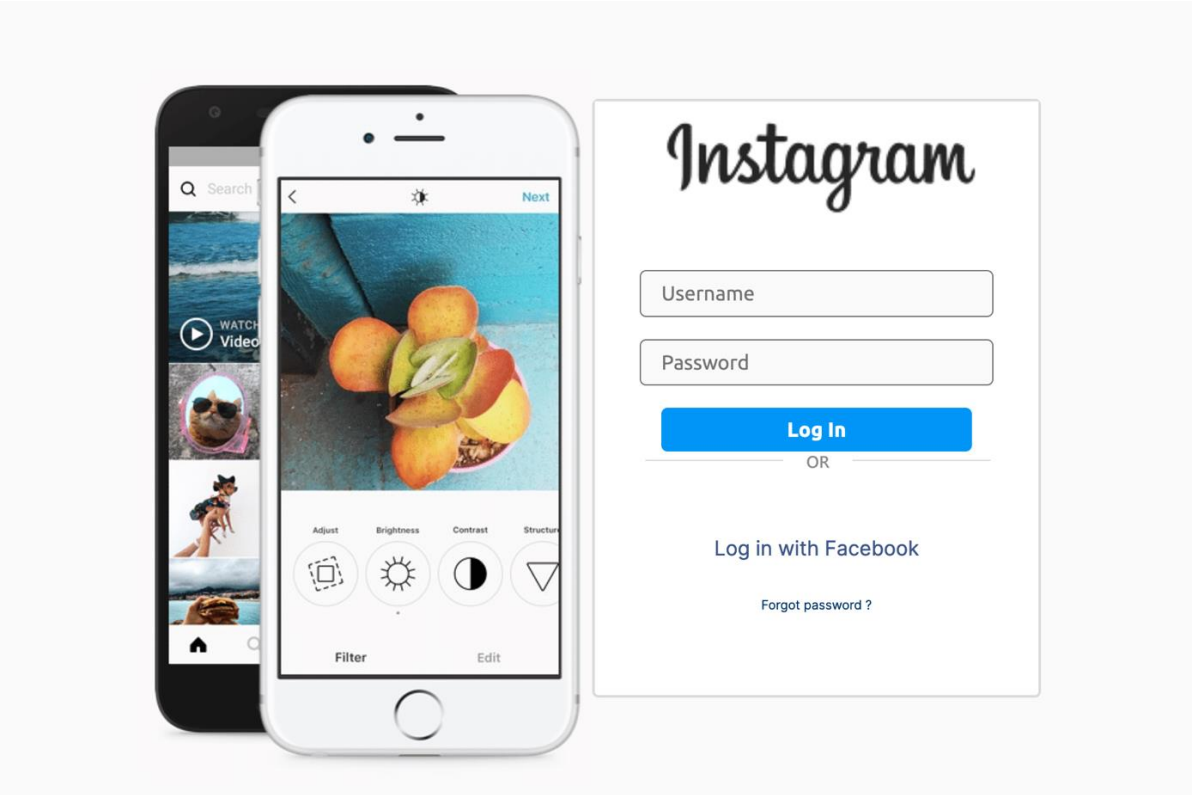


Figure 26: Instagram sign-in clone.

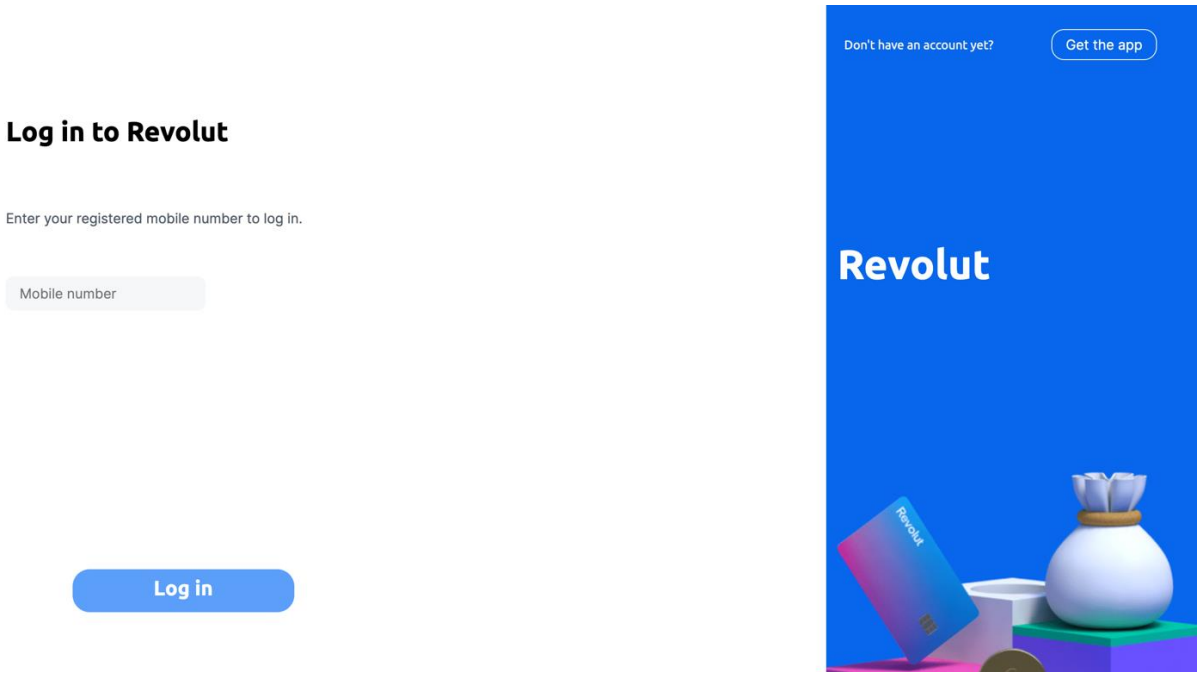


Figure 27: Revolut sign-in clone.