

# Guarding Against Deception: A Traffic Light System for Detecting phishing Emails

By

Rohan Dina Nath B01122462

Computing in Digital Forensics and Cyber Security

Technology University Dublin

Supervisor : Mark Lane

12<sup>th</sup> of May 2023

# Table of Contents

Table of Figures .....	3
Acknowledgement .....	4
Abstract.....	4
1. Introduction .....	5
1.1 Aims .....	6
1.3 Research Questions .....	6
1.4 Chapter Overview .....	6
2. Background and related technology .....	9
2.1 Defining Phishing Emails .....	9
2. Historical Development of Phishing Emails .....	9
3. The Latest Statistics of Phishing attacks .....	11
3.1 Phishing Attack Trends.....	11
3.2 Impact of Phishing Attacks.....	12
4. Real World Phishing Attacks .....	13
5. Phishing Techniques .....	14
5.1 Deceptive Phishing .....	14
5.1.1 Phishing E-mail.....	15
5.1.2 Spoofed Website .....	15
5.1.3 Phone Phishing (Smishing) .....	16
5.1.4 Spear phishing .....	17
5.1.5 Social Media Attack (Soshing, Social Media Phishing) .....	18
5.2 Technical Subterfuge .....	19
5.2.1 Malware-Based Phishing.....	19
5.2.2 Whaling .....	19
5.2.3 DNS-Based phishing .....	20
5.2.3 Contect Injection.....	21
5.2.4 Man-in-the-Middle.....	22
5.2.5 Search Engine Phishing .....	23
5.2.6 URL Attacks .....	24
6. Literature Review .....	25
6.1 Introduction .....	25
6.2 Content-based Filtering .....	25
6.3 Sender Reputation .....	26
6.4 Email Authentication and Encryption .....	27

6.5 Challenges and Limitations .....	27
6.6 Gmail Filtering System .....	28
6.6.1 Machine Learning-Based filtering – Gmail .....	29
6.6.2 Sender Reputation and Domain-based Filtering - Gmail .....	29
6.6.3 Community Signals and Collaborative Filtering - Gmail.....	30
6.6.4 Challenges and Limitations - Gmail.....	30
7 Methodology.....	31
7.1 Introduction .....	31
7.2 Survey.....	31
7.2.1 Questions .....	31
7.2 Phishing email Anatomy .....	33
7.3 Pyphisher.....	34
8 Results.....	36
8.1.1 Survey Results .....	36
8.1.2 Overall.....	42
8.2 Phishing email Testing .....	43
8.2.1 Testing with Pyphisher.....	43
Figure 19 shows that the next step in the study was to check the link with two security tools, VirusTotal and URL Scanner. The point of these sites is to make sure the link is real by checking it. After a close look, it was clear that the link didn't follow the rules of a real connection. This shows that it was made up. ....	45
Fake Links:.....	45
Spam Links .....	46
Fake Links from Spam .....	47
9. Conclusion .....	49
9.1 Answering the Questions.....	50
Referencing.....	52

## Table of Figures

Figure 1 Last 5 years.....	11
Figure 2 Statics figures .....	12
Figure 3 Type of Phishing attacks.....	14
Figure 4 Spear Phishing attack.....	17
Figure 5 Pyphisher .....	34
Figure 6 Q1- How often do you receive phishing emails? .....	36
Figure 7 Q2 - Have you ever fallen for a phishing email? .....	37
Figure 8 Q3 - How confident are you in your ability to identify a phishing email? .....	37
Figure 9 Q4 - What types of emails do you think are most likely to be phishing attempts?.....	38
Figure 10 Q5 - Have you ever reported a phishing email to your IT department or security team? ...	38
Figure 11 Q6 - How do you think companies can better educate their employees about phishing emails? .....	39
Figure 12 Q7 - How do you typically respond to a suspected phishing email? .....	40
Figure 13 Q8 - What do you think are the biggest challenges in preventing phishing attacks?.....	40
Figure 14 Q9 - Have you ever had to deal with the consequences of falling for a phishing email, such as identity theft or financial loss? .....	41
Figure 15 Pypisher (facebook) .....	43
Figure 16 Creating a Facebook link .....	44
Figure 17 Facebook prototype.....	44
Figure 18 Email sent to me .....	45
Figure 19 results of the Facebook.....	45
Figure 20 Spam emails .....	46
Figure 21 link to my email.....	47
Figure 22 checked with my tool.....	47

## Acknowledgement

Many importantly, I would like to thanks to my parents that have supported me thought out the semester. I would like to say thank to my girlfriend (Simone) who believed in me especially this year. Without her I would have not made it this far. I would like to thank my brother who helped me with the coding without him I would have been lost and confused. I have gained more knowledge in terms of coding in cyber security.

I would like the thank Mark Lane for supporting me throughout the semester and believing in me doing this project. The guidance Mark gave was outstanding and couldn't thank Mark enough.

Finally, I want to thank all my friends and family who understood my struggle this year.

## Abstract

The goal of this thesis was to make an app that protects against phishing emails in an easy-to-use way. The app uses the Virus Total and URLS scan databases to find possible scam URLs. The results are shown as a simple set of traffic lights.

This work helps stop unauthorised entry by giving non-technical users an easy-to-use tool and pointing out places where user education could be improved. It shows how everyone can help users spot phishing emails and how important it is to give all users, no matter how tech-savvy they are, the right information and tools.

# 1. Introduction

Phishing email assaults are growing more frequent and can seriously jeopardize company security. According to Stojnic et al., (2021) phishing is a kind of fraudulent behaviour in which a cybercriminal tries to obtain sensitive data from its victims, including usernames, passwords, and information for online banking. An overview of the most recent studies on phishing email assaults and their effects on businesses is what this literature review seeks to do. The most prevalent kind of online crime is phishing.

Every single day, an estimated 3.4 billion phishing emails are sent. In 2021, phishing continued to be a significant threat to European organizations, accounting for 42% of all attacks. This is greater than brute force assaults, which made up 12% of attacks but is significantly less than vulnerability exploitation, which accounted for 46% of attacks. It's important to remember that phishing is a growing threat that companies must protect against as it becomes more prevalent (AAG IT Services, 2023).

Emails that are intended to deceive recipients into giving away sensitive data, such as login passwords or financial information, are known as phishing emails. In order to trick recipients into clicking a link or downloading an attachment, these emails frequently seem to be from reputable sources like banks or well-known corporations.

Email phishing attacks can cause devastating effects on organisation, including data breaches, financial losses and reputational harm. All of these attacks have the potential to lead to the installation of malware on a company's system, which may result in data theft and other cybercrimes.

The practical implications this assessment carries will also encompass the measures that companies can adopt to safeguard themselves against phishing email attacks, including employee training, technological safeguards implementation, and incident response preparedness. This analysis intends to give insights into the best practices for defending enterprises against phishing email attacks by reviewing the current research that is being conducted on the subject of interest. The study will also be explored through quantitative research in the form of online questionnaires.

## 1.1 Aims

The primary goal of a project to implement a traffic signal system to prevent users from engaging on external and internal links would be to enhance cybersecurity and reduce the risk of security breaches resulting from fraudulent attacks. The traffic system would help non-IT users see through the traffic light system. The green suggests it's a safe link, the yellow suggests it's potentially hazardous, and the red link suggests it's malicious and should be flagged to the IT team. The project is to reduce the likelihood of workers falling for phishing emails, which can result in data breaches, financial losses, and reputational damage to organisations.

## 1.2 Objectives

- Develop a traffic signal system for external and internal links
- Train employees to recognize and understand the traffic signal system
- Implement a system that automatically assigns colour codes (green, yellow, red) to links based on their level of risk

## 1.3 Research Questions

The following research questions have been developed to explore the topic of phishing emails and investigate ways to develop resilience against these types of potential threats or cyber-attacks.

How do individuals and organizations typically respond to phishing emails, and what factors influence their response?

How can employee training and awareness programs be developed and implemented to improve resilience against phishing emails within organizations?

## 1.4 Chapter Overview

### **Chapter 2:**

This chapter associated with topics e.g. spear phishing, social media phishing, technical deception, malware phishing, extortion DNS phishing, content injection, man-in-the-middle attacks and URL attacks are discussed in this chapter. The chapter also emphasises several prevention strategies for each attack type, including multi-factor authentication implementation, user education, secure coding practises, and real-time monitoring. Individuals

and organisations can protect themselves from phishing attacks and maintain a more secure online presence by understanding these threats and implementing the appropriate countermeasures.

## **Chapter 3:**

This chapter gives a brief overview of different methods and tools that can be used to identify and stop damaging emails like spam, scams, and phishing efforts. The topics start with content-based screening, which focuses on machine learning methods as well as deep learning methods. The chapter then talks about user reputation systems and the benefits of mixing these systems with content-based screening to improve email filters. It also talks about ways to verify and secure email, like DKIM, SPF, and DMARC. The problems and limits of the email screening methods that are used now are talked about, and then suggestions are made for future study to improve machine learning, AI techniques, and user education. The part ends with a detailed look at Gmail's filtering system, including how it works, what problems it faces, and where it might go in the future.

## **Chapter 4:**

This chapter talks about how important it is to understand and stop hacking attacks, especially for people who don't work in IT. It starts by talking about a poll that was made to find out how non-IT people deal with fake emails, what they know about them, and what problems they face. The goal of the poll is to help organisations come up with better policies, training programmes, and security steps to protect non-IT users from hacking attacks.

The chapter then looks at a Python tool that checks the safety of URLs in Gmail messages to improve email security. The script uses VirusTotal and URLScan.io, which are third-party services, to check the safety of URLs. It then uses a "traffic light" method to show how safe each URL is. This tool helps people avoid links that could be dangerous, making email safer.

The chapter ends by talking about PyPhisher, a Python-based tool that security experts and penetration testers can use to model real-life phishing attacks. The tool helps users find weak spots in their own or their organization's security, so they can shore up their defences. PyPhisher is easy to use and can practise different types of phishing attacks, such as gathering passwords, distributing software, and manipulating people.



## Chapter 5

The phishing email study and tests show how people have dealt with and responded to scam emails. This shows how important it is to raise knowledge and educate people about this important problem. Most of the people who answered the question get scam emails between one and three times a month. Even though most people don't fall for them or have bad things happen because of them, some have lost money or had their identities stolen because of phishing attacks. Many of the people who answered the poll didn't feel confident in their ability to spot scam emails, which shows that more people need to know about them and learn how to spot them. People think that the biggest problem with stopping these acts is that not enough people know about them.

Companies can help their employees learn more about security by giving them regular security training, hacking drills, and learning tools. Most people who get what they think is a fake email delete it without clicking on any links or files. But a large number of responders don't know if an email is a phishing attempt. This could be because phishing techniques change all the time and it's hard to find and catch attackers.

To learn more about phishing emails, the author used the Pyphisher social engineering tool to send themselves emails with fake links, including links to popular sites like Facebook, Messenger, Twitter, LinkedIn, Outlook, Spotify, and eBay. Also, the author tried links from their junk Yahoo email to see if they would be marked as suspicious. All of them were marked as yellow, which means they shouldn't be clicked on and should be reported to the IT team.

## 2. Background and related technology

This background review looks at the trends, effects, and methods of phishing attacks, which are still a major threat to safety around the world. As a result of the COVID-19 virus, more people are using technology. This gives hackers more chances to take advantage of weaknesses in online systems. A lot of data breaches are caused by phishing, which can cause businesses to lose money and have private information get into the wrong hands. We talk about real-world cases of phishing scams and the different types of phishing, like false phishing, email phishing, fake websites, smishing, spear phishing, and social media phishing. Understanding these dangers is important if you want to put in place effective solutions and best practises to reduce risks and keep people and organisations safe.

### 2.1 Defining Phishing Emails

Phishing emails are fake messages that look like they came from a reliable source. They are meant to trick people into giving out personal information, like passwords and credit card numbers, or downloading malware (National Cyber Security Centre, 2021). The word "phishing" comes from the word "fishing," which is what attackers do to get private information from people who don't know what's going on (FraudWatch International, 2017). These tactics often use "social engineering" to take advantage of people's weaknesses and trick them into doing things that are bad for their security.

### 2. Historical Development of Phishing Emails

Phishing attacks have been around since the mid-1990s, when hackers pretended to be system admins and asked AOL users for their passwords (Trend Micro, 2016). The word "phishing" was used for the first time in 1996 on the hacking tool AOHell, which made it easy to send fake emails to AOL users. Phishing attacks have become more sophisticated over time and now target a wider range of businesses, such as banks, e-commerce sites, and social media sites (Kaspersky, 2021).

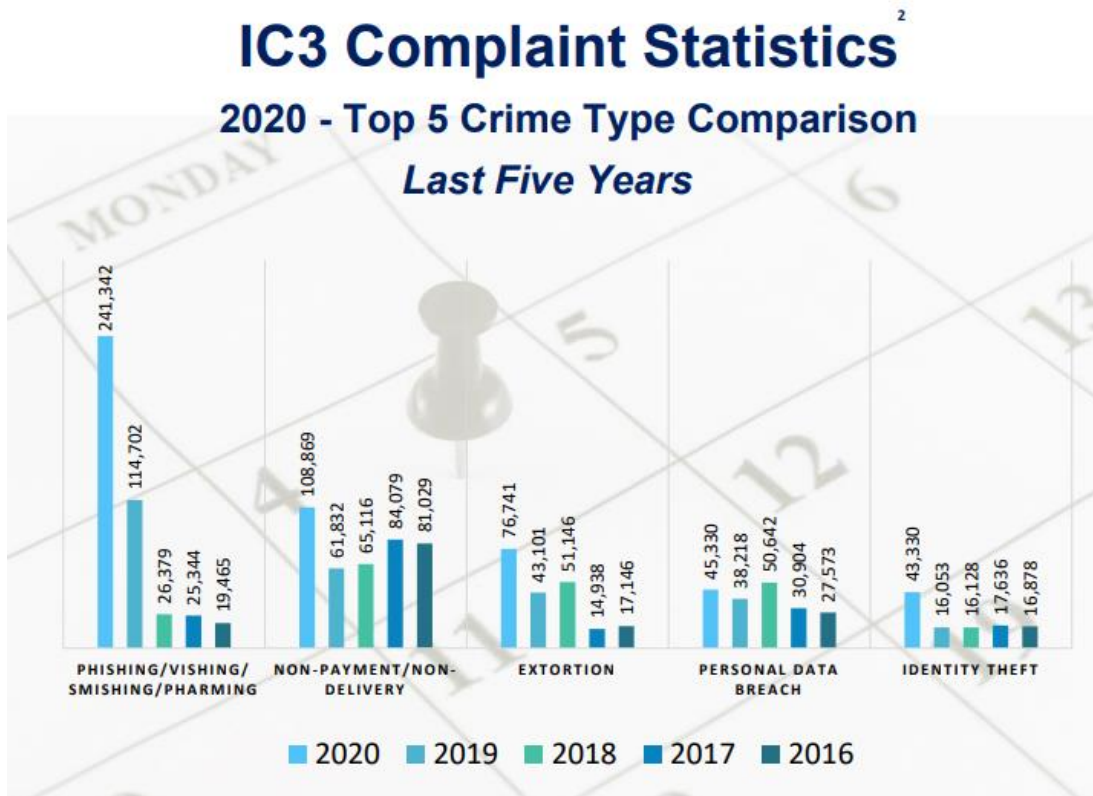
Phishing attempts have continued to grow as the internet and digital interactions have become more and more important. Attackers have gotten better at what they do by learning to use new technologies and coming up with new ways to take advantage of people. As smartphones and

other mobile devices have become more popular, the attack area has grown even more. Phishing attacks now target users through SMS texts, social media, and messaging apps.

### 3. The Latest Statistics of Phishing attacks

#### 3.1 Phishing Attack Trends

In the world of cybersecurity, phishing scams continue to be a big problem that affects people, companies, and organisations all over the world. Since the COVID-19 pandemic, people are using technology more and more. This has given hackers more chances to take advantage of weaknesses in online systems (FBI, 2021) Shown in Figure 1. In this review of the literature, recent articles and websites are used to look at the newest data and trends in phishing attacks.



**FIGURE 1 LAST 5 YEARS FROM 2016 -2020**

According to the findings of the 2021 Data Breach Investigations Report (DBIR) published by Verizon, phishing was responsible for 36 percent of all data breaches. This places it among the most significant threat activities that contributed to data breaches (Verizon, 2021). This data emphasises the substantial danger that phishing attacks represent to organisations and stresses the need for organisations to have effective measures to counteract these threats.

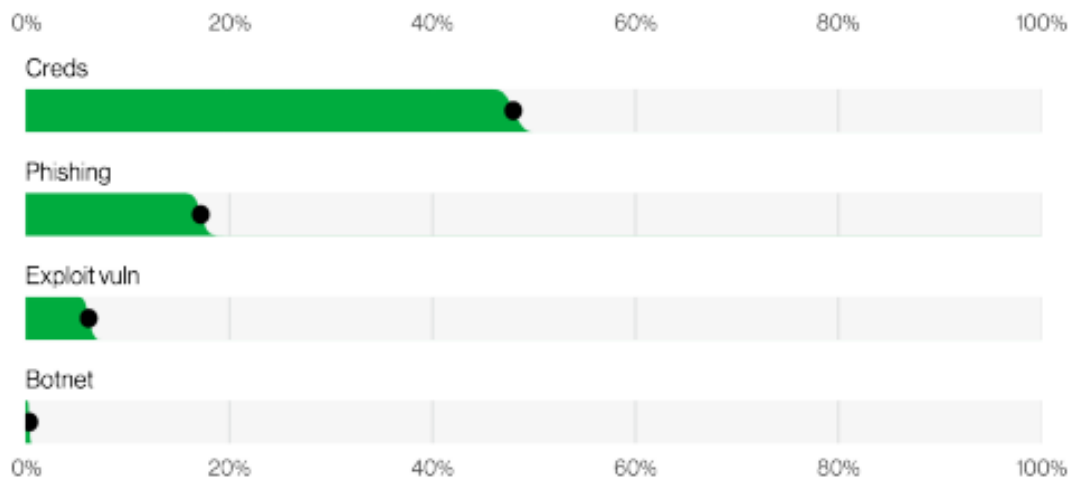


FIGURE 2 STATICS FIGURES

### 3.2 Impact of Phishing Attacks

According to the findings of a survey conducted by Tessian in 2020, 74% of organisations were victims of a successful phishing attack, and 43% of workers admitted to having clicked on a phishing email while they were at work (Tessian, 2021). These data illustrate the widespread nature of phishing assaults and the ease with which cybercriminals may penetrate organisations via the workers of such organisations. [Cybercriminals] can easily get access to sensitive information by impersonating legitimate employees.

According to the results of Proofpoint's State of the Phish study for 2021, 57% of companies lost data, had private information compromised, or lost money because of a successful phishing attack in 2020. The study also found that a successful phishing attack costs an average of \$3.92 million (Proofpoint, 2021). This shows that hacking attacks could cost businesses a lot of money and hurt their names and customers' trust.

## 4. Real World Phishing Attacks

Over 230,000 people lost power as a consequence of a phishing assault conducted against Ukraine's power infrastructure in December 2015. The attack has had a major impact on the security of vital infrastructure throughout the globe and is one of the first recorded cyberattacks to result in a power outage. The installation of a traffic light system is one feasible way to stop or reduce the effect of such assaults.

In academic research as well as the media, the attack on Ukraine's electrical infrastructure has received much study and discussion. According to Zetter (2016), the attack was started by a phishing email that was addressed to workers at the power business in Ukraine. The email included a malicious attachment that, when viewed, infected the worker's machine with malware. After gaining access to the network and systems of the power company, the attackers were able to remotely manage crucial systems and turn off electricity to a number of substations.

The fake invoice scheme is a type of phishing attack that involves sending false invoices to businesses with the goal of deceiving them into paying for services or goods that aren't really there. Google and Facebook, two of the biggest internet businesses in the world, were conned between 2013 and 2015 and jointly lost more than \$120 million as a consequence (Fazzini, 2019).

The attackers in this case impersonated legitimate suppliers of Google and Facebook, and sent fake invoices to their accounting departments requesting payment for services or products. The invoices appeared to be genuine and were designed to look like they were from reputable suppliers, which made it difficult for the accounting staff to detect the fraud.

The fraud was linked to Evaldas Rimasauskas, a Lithuanian hacker who was detained and deported to the US in 2017 (NPR, 2019). The incident demonstrated the need for businesses to have strong cybersecurity measures in place to guard against similar attacks.

## 5. Phishing Techniques

Phishing attackers usually use two main methods: using psychological tricks to get people to give out personal information or using technology. But phishers usually use tricks that play on the emotions of people instead of technology methods. Figure 3 shows the different kinds of phishing and the methods used by phishers to attack. In the parts and subsections that follow, you'll learn more about each type and method.

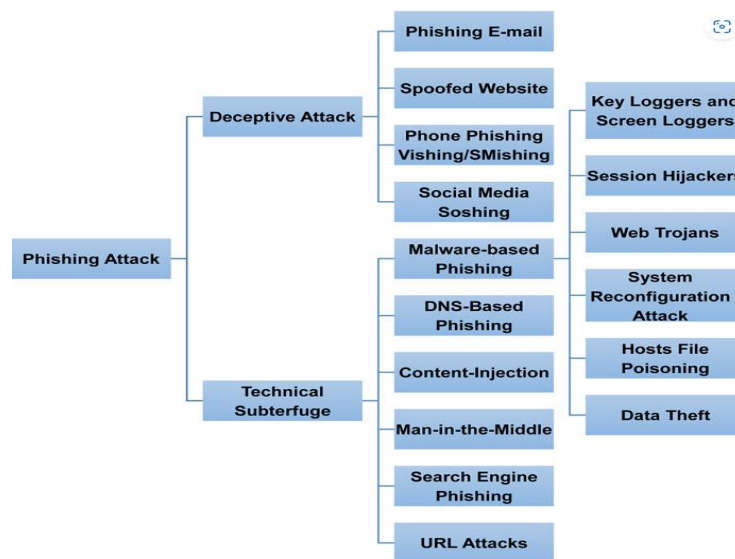


FIGURE 3 TYPE OF PHISHING ATTACKS

### 5.1 Deceptive Phishing

Deceptive phishing is a common type of phishing attack in which hackers pose as trusted entities to trick people into giving them private information like login keys or credit card data. Attackers usually use email as their main way to talk to each other. They write believable emails that look like they came from the entity they are pretending to be. These emails often use hurry or fear to get the person who gets them to act right away. Cybercriminals usually send the target to a fake website that looks like the real organization's site. There, they steal their private information.

### 5.1.1 Phishing E-mail

Phishing emails are still a big hacking risk, and hackers are always changing their tricks to trick people who don't know what's going on. In this part, we talk about recent pieces that use the Harvard referencing style to show the latest trends in fake emails.

Phishing emails about COVID-19: Since the start of the pandemic, attackers have taken advantage of people's fear and confusion by sending COVID-19-related fake emails. These emails may pretend to be from health organisations and give false information about the virus or say they have access to medicines and cures.

Business Email Compromise (BEC) attacks: Cybercriminals are increasingly using scam emails to hack into business email accounts and ask for fake money transfers. According to the FBI's 2020 Internet Crime Report, BEC scams cost an estimated \$1.8 billion, making them one of the most expensive internet crimes (FBI, 2021).

Increase in phishing for people who work from home: As the number of people who work from home has grown, so has the number of fake emails sent to those people. Cybercriminals take advantage of the fact that people don't talk to each other face-to-face and use "social engineering" to trick workers into giving up private information or letting them into company networks without permission.

### 5.1.2 Spoofed Website

In the world of safety, frauds are a major worry. These fake websites are made to look like real ones as much as possible. The main goal is to trick users into thinking they are using a real site. Cybercriminals make fake websites for a variety of reasons, such as to steal private information, spread malware, or carry out phishing attacks.

Cybercriminals make fake websites look real by using the same URLs, brands, and styles. Homograph attacks use letters from different writing systems to make URLs that look like they are real.

The fact that cybercriminals use HTTPS makes it hard to stop fake websites. When scam sites use HTTPS, it makes it harder to find them. HTTPS gives people a false sense of protection and makes it hard to tell if a site is real or not.



To avoid fake websites, users must be careful, check the URLs of websites, and use web filters and anti-phishing browser tools. It's also important to teach people about fake websites and tell them to be careful when giving out personal information online.

### 5.1.3 Phone Phishing (Smishing)

Smishing, also called SMS phishing, is a type of social engineering attack that uses text messages to trick people into giving away private information, clicking on malicious links, or getting malware. Combining "SMS" (Short Message Service) and "phishing" makes the word "smishing" (Ponemon Institute, 2021). Smishing attacks have become popular among hackers. This is because mobile devices and text services are becoming more common.

Smishing attacks often rely on making the target feel rushed or curious to get them to do something. For example, an attacker may send a text message to a target saying that their bank account has been hacked and telling them to click on a link to a fake website where they will be asked to enter their account information. Or, the message could look like it came from a trusted source, like a friend or family member, and contain a link to download a harmless-looking app that is actually malware meant to access the victim's personal information (Norton, 2022).

People and businesses should take a strategic approach to security, including education and knowledge, to avoid smishing attacks. Users should be careful when reacting to unexpected or unwanted text messages and check the sender's name before doing anything (Kaspersky, 2021). Also, users shouldn't click on links in text messages. Instead, they should go directly to the organization's official website by typing the URL into their browser or using a safe bookmark (Proofpoint, 2021).

Also, companies should spend money on security measures like mobile device management (MDM) and mobile threat defence (MTD) systems to protect the devices and private data of their employees (Gartner, 2021). These solutions can help find and stop smishing attacks and give insight and control over the security of mobile devices used in the organisation (Norton, 2022).

### 5.1.4 Spear phishing

Spear phishing targets individuals or corporations. Spear phishing emails employ personal information to seem to be from a reputable source, such a co-worker or a well-known organisation (Hadnagy, 2018). Because people respond to significant and trustworthy messages, this increases success odds.

Attackers gather personal data from social media, professional networking sites, and corporate websites (Bursztein et al., 2014). The target's name, job title, co-workers, and interests may be used to generate more engaging letters. Spear-phishing emails may reference a recent workplace event or utilise industry-specific language.

Hadnagy (2018): Spear phishing uses current events or urgency to encourage the victim to act. This might involve clicking on a malicious link, opening an infected file, or providing login credentials or financial information. Spear phishing can cause financial loss, image harm, and data theft.

According to Bursztein et al. (2014), spear phishing emails are up to 45% more effective than conventional phishing emails. This highlights the need of spreading awareness of spear phishing and using technology defences like email filtering and multi-factor authentication.

To stop spear phishing, companies should give their employees security training that teaches them how to spot scam emails and stay safe online. Spear phishing attacks can also be less likely if you use security measures like email authentication methods, safe email servers, and endpoint protection (Trendmicro.com, 2023).

This diagram shows the steps of a spear phishing attack. In Figure 1. This shows the process



**FIGURE 4 SPEAR PHISHING ATTACK**

of a Spear phishing attack.

1. **Target Selection:** The attacker chooses a specific person or organisation to attack, usually someone who has access to important information or resources.
2. **Information Gathering:** The attacker does study on the target, gathering personal and professional information from places like social media accounts, professional networking sites, and company websites.
3. **Crafting a Persuasive Message:** With the information gathered, the attacker makes a customised email that looks like it came from a trusted source. This personalised statement makes it more likely that the person receiving the email will do something with it.
4. **Call to Action:** Most spear phishing emails have a call to action that tells the target to do something right away. This could be done by clicking on a bad link, downloading an infected file, or giving out private information like login credentials or banking information.
5. **Exploiting the Target's Response:** If the target falls for the spear phishing email and does what it says, the attacker can get into the target's accounts, private information, or resources. This can cause data leaks, money losses, and other problems for both the person and the organisation.

#### 5.1.5 Social Media Attack (Soshing, Social Media Phishing)

Social media attacks, especially social media hacking or "soshing," use social networking sites to trick users into giving up private information or clicking on harmful links. Soshing is when hackers pretend to be trusted entities, like friends, family members, or well-known organisations, to gain the trust of their targets. (Chu et al., 2010) says that these attackers use direct messaging, sharing harmful links on public profiles, and making fake accounts or pages to entice victims. Recent study has shown that social media hacking is particularly successful because people tend to believe the material they get from their links. To stop social media scams, users need to be careful about the material they deal with and check the validity of messages and accounts before responding to them (Choo & Smith, 2008). Choo and Smith (2008) say that the risk of being a target of a soshing attack can be reduced by making sure that social media sites have the right security settings and by spreading information about the possible risks.

## 5.2 Technical Subterfuge

When talking about cybersecurity or information security, the word "technical subterfuge" refers to the technique of using different kinds of technology, tools, or strategies to fool, confuse, or trick a target. In these kinds of situations, cybercriminals will use a variety of methods, such as making fake websites, changing URLs, taking advantage of software flaws, and using malware, to gain unauthorised access to systems, steal sensitive data, or compromise user accounts. The main goal of technological deception is to get someone to do something bad without their knowledge or permission. This can be done by getting around security measures, taking advantage of flaws, and other things.

### 5.2.1 Malware-Based Phishing

Malware-based hacking is a type of cyberattack that uses harmful software to steal private information from users or gain unauthorised access to their systems. Hadnagy and Fincher (2020) say that these attacks often start with fake emails, texts, or social media posts that trick users into getting malware by making it look like a real file or link. Keyloggers, which record a user's keystrokes and send the information to the attacker, and ransomware, which locks a user's files and asks for a pay to recover them, are two common types. Some fake emails may have links to harmful websites that take advantage of weaknesses in a user's browser or software to put malware on their system (Barbosa & Neto, 2021). To guard against malware-based phishing attacks, it's important to keep security software up-to-date, keep operating systems and apps fixed, and teach users about the risks of getting files or clicking on links from unknown sources (Hadnagy & Fincher, 2020).

### 5.2.2 Whaling

Whaling, a targeted kind of phishing, targets celebrities, politicians, and senior executives. The attacks are increasingly complex and tailored to the target, increasing their success rate. Social engineering and major background research help attackers win.

Whaling attacks target sensitive data or financial assets, unlike phishing attacks. An attacker may mimic a high-ranking executive and request an urgent financial transfer to a specific account (Proofpoint, 2022). The attacker raises the chance of an effective attack by taking advantage of urgency and the target's organisational authority.

Organisations should use more than one strategy to stop whale attacks. This means putting in place strong security measures, spending money on teaching employees, and promoting a security-aware society (Fortinet, 2022). Employees can be less likely to be attacked successfully if they are kept up-to-date on the latest risks, told to check the legitimacy of any strange requests, and encouraged to be sceptical of unwanted communications.

Radware (2022) says that another good way to reduce the risk of hacking attacks is to use multi-factor identification. This adds an extra layer of security by requiring users to provide multiple pieces of information, like a password and a unique code sent to their mobile device, before they can access private systems or data. Even if an attacker is able to trick a high-profile target, this method makes it harder for them to get unauthorised entry.

For whaling attacks to have less of an effect, it is also important to keep a close eye on money activities. Implementing strict procedures for financial transactions, especially those involving large amounts of money or private information, can help stop unauthorised transfers and alert the organisation to any strange activity. Also, organisations can use advanced threat tracking tools that can find and stop possible whaling attacks before they reach their intended target (Radware, 2021).

### 5.2.3 DNS-Based phishing

DNS-based hacking, also known as "pharming," is a type of cyberattack that uses the Domain Name System (DNS) to trick users into inputting sensitive information, such as logon credentials or credit card information, on fake websites. This form of cybercrime is also referred to as "pharming." Attackers either exploit DNS infrastructure vulnerabilities or alter the configuration of the local DNS server. They will occasionally contaminate a server's DNS cache, causing it to deliver the incorrect IP address for a legitimate domain. Users are deceived into divulging their confidential information by being redirected to imposter websites that appear identical to the genuine sites. Individuals and organisations can better defend themselves against DNS-based phishing attacks by keeping their software and operating systems up-to-date, employing strong and unique passwords, enabling two-factor authentication, implementing DNS Security Extensions (DNSSEC), establishing firewalls and intrusion detection systems, and educating users about phishing risks and how to recognise malicious websites.

The fact that DNS-based hacking, also called "pharming," is so common shows how important it is to stop this kind of cyberattack in today's digital world. Researchers and cybersecurity experts are still looking for ways to find these attacks and stop them. They are a major threat to both people and organisations. Since these attacks are getting smarter, more and more people are giving their private information to bad people without knowing it (ACM Conferences, 2023). This can lead to financial loss, identity theft, and other problems. Since phishing methods are always changing, the cybersecurity community needs to come up with new tools, strategies, and training programmes to stop DNS-based attacks. Combining technology solutions like DNSSEC (Rose et al., 2005) with user knowledge and teaching programmes can help reduce the risk and effects of these kinds of threats, making the Internet a better place for everyone.

### 5.2.3 Content Injection

A cybersecurity risk known as content injection occurs when hackers change or introduce harmful material into legitimate websites or online applications. This kind of attack often takes advantage of vulnerabilities such as SQL injection, cross-site scripting (XSS), or server-side code injection. By manipulating text, photos, links, or scripts, the purpose of content injection is to trick people, steal sensitive information, or spread malware. These goals may be accomplished. Users who visit hacked websites run the risk of coming across deceptive information, harmful links that take them to phishing websites, or being urged to download malicious software. The adoption of best practises in web application development, the use of robust passwords, the use of up-to-date software and plugins, and the implementation of intrusion detection and prevention systems are all critical actions that may be taken to reduce the effects of content injection attacks.

Due to the enormous risk they pose to both individuals and organisations, content injection attacks have emerged as a significant issue in the field of cybersecurity. According to the findings of a recent study, these assaults may result in a wide range of outcomes, from financial losses to reputational damage. In recent years, the sophistication of content injection attacks has increased, with attackers targeting a broader range of vulnerabilities and employing more sophisticated techniques. As a result, businesses must make significant investments in robust security measures and stay abreast of the latest developments in content injection attacks. Hassan et al. (2020) recommend a combination of safe coding practises, input validation, frequent security audits, and real-time monitoring to identify and prevent

attacks of this type. According to research conducted by Al-Dmour et al. in 2021, increasing workers' knowledge of cybersecurity issues and training them will further reduce the likelihood of content injection attacks and the potential harm they can cause to organisations.

#### 5.2.4 Man-in-the-Middle

A man-in-the-middle (MITM) attack is a privacy risk in which an attacker listens in on a conversation between two parties, like a client and a server, without them knowing. The bad guy can listen in on conversations, change data being sent, and add harmful content. MITM attacks use ARP spoofing, DNS spoofing, SSL/TLS hacking, and listening in on Wi-Fi connections. Users and companies should use security standards like HTTPS, validating digital certificates, implementing public key infrastructure (PKI), using virtual private networks (VPNs), and updating software and hardware regularly to protect themselves from these threats. Users should also be careful when linking to public Wi-Fi networks and shouldn't send private information over links that aren't safe.

Attacks called "man-in-the-middle" (MITM) continue to be a problem for internet security, and they also bring up new issues. (Yadav et al., 2021) New study shows that MITM attacks are getting harder to spot and stop because they are getting more complicated. Kumar et al.'s study from 2020 shows that criminals often take advantage of flaws in security measures and the actions of users to get private information and control contact between different parties.

Due to this, security experts say that you should use multiple layers of security to make MITM attacks less likely. These methods include educating users about possible risks and best practises, as well as using strong encryption protocols like HTTPS and Transport Layer Security (TLS), certificate pinning, and ensuring safe contact over virtual private networks (VPNs). Dinakaran et al.'s study from 2020 says that companies should use real-time breach detection systems and constant tracking to find potential dangers as soon as possible and take action.

### 5.2.5 Search Engine Phishing

Using search engines for phishing is a type of cyberattack that entails the creation of fake websites or web pages, the manipulation of search engine algorithms to rank the attackers' websites higher in search results, and the use of deception to trick individuals into submitting personal information or downloading malware. Due to the similarities between hazardous and legitimate websites, it may be difficult for users to distinguish between the two. Users can protect themselves from search engine phishing by carefully inspecting URLs and domain names, ensuring that websites use HTTPS, sticking to reputable search engines, regularly updating browsers, operating systems, and antivirus software, and refraining from disclosing sensitive information on websites that appear unfamiliar or suspicious. By adhering to these precautions, search engine users can reduce the likelihood of falling victim to fraudulent schemes.

Search engine scamming is still a major security risk, with attackers using sophisticated methods to trick users. A study by Le et al. (2014) shows how search engine phishing takes advantage of people's trust in search engines and their habit to think that high-ranking search results are real. The writers stress that "the higher the ranking of a phishing website, the more likely it is that users will visit it" (Le et al., 2014, p. 123). In a similar way, Sheng et al. (2010) found that "users are more likely to fall for phishing attacks when the attack seems to come from a trusted source, like a high-ranking search result."

(Canali et al., 2013) To stop search engine hacking, experts advise users to be careful when using search results and to check the legitimacy of websites before giving out private information. Zhang et al. (2019) say that the risk of phishing attacks can be greatly reduced by teaching users about the dangers of search engine phishing and giving them tools and strategies to spot harmful websites. Also, it is important for search engine providers to keep improving their algorithms and security measures (Wang et al., 2020) to find and block fake websites from showing up in search results. Moore et al. (2009) also say that search engine providers, web hosting companies, and domain owners need to work together to solve the problem of search engine hacking.



### 5.2.6 URL Attacks

URL attacks are a group of methods that use harmful URLs to take advantage of weaknesses or trick users. These attacks include misleading URLs, URL shortening, encryption, drive-by downloads, and watering hole attacks. In these attacks, URLs are often made to look real or like well-known websites. This makes it hard for users to tell the difference between safe and dangerous links. To avoid these kinds of attacks, users should keep their security software up-to-date, use private browsing, be careful when clicking on links they don't know, and stay informed about the risks of URL attacks. Organisations should also teach their users how to spot and avoid links that are harmful.

As URL threats get more complicated, they pose a lot of problems for both security experts and users. Chiew et al. (2018) found that the success of URL attacks is due to the attackers' ability to take advantage of cognitive errors and trick people into thinking that harmful URLs are real. The authors write (Chiew et al., 2018, p. 324) that "users have a limited ability to tell the difference between malicious and safe URLs, which makes URL attacks much more effective." This shows how important it is to teach users how to protect themselves against URL threats.

Lauinger et al. (2017) also found that even well-known web apps and content management systems (CMS) are often open to URL attacks. The researchers found a number of vulnerabilities in popular CMS platforms that attackers could use to launch URL-based attacks. They stressed that "while these platforms are widely used and trusted, they are not immune to the threat of URL-based attacks" (Lauinger et al., 2017, p. 452).

Organisations should not only focus on educating users about URL threats, but also put in place strong security steps to protect their online assets. Whittaker et al. (2010) say that organisations can find and stop harmful URLs by using a mix of security technologies, like web application firewalls, intrusion detection systems, and real-time tracking. The writers say that "a multi-layered security approach can significantly reduce the likelihood of a successful URL attack" (Whittaker et al., 2010, p. 89).

## 6. Literature Review

### 6.1 Introduction

Since the Internet and digital contact has been so popular, the number of phishing email has grown over the years. Email is still one of the most normal way to make communication, which now has made it vulnerable to threats like spams, scams and malware. Because of this, making email screening systems that work well has become an important area of study to protect users from dangerous material. The study of this literature review will look into the current emails screening methods, how well the work, what problems they face and where future research should been done. The topics will be focused on is content-based filtering, user reputation and domain-based filtering, email authentication and encryption techniques, and then machine learning.. It will also look at the problems and limits of current methods and Gmail's filtering system, which uses TensorFlow, joint filtering, and community signs, among other things. The review will also talk about recent improvements in mixing user reputation, domain-based filtering, and content-based filtering methods to make it easier to find spam and lessen the number of false positives. The importance of educating and making users aware of their rights will also be talked about, as will the study of fun and simulation-based training. This study will help people understand email filtering systems better and guide future research in this area by giving a broad account of the research that has already been done.

Malicious material has grown along with the popularity of the internet and digital contact. Email is one of the most popular ways to talk to people, which makes it a prime target for attacks like scams, malware, and spam. The goal of this literature study is to look at the different ways to screen email to protect users from harmful material. It will look at how well these methods work, what problems they face, and where study in this area is headed.

### 6.2 Content-based Filtering

One of the main ways to find and stop harmful emails is through content-based screening. (Mishra et al., 2020) This method includes looking at the content of emails to find strange things like URLs, files, and text trends. Abusitta et al.'s (2019) research showed that machine learning methods like Naive Bayes, Decision Trees, and Support Vector Machines could be used to identify emails based on their text. (Kumar & Sachdeva, 2020) Another way to find scam emails is to use natural language processing and text mining to look at the content of an email.

Abusitta et al.'s (2019) research showed that machine learning methods like Naive Bayes, Decision Trees, and Support Vector Machines could be used to identify emails based on their text. They found that these systems could find fake emails with a high degree of accuracy. In the same way, Kumar and Sachdeva (2020) looked into how natural language processing and text mining could be used to analyse the content of emails to find fake emails. Their work showed that phishing emails could be found much more often if they extracted data from the text of emails and used machine learning models.

Deep learning has also been looked at as a possible way to make content-based screening work better. Raff et al. (2020) came up with a deep learning model that uses convolutional neural networks (CNN) to pull features from email text. This model was very good at finding harmful emails. This shows that deep learning methods could be used to make content-based screening work even better.

### 6.3 Sender Reputation

Checking the sender's image is another way to clear out spam emails. author reputation systems (Ramachandran & Feamster, 2019) figure out how trustworthy an email author is based on how they have sent emails in the past and other factors. These tools can help you find emails from known bad sources and stop them. (Liu et al., 2021) Several studies have shown that mixing source reputation systems with content-based filters can make it easier to spot bogus emails.

When you combine user reputation and content-based blocking, you can make your defence against harmful emails stronger and more complete. source reputation systems look at how trustworthy the source is, while content-based screening looks at the email's text to find shady parts. When these two methods are used together, it's easier to find spam, scams, and other bad emails.

Zhou et al. (2020) showed that source reputation and machine learning-based content screening work well together. Their suggested framework is based on a multi-step process that starts with figuring out how trustworthy the writer is. If the sender is thought to be reliable, the email is sent to the intended receiver. But if the author has a bad image, the email is filtered based on its content using machine learning techniques. This method makes it easy to find harmful emails while reducing the number of false positives because it focuses on checking emails from less reliable sources.

Yang et al. (2021) also looked at what would happen if source reputation and content-based screening were used together. Their adaptable email filtering system uses a reputation level that changes based on how well the content-based filtering component works at finding spam. When the content-based filtering system works well, the reputation barrier goes up. This lets more emails from senders with a lower reputation get through without being looked at more closely. On the other hand, if the performance of content-based filtering goes down, the reputation barrier goes down, causing more emails to be subjected to content analysis. This method helps keep a balance between the efficiency of identification and the number of false positives, even as the email danger situation changes.

In conclusion, email filtering is better at finding harmful emails when it uses both source reputation systems and content-based screening methods. When you use these two ways together, you can learn more about both the sender and the text of an email. This makes it easier to protect yourself from trash, scams, and other threats that come through email. Future research should keep looking for ways to improve how these methods work together and look into the possible benefits of adding more data sources to the screening process, such as network traffic analysis and user behaviour trends.

#### 6.4 Email Authentication and Encryption

Mittal and Kaur (2020) say that email authentication and encryption methods like DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) have been created to make sure that email messages are real and genuine. These methods help stop faking and fake attempts, which makes it less likely that you will get malware. Gupta and Arora's research from 2021 showed that broad use of email authentication and encryption protocols can make email security much better.

#### 6.5 Challenges and Limitations

Due to the problems and limits of current email screening methods, future study could focus on improving machine learning and artificial intelligence techniques and finding new ways to educate and inform users.

(Hadiosmanovi et al., 2022) say that advanced machine learning and artificial intelligence methods can be used to better understand and spot the changing ways that hackers work. For example, experts could look into how unstructured and semi-supervised learning methods can

be used to find new risks and trends of bad behaviour. Also, deep learning models like recurrent neural networks (RNNs) and transformer-based designs could be used to improve the text and structure analysis of emails.

Integrating various data sources can make it much easier for email screening tools to find spam. Researchers can make filtering models that are more complete and aware of context by mixing information from network data, user behaviour, and external danger intelligence. Also, using advanced analytics and data fusion methods can help connect events and find trends that may be signs of bad behaviour. This can help risks be found more quickly and accurately.

Exploring new ways to educate and inform users is important if users are to be able to spot scam emails and other harmful material and know what to do about it. (Tsikrika et al., 2021) For example, gamification can make cybersecurity training more fun and participatory, which encourages users to take part in learning tasks. By adding game-like features like awards, leader boards, and tasks, users can learn more about cybersecurity best practises and become better at spotting possible threats.

Simulation-based training can give users a safe place to practise recognising scam emails and other harmful material and how to respond to them. These interactive learning experiences can help users learn important skills by putting them in real-world situations and giving them the chance to make choices and see the results of those choices in a safe environment.

Users will need less training and knowledge programmes if email platforms are made easier to use and more safe. Researchers can make email platforms that make it easier for users to spot possible threats and move safely through their email world by using visual cues, context-aware advice, and user-centred design principles. These platforms could have features like automatic screening of suspicious emails, color-coding to point out possible risks, and real-time security signs that tell you how trustworthy an email source has become.

In conclusion, exploring advanced machine learning and artificial intelligence techniques, integrating multiple data sources, and coming up with new ways to educate and inform users can make email filtering systems much better at fighting cyber threats that are always changing.

## 6.6 Gmail Filtering System

Spam has gotten worse because so many people use email. The enormous challenge facing people who use email and companies who provide email services. Gmail is one of the most

popular online services, and it employs a variety of security measures to ensure the privacy of its users. This literature study looks at the current research on spam filters and how Gmail handles it. It talks about how well they work, what problems they face, and where future research could go.

#### 6.6.1 Machine Learning-Based filtering – Gmail

Machine learning techniques are used by Gmail to analyse and remove spam emails. These algorithms are taught to look for spam-like trends and characteristics in the text, labels, and information of emails (Hunt, 2020). Google's Gmail uses the TensorFlow framework, which is one of the most important machine learning methods (Google, 2019). This framework helps Gmail find trash better.

Recent study has shown that machine learning methods like Naive Bayes, Decision Trees, and Support Vector Machines can be used to identify emails based on their text (Kumar & Sharma, 2021). Deep learning methods like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have also shown promise for making content-based spam screening more effective (Alam et al., 2021).

#### 6.6.2 Sender Reputation and Domain-based Filtering - Gmail

Gmail uses user reputation and domain-based screening to figure out which email senders you can trust and which ones might be sending spam. These methods include looking at how the sender has sent emails in the past, their IP addresses, and whether or not they follow email security standards like SPF, DKIM, and DMARC (Google, 2020). Gmail can stop or put emails from known spam sources in a separate folder based on how trustworthy the writer and site are. (Zhang et al., 2021) Recent studies have shown that mixing user reputation, domain-based filtering, and content-based filtering can make it easier to find spam and reduce the number of false positives.

### 6.6.3 Community Signals and Collaborative Filtering - Gmail

Gmail's spam detection capabilities are enhanced through the use of collaborative filtering and community signals. By aggregating user feedback, such as designating emails as spam or reporting fraud attempts, Gmail can refine its filtering algorithms to detect and block spam emails more effectively (Google, 2019). Collaborative filtering permits Gmail to utilise the collective intelligence of its user base to enhance its spam detection capabilities. Dey et al. (2020) have demonstrated that collaborative filtering techniques can effectively identify spam emails based on user feedback and interactions.

### 6.6.4 Challenges and Limitations - Gmail

Even though Gmail's junk screening methods work well, there are still some problems and limits. One problem is that spam is always changing, and marketing methods are always getting better. Attackers are always coming up with new ways to get around email screening systems, which makes it hard for these systems to keep working (Bursztein et al., 2022). To deal with this, Gmail uses algorithms that keep learning from new data to adapt to the new ways hackers are using (Hunt, 2020).

Second, false positives and false negatives continue to be a problem because genuine emails can be incorrectly marked as spam, and vice versa (Abdelhamid et al., 2021). This problem can make it hard to send and receive emails and cause important information to be lost. Gmail solves this problem by constantly improving its filtering algorithms and taking user comments into account to cut down on false positives and false negatives (Google, 2019). In a recent study by Zhang et al. (2022), the authors found that mixing user reputation, domain-based filtering methods, and content-based filtering could lead to better spam detection rates and lower false positive rates.

In addition, Gmail has added new tools that make it better at blocking spam. For example, Gmail now uses machine learning algorithms to find emails with links or files that could be harmful and tells users about them (Google, 2021). This extra layer of protection helps keep users safe from threats like phishing and malware.

## 7 Methodology

### 7.1 Introduction

People and companies alike are always under danger from phishing assaults. Hackers constantly devise novel methods of taking advantage of vulnerabilities and unsuspecting users as the number of people who rely on technology and digital communication grows. In this article, we'll discuss the experiences of non-IT users who have had to deal with phishing emails, shedding light on their level of awareness, confidence, and ability to recognise and deal with bogus messages. We'll discuss the structure of phishing emails and how tools like PyPhisher can help businesses replicate attacks to identify and address vulnerabilities. Our goal is to assist institutions in developing security measures, pedagogical plans, and training initiatives that are adapted to the specific challenges faced by non-IT users. The objective is to provide individuals and institutions with the knowledge and resources they need to combat the evolving threat of phishing attempts and improve the online environment for everyone.

### 7.2 Survey

The survey will find out information about the no-IT users thoughts and their experiences with phishing emails. The main goal is to see how often phishing emails are sent to the group and how well they can recognise and react to them. By focusing on people who don't have an IT background, the survey will find out the weaknesses and knowledge of people who may have a lot of experience or training in detecting phishing emails.

#### 7.2.1 Questions

The poll had nine multiple-choice questions, each of which was meant to give information about a different part of phishing.

- How often you get phishing emails: The goal of this question was to find out how big of a problem phishing is for non-IT people by finding out how often they get phishing emails.

These questions are meant to find out how many non-IT users have been caught by phishing emails, from the past and how the result were.

- Confidence in being able to spot phishing emails: This question was meant to find out how confident non-IT users are in their ability to spot phishing emails and see if they need more education and training.



- People's ideas about what kinds of emails are most likely to be scam attempts: This question was meant to find common misunderstandings and make people more aware of the different ways that hackers use in fake attacks.
- Getting the IT department or security team to know about scam emails: This question was meant to find out if people who don't work in IT know how to report fake emails and if they do so when they see them.
- Favourite ways for companies to teach their workers more about scam emails: This question looked for the best ways for companies to make their employees more aware of and knowledgeable about hacking attacks.
- Typical reactions to emails that might be phishing: This question was meant to test how well current training and teaching programmes work by looking at how non-IT users usually reply to emails they think might be scams.
- Most difficult things people think they have to do to stop scam attacks: This question was meant to find out what the biggest problems are for people who don't work in IT when it comes to stopping hacking attacks. This can help organisations make their security plans more effective.
- Dealing with the effects of clicking on a scam email, such as having your name stolen or losing money: This question was meant to find out how phishing attacks affect non-IT people and how well they can get over them.

The main of the survey is to get a full understanding of how non-IT users are targeted and to find out where education, training and knowledge can be improved. The survey results should give organisations useful information from the survey that can help them come up with better ideas to protect their work environment. By learning more about non-IT users go through and what kind of problems the face, organisations can make safety programmes that are especially made for the needs and weakness of this group.

In the end, the results of the survey can be used to make policies and training program for organisations and aim to reduce the risk of phishing attacks. By using the information from the survey, companies can make a better approach on where or how to allocate resources, create training plans, set up security features and measures to protect the non-IT users.

## 7.2 Phishing email Anatomy

The code is a complete Python script that aims to improve the user's email security by finding and judging the safety of URLs in the user's most recent open Gmail message. To do this, the script uses two well-known third-party services: Virus Total and URLScan.io. Both of these services have APIs that can be used to check the safety of URLs.

At first, the script goes through a login process to access the Gmail API. This includes updating or making new access keys and connecting to the user's Gmail account. Once the link is made, the script gets the most recent open email, pulls out important information like the topic, author, and body, and looks for URLs in the email body.

There are two steps to the safety analysis: First, the script checks the base URL by sending a request to the Virus Total API. The API checks the URL against various antivirus databases and gives the number of good detections. At the same time, the base URL is sent to URLScan.io, a service that checks the URL in a lab and gives a general safety score based on things like scam attempts, harmful content, and strange behaviour.

If the special "traffic light" system built into the script says that the base URL is safe (green), the script checks to see if there are any links connected to the base URL. By following the redirection, the script gets the target URL, if there is one, and continues the safety analysis process for the target URL, which includes checking with the VirusTotal API and sending it to URLScan.io for screening.

The "traffic light" method is the most important part of how the script makes decisions. It uses the data from both the VirusTotal API and the URLScan.io API to figure out how safe each URL is as a whole. Green means that the URL is safe, yellow means that there might be risks, and red means that the URL is dangerous and should be avoided. This method shows the user how safe each URL in the most recent open email is.

In short, this Python tool is a useful and efficient way to check the URLs in the most recent open email and make them safer. By using the power of the Virus Total and URLScan.io APIs, it gives users a clear, easy-to-understand safety level (green, yellow, or red) for each URL. This helps users avoid clicking on possibly dangerous links and gives them a safer email experience.

### 7.3 Pyphisher

```

[?] Enter shadow url (for social media preview)[press enter to skip] : 
[?] Enter redirection url[press enter to skip] : 

```

### FIGURE 5 PYPHISHER

Figure 5 shown above is PyPhisher is a Python-based tool that helps security experts and penetration testers set up and run hacking operations. The main goal of this tool is to try look like a social media page and person is to hacking attacks. This tool lets you figure out where they are weak and improve the security. Pyphisher simulates real-life phishing attacks so the users can learn how these attacks are done and come up with ways to reduce them.

PyPhisher comes with a simple, easy-to-use command-line interface that makes it easy for even people with little technical knowledge to set up and run hacking operations. To send scam emails, the tool usually needs a draught email, a list of email names to target, and a Simple Mail Transfer Protocol (SMTP) server that has been set up. Users can also change the email's topic, source address, and other details to make it look more like a real email.

PyPhisher's ability to use multiple email themes is one of its most important features. This lets users practise different types of phishing attacks, such as password harvesting, software distribution, or social engineering. The tool also lets you add harmful files or links to the email body, which is another way to simulate real-world phishing attacks.

Like any other security testing tool, PyPhisher should be used in a legal and responsible way. Before running a hacking operation, users must make sure they have permission and authorization from the organisation or person they are trying. Using PyPhisher for bad things is against the law and could get you in trouble with the law.

## 8 Results

This report shows the result of a poll that asked people about their experiences with phishing emails, how well then can spot and react to them, and how they thought it can be stopped. By pretending to be a trustworthy organisation, phishing emails try to get all information like passwords or bank information. As phishing attempts grow its very important to know and be aware or ready the public is to deal with these dangers.

The survey asks about related phishing emails, such as how often people get them, how confident you are with them, the types of email that are most likely to be phishing attempts and how hard it is to stop them.

The goal of the analysing the survey data to find relative pattern and trends in the experiences and opinions on the non-IT users. This survey will give the organisation and individuals who want to learn more about phishing attacks and be prepared to deal with with fact growing cyber threat information.

### 8.1.1 Survey Results

- **Q1 - How often do you receive phishing emails?**



**FIGURE 6 Q1- HOW OFTEN DO YOU RECEIVE PHISHING EMAILS?**

The bar chart shows that most of the people who answered the survey get fake emails between one and three times a month (19), then more than once a week (20), and less than once a month (11). Only 3 of the people who answered said they got fake emails once a week or more.

- **Q2 - Have you ever fallen for a phishing email?**



**FIGURE 7 Q2 - HAVE YOU EVER FALLEN FOR A PHISHING EMAIL?**

The pie chart shows that most of the respondents (33 of them) have almost been fooled by a phishing email, while a smaller number (11 of them) have been fooled by a phishing email but didn't get hurt. Some people (four) lost money or had their name stolen because they fell for a phishing email, and only five people have never gotten or fallen for a phishing email.

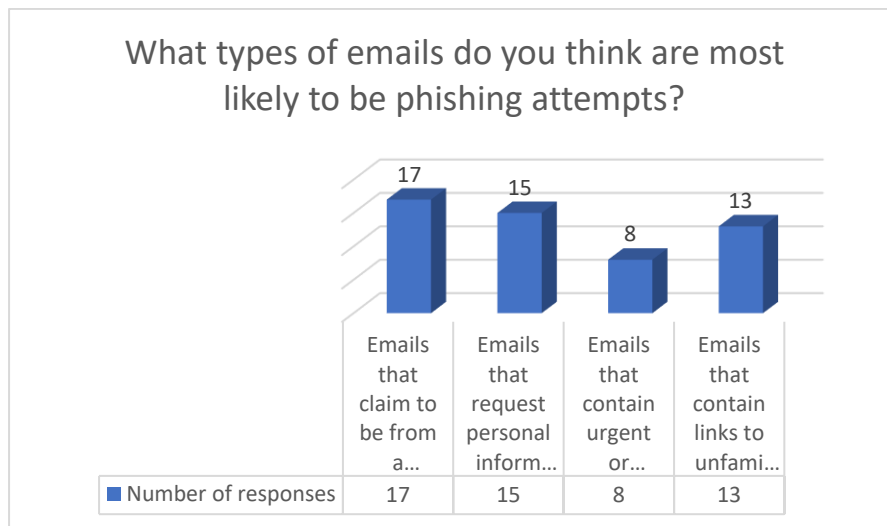
- **Q3 – How confident are you in your ability to identify a phishing email?**



**FIGURE 8 Q3 - HOW CONFIDENT ARE YOU IN YOUR ABILITY TO IDENTIFY A PHISHING EMAIL?**

The bar chart shows that most respondents (18) are somewhat confident in their ability to spot fake emails and (20) are not at all confident in their ability to do so. Only 13 individuals are very confident in their ability to spot fake emails, and only 2 are not very confident.

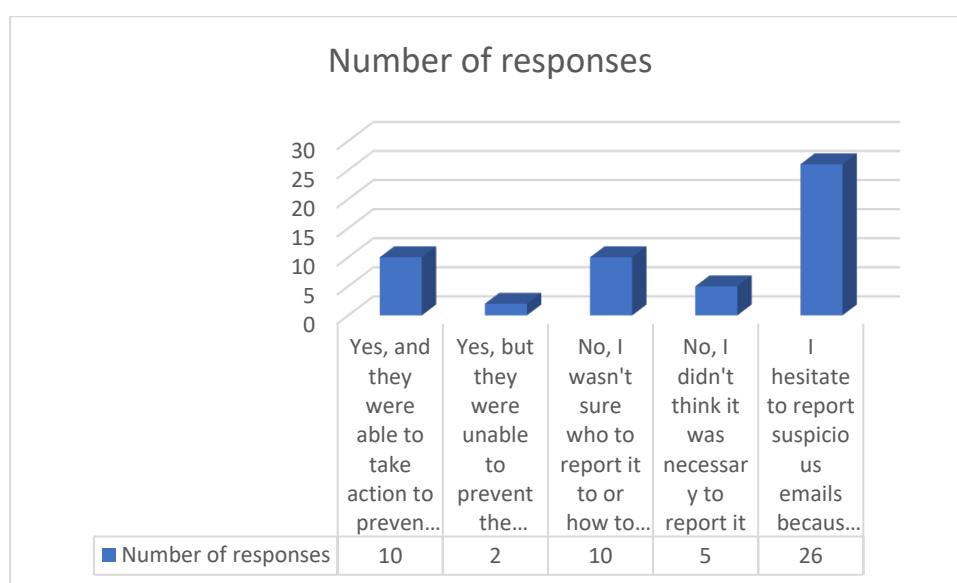
- **Q4 – What types of emails do you think are most likely to be phishing attempts?**



**FIGURE 9 Q4 - WHAT TYPES OF EMAILS DO YOU THINK ARE MOST LIKELY TO BE PHISHING ATTEMPTS?**

The bar chart shows that people think the most likely scam emails are those that claim to be from banking institutions (17) and those that ask for personal information (15). Emails with urgent or frightening wording (8) and links that look strange (13) are also thought to be risky.

- **Q5 – Have you ever reported a phishing email to your IT department or security team?**



**FIGURE 10 Q5 - HAVE YOU EVER REPORTED A PHISHING EMAIL TO YOUR IT DEPARTMENT OR SECURITY TEAM?**

The bar chart shows that 26 of the people who answered the survey don't report strange emails because they aren't sure if they are hacking attempts. Some people have reported fake emails, and their IT staff or security team did something about it (10), while others have done the same but nothing was done about it (2). Some people didn't fill out the form because they didn't know how (10) or thought it wasn't important (5).

- **Q6 - How do you think companies can better educate their employees about phishing emails?**

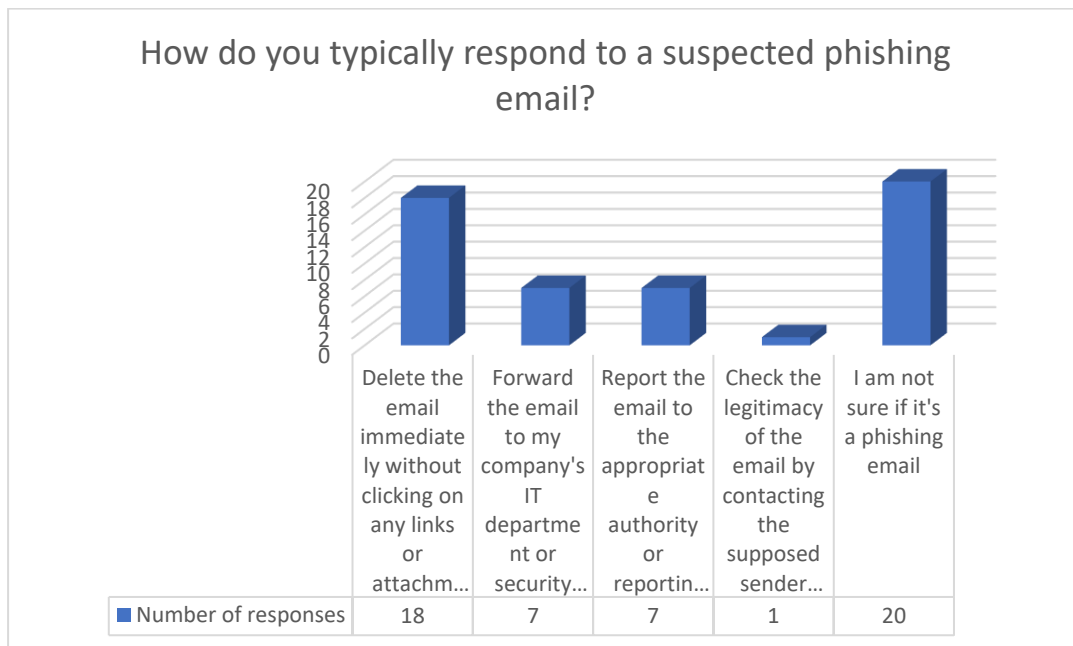


**FIGURE 11 Q6 - HOW DO YOU THINK COMPANIES CAN BETTER EDUCATE THEIR EMPLOYEES ABOUT PHISHING EMAILS?**

The bar chart shows that respondents think that the best ways for companies to teach their employees about scam emails are through regular security training meetings (22) and phishing exercises (17). People also think that providing educational tools (10) and encouraging sharing with comments (4) are good ways to help.



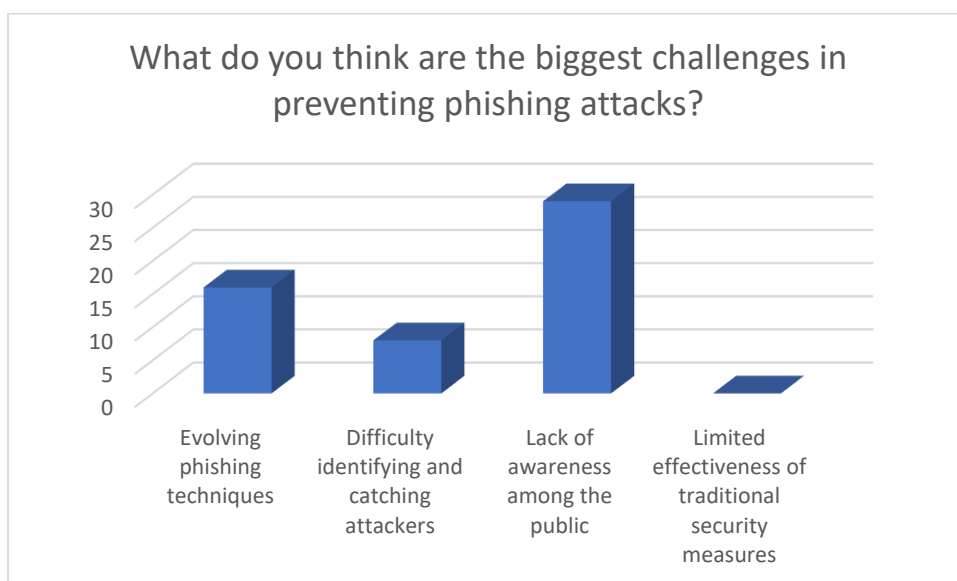
- **Q7 – How do you typically respond to suspected phishing email?**



**FIGURE 12 Q7 - HOW DO YOU TYPICALLY RESPOND TO A SUSPECTED PHISHING EMAIL?**

The bar chart shows that most of the people who answered either deleted the email right away without clicking any links or files (18) or didn't know if it was a scam attempt (20). Fewer people send the email to their company's IT staff (7), report the email to the right people (7), or call the writer directly (1) to make sure the email is real.

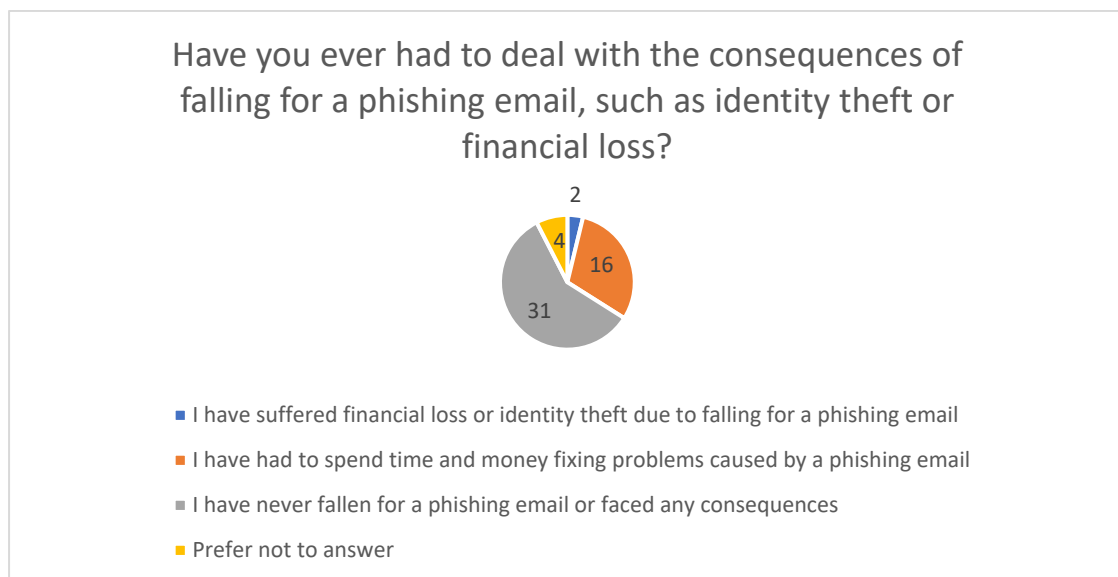
- **Q8 – What do you think are the biggest challenges in preventing phishing attacks?**



**FIGURE 13 Q8 - WHAT DO YOU THINK ARE THE BIGGEST CHALLENGES IN PREVENTING PHISHING ATTACKS?**

The bar chart shows that most of the people who answered think that the biggest problem with stopping phishing attacks is that the public is not aware of them (29). Changes in hacking methods (16) and the difficulty of finding and getting attackers (8) are also seen as big problems, but no one said that standard security measures aren't as good as they used to be.

- **Q9 – Have you ever had to deal with the consequences of falling for a phishing email, such as identify theft or financial loss?**



**FIGURE 14 Q9 - HAVE YOU EVER HAD TO DEAL WITH THE CONSEQUENCES OF FALLING FOR A PHISHING EMAIL, SUCH AS IDENTITY THEFT OR FINANCIAL LOSS?**

The pie chart shows that most of the people who answered (31 of them) have never been tricked by a scam email or had to deal with the results. Some of the people who answered have spent time and money fixing problems that spam emails caused (16), and a few have lost money or had their name stolen (2). Only a few of the people who were asked chose not to answer the question (4).

### 8.1.2 Overall

Overall , the result of the phishing email poll us a lot about people have dealt with phishing emails and how well they can identify them. The data above shows that most of the people who have answered the survey get a lot of scam emails less than once a month or between one and three months. Most of them haven't fallen for a fake email or were close to falling for it. It's important to note that some of them have lost money, had their identity stolen or cost money to get them fixed.

The survey also shows that its vital to learn more about phishing emails or be more aware of them. Many people didn't feel confident at all spotting phishing emails and the lack of knowledge was seen as the biggest problem. Non-IT users can say that companies can do a better job educating their workers by giving them regular security training, hacking scenarios and other learning tools.

When non-IT thing an email is a phishing attempt, they would usually delete it right away without even clicking any links or opening any files. A large number of respondents don't know if an email is a phishing attempt or not. This might be the lack of education and how quickly hackers tactics change and how hard it is to find and catch attackers.

In conclusion, the survey shows how important it is to make people aware of phishing emails and teach them and their workers how to spot them, report them and reply to them.

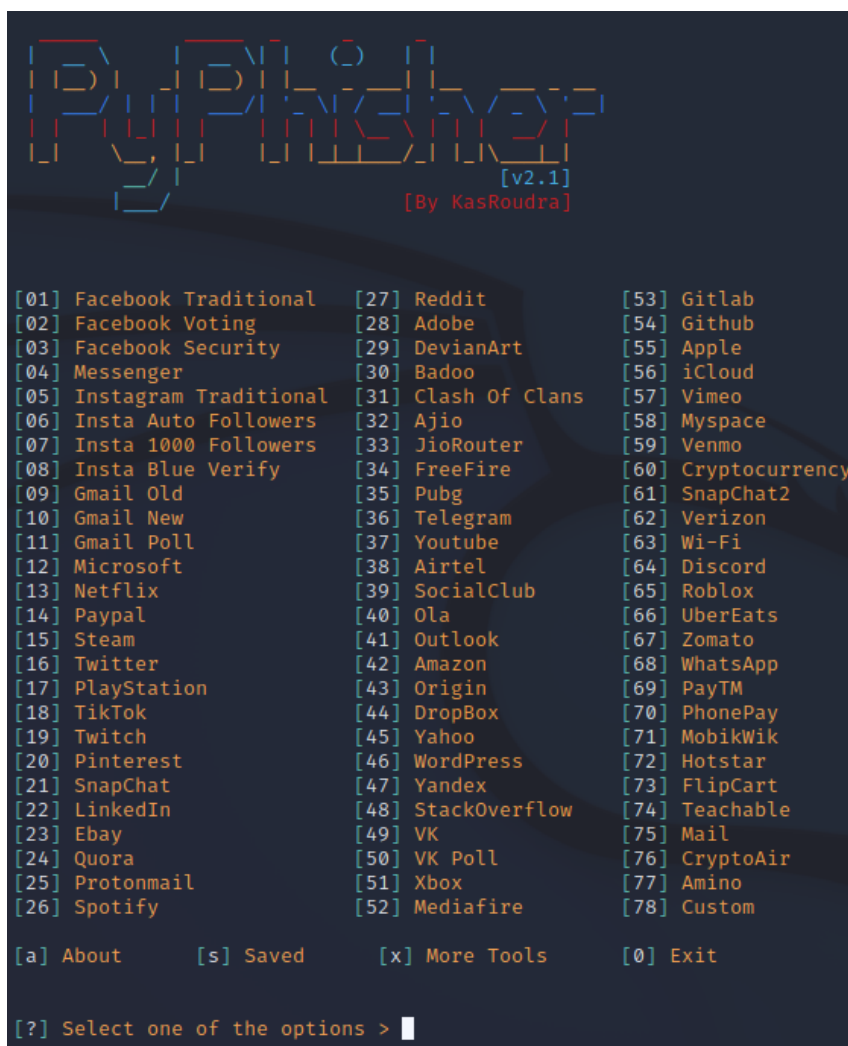
As phishing attacks continue to change, it is important to make people aware of the risks they spread and best ways to find them.

## 8.2 Phishing email Testing

### 8.2.1 Testing with Pyphisher

In the subsequent discourse, my actions were predominantly determined by my determination to conduct exhaustive experiments. My initial project required the use of a tool incorporating social engineering techniques, specifically the PyPhisher tool. This tool enabled me to generate and send electronic messages to my own address, thereby facilitating a subsequent analysis of their authenticity.

Figure 15 outlines the upcoming case study, which will illustrate a typical Facebook authentication procedure.



```
[v2.1]
[By KasRoudra]

[01] Facebook Traditional  [27] Reddit                [53] Gitlab
[02] Facebook Voting      [28] Adobe                  [54] Github
[03] Facebook Security    [29] DevianArt               [55] Apple
[04] Messenger             [30] Badoo                   [56] iCloud
[05] Instagram Traditional [31] Clash Of Clans         [57] Vimeo
[06] Insta Auto Followers  [32] Ajio                   [58] Myspace
[07] Insta 1000 Followers  [33] JioRouter              [59] Venmo
[08] Insta Blue Verify     [34] FreeFire               [60] Cryptocurrency
[09] Gmail Old              [35] Pubg                   [61] SnapChat2
[10] Gmail New              [36] Telegram               [62] Verizon
[11] Gmail Poll             [37] Youtube                [63] Wi-Fi
[12] Microsoft              [38] Airtel                 [64] Discord
[13] Netflix                [39] SocialClub             [65] Roblox
[14] Paypal                 [40] Ola                    [66] UberEats
[15] Steam                  [41] Outlook                [67] Zomato
[16] Twitter                [42] Amazon                 [68] WhatsApp
[17] PlayStation            [43] Origin                 [69] PayTM
[18] TikTok                 [44] DropBox                [70] PhonePay
[19] Twitch                 [45] Yahoo                  [71] MobikWik
[20] Pinterest              [46] WordPress              [72] Hotstar
[21] SnapChat               [47] Yandex                 [73] FlipCart
[22] LinkedIn               [48] StackOverflow          [74] Teachable
[23] Ebay                   [49] VK                     [75] Mail
[24] Quora                  [50] VK Poll                [76] CryptoAir
[25] Protonmail             [51] Xbox                   [77] Amino
[26] Spotify                [52] Mediafire              [78] Custom

[a] About    [s] Saved    [x] More Tools  [0] Exit

[?] Select one of the options > |
```

FIGURE 15 PYPISHER (FACEBOOK)

```
rohit@kali: ~/PyPhisher
File Actions Edit View Help

[By KasRoudra] [v2.1]

[*] Initializing PHP server at localhost:8080....
[+] PHP Server has started successfully!
[*] Initializing tunnelers at same address.....
[+] Your urls are given below:

CloudFlared
URL : https://attributes-wins-beyond-surround.trycloudflare.com
MaskedURL : https://blue-verified-facebook-free@attributes-wins-beyond-surround.trycloudflare.com

LocalHostRun
URL : https://01ff5fe24c031e.lhr.life
MaskedURL : https://blue-verified-facebook-free@01ff5fe24c031e.lhr.life

[?] Wanna try custom link? [y or press enter to skip] : www.facebook.com
[?] Enter custom domain(Example: google.com, yahoo.com > facebook.com
[?] Enter bait words with hyphen without space (Example: free-money, pubg-mod) > Click-here

Custom
URL : https://facebook.com-Click-here@is.gd/2WNEpL

[+] Waiting for login info....Press Ctrl+C to exit
```

FIGURE 16 CREATING A FACEBOOK LINK

In Figure 16, you can see how a Facebook link is made. This URL has been changed to try to make the link more trustworthy. This method tries to make the link look like a normal, original link. This gives the link a better reputation for being real.

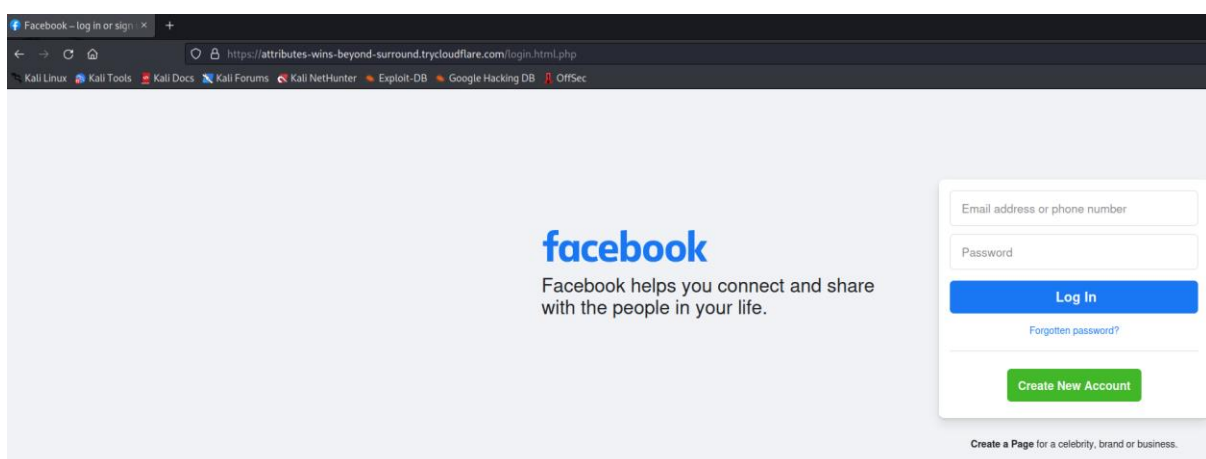
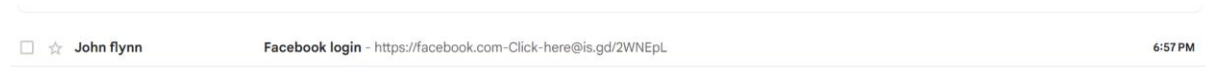


FIGURE 17 FACEBOOK PROTOTYPE

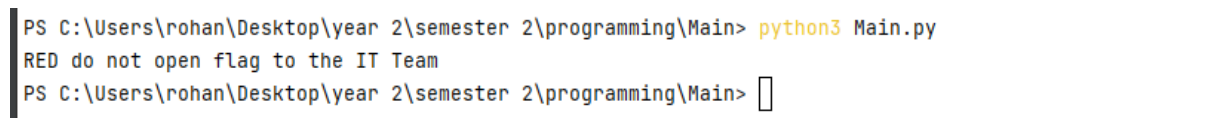
Figure 17 shows that if you click on the link above, you will be taken to a page that looks just like Facebook's user interface. It's important to know that even people who don't know much

about Information Technology (IT) could easily use this website and enter data. Because the website is easy to use and looks real, people may not realise what it is really for.



**FIGURE 18 EMAIL SENT TO ME**

I chose to send the created link to my personal Gmail account so I could do a more thorough study. Strangely, a programme I made can tell the difference between a fake link and a real one. By looking at this information, you can find out more about whether or not the link in question is real.



**FIGURE 19 RESULTS OF THE FACEBOOK**

Figure 19 shows that the next step in the study was to check the link with two security tools, VirusTotal and URL Scanner. The point of these sites is to make sure the link is real by checking it. After a close look, it was clear that the link didn't follow the rules of a real connection. This shows that it was made up.

## Fake Links:

Social Media	Link	Colour
Facebook Traditional	https://facebook.com-Click-here@is.gd/2WNEpL	RED
Messenger	https://messenger.com-Click-here@is.gd/wBMQWZ	RED
Twitter	https://twitter.com-is.gd/8c3it1	RED
LinkedIn	https://LinkedIn-Login-in@is.gd/WqyGdt	RED
Outlook	https://outlook.com-Reset-password@is.gd/IutEG8	RED
Spotify	https://Spotify.com-Login@is.gd/MIExHR	Yellow
Ebay	https://www.ebay.com-Login-@is.gd/qVmSSL	Yellow

After that, I looked at other social media sites to add to what I knew. The goal of this update was to find out if the tool could find problems on any website or if it only worked on certain kinds of websites. The goal of this complicated study was to find out how flexible and reliable the tool was at finding fake links across different websites.

## Spam Links

I tried to learn more about how the tool could be used in the next round of tests. I tried it in particular with a Yahoo email account that was set up to send spam. The main goal was to find out if the tool still works well to examine links that are built into this email platform.

The fact that these links were hidden in pictures made them more interesting. This is a way that hackers often hide where a link really goes. When I got the URLs for these links that were in pictures, I sent them to the final project so that it could take a closer look. So, this project pushed the boundaries of how the tool could be tried, giving us more information about how it works in different settings.

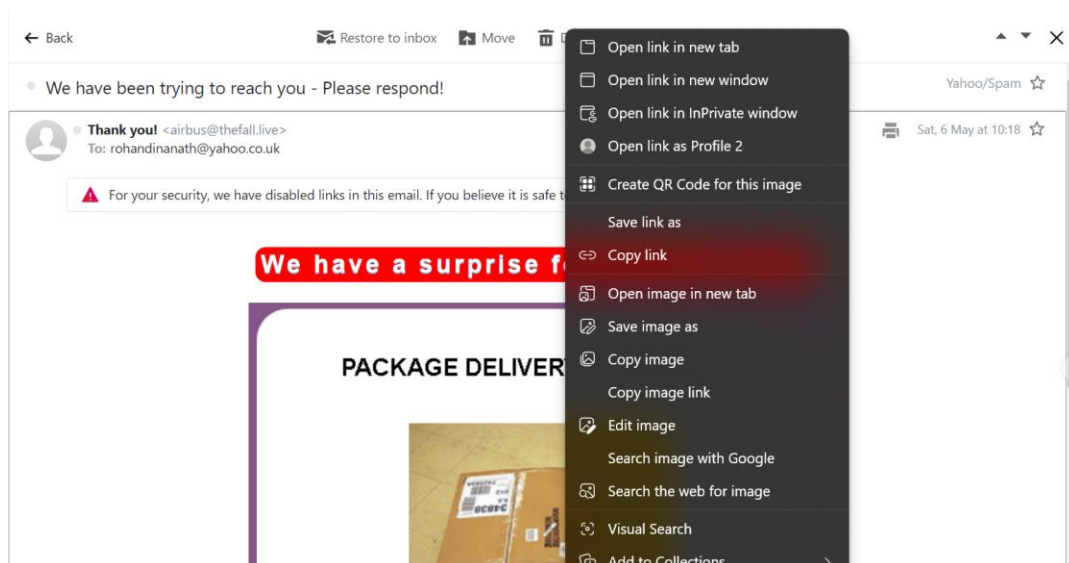


FIGURE 20 SPAM EMAILS

Figure 20 shows that the next step in my project was to look at my spam emails. To do this, I had to get the URLs from these emails and put them into my tool so it could examine them.

The idea was to see if the software could tell if these links were real or not. If it could, that would show that it can be used to find and stop threats that come from spam emails.

<input type="checkbox"/> ☆ Rohan Dina Nath	Link 1 - <a href="http://thefall.live/rd/c45653UvxXJ8536366uEgd10923sDQ60018BRQY5891">http://thefall.live/rd/c45653UvxXJ8536366uEgd10923sDQ60018BRQY5891</a>	8:44 PM
<input type="checkbox"/> ☆ John flynn	login - original link - <a href="https://www.facebook.com/">https://www.facebook.com/</a>	8:35 PM
<input type="checkbox"/> ☆ John flynn	Login to receive your ebay - <a href="https://www.ebay.com/Login-@is.gd/qVmSSL">https://www.ebay.com/Login-@is.gd/qVmSSL</a>	8:33 PM

**FIGURE 21 LINK TO MY EMAIL**

In Figure 21, the person doing the trial tried a slightly different method. They chose to send the clipped URLs to their personal email account to see if the security systems of their email service could recognise these links as possible threats. The goal of this move was to find out how well popular email services can spot fake attacks. This would tell us a lot about how well these services work as the first line of defence against online risks like these.

```
PS C:\Users\rohan\Desktop\year 2\semester 2\programming\Main> python3 Main.py
Yellow flag to the IT Team
PS C:\Users\rohan\Desktop\year 2\semester 2\programming\Main>
```

**FIGURE 22 CHECKED WITH MY TOOL**

Figure 22 shows that the result of this trial was to name the URLs as "yellow." This color-coded way is a middle-of-the-road warning. It tells you that the link might not look bad at first glance, but there are signs that you should be careful. This rating lets users share cases that aren't clear to their IT teams, which helps the company protect itself more proactively. This reporting method adds an extra layer of security and gives IT experts a chance to learn more about possible threats and stop them.

## Fake Links from Spam

Link 1:	<a href="http://thefall.live/rd/c45653UvxXJ8536366uEgd10923sDQ60018BRQY5891">http://thefall.live/rd/c45653UvxXJ8536366uEgd10923sDQ60018BRQY5891</a>	
Link 2 :	<a href="http://jaiuber.site/rd/c44678nBwOz8536366bjls10923khH59989PMFw4660">http://jaiuber.site/rd/c44678nBwOz8536366bjls10923khH59989PMFw4660</a>	
Link 3:	<a href="http://jaiuber.site/rd/c45630zpqxp8536366UTSH10923usu58722wYLu6231">http://jaiuber.site/rd/c45630zpqxp8536366UTSH10923usu58722wYLu6231</a>	
Link 4:		



Link 5:		
Link 6:		
Link 7:		
Link 8:		

The results show that the recognition software marked as "yellow" all of the links in my junk inbox. This neat grouping shows how dangerous it is to click on URLs in spam emails. Because of this risk, you should avoid clicking on these sites. Instead, these cases should be recorded and brought to the attention of the IT team. This step makes sure that cybersecurity experts deal with the possible threats in the right way. This makes the organisation more secure and lowers the chance of a break-in.

## 9. Conclusion

In conclusion, this study has shown how widespread and complicated phishing risks are, highlighting their importance in the modern cybersecurity scene. The study also showed how important it is to keep educating people, develop better ways to find them, and make users more aware.

The poll results were helpful because they showed how people in real life have dealt with and thought about hacking threats. It was found that most of the people who answered the survey get scam emails at an alarmingly high rate. While many people can recognise and avoid these threats, a large number of people still fall for them. This shows that users need better education and training to help them recognise scam and respond to it better.

In this study, the actual use of the Pyphisher tool helped show how complicated and cunning phishing attempts can be. As we've seen, it's shockingly easy for bad people to hide their plans behind what look like normal interactions, which can trick even careful users into falling for their scams.

The study's examination of the Pyphisher tool also showed how useful it is for finding links that could be dangerous on social media sites and in spam emails. But the fact that there are 'Yellow' flagged links, which indicate possible but not proven threats, shows how subtle and complicated phishing attempts can be. Not all hacking attempts are obviously bad, and standard ways of finding them can often miss them. This makes it harder to find them and stop them.

So, this study has shown how important improved anti-phishing tools are to a full protection plan. But tools like Pyphisher are only a small part of the whole. The end customer, who is a part of the human element, is a key part of the fight against scams. Phishing risks can be reduced by making users more aware of them, giving them regular training, and putting in place improved tracking tools.

The results of this study have important effects for people, organisations, and the wider cybersecurity community as a whole. They also provide practical information that can be used to improve anti-phishing tactics in the future. As hacking techniques change, so must the ways we protect ourselves. Fighting hacking is a constant, ever-changing process that requires a multifaceted approach and a commitment to learning, changing, and staying alert all the time.

This research has set a strong basis for future studies in this area, and it is hoped that future research will continue to build on this work, finding new ways to stop hacking and promoting a culture of safety knowledge. In the end, we all have a part to play in the fight against hacking, and only by working together can we hope to stay one step ahead of the phishers.

### 9.1 Answering the Questions

- How can employee training and awareness programs be developed and implemented to improve resilience against phishing emails within organizations?

The poll results in this thesis show that hacking efforts can be stopped by training and learning programmes for all employees. Non-IT users don't know much about phishing emails, which shows how important it is to raise understanding. Here are some things that organisations can do to become more resistant to scam emails:

Employee education shouldn't be a one-time thing. They should be trained regularly. Training should be an ongoing process, with regular lessons on hacking techniques, how to spot scam emails, and what to do if you get one. Real-world cases can be used to show how phishing works, and training materials should be updated to include the most recent phishing methods.

Simulated phishing exercises: Imitating phishing attacks is a great way to train. Employees learn how to spot scam attempts in a safe and controlled setting, and they can get hands-on practise with how to deal with these emails.

Use the Phishing Application: The Python application made for this thesis can be a very useful tool for training programmes for employees. By making this tool a regular part of workers' work, they can learn how to use it to spot possible phishing emails. This will help them learn more about hacking and be better able to spot phishing attempts.

Encourage a culture of cybersecurity by asking workers to talk about their experiences with scam emails and what they know about them. This not only keeps everyone up-to-date on the latest tricks, but also creates an atmosphere where safety is valued.

Encourage safe behaviour by giving rewards or praise to employees who spot or avoid virtual hacking attempts. This can encourage employees to pay more attention during training classes and be more careful in their daily lives.

Give Continuous Support: There should be a designated team or person who can help workers with fake emails or answer any questions they may have. This makes sure that workers don't have to figure out what to do when they get strange texts.

By using these methods, organisations can make themselves much more resistant to hacking efforts. Not only do you need the right tools, but you also need to make sure that your workers know how to use them well and understand how important their part is in keeping the organization's safety safe.

## Referencing

Stojnic, T., Vatsalan, D. and Arachchilage, N.A.G. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. *Security and Privacy*, [online] 4(5). doi:<https://doi.org/10.1002/spy2.165>.

AAG IT Services. (2023). *The Latest Phishing Statistics (updated March 2023) | AAG IT Support*. [online] Available at: <https://aag-it.com/the-latest-phishing-statistics/#:~:text=Yes%2C%20phishing%20is%20the%20most,emails%20are%20sent%20every%20day>.

Ncsc.gov.uk. (2023). *Phishing attacks: defending your organisation*. [online] Available at: <https://www.ncsc.gov.uk/guidance/phishing> .

Digital Brand Protection – FraudWatch. (2023). *Phishing protection and prevention services | FraudWatch*. [online] Available at: <https://fraudwatch.com/services/phishing/> .

Trend Micro. (2021). *What Is Phishing?* [online] Available at: [https://www.trendmicro.com/en\\_us/what-is/phishing.html](https://www.trendmicro.com/en_us/what-is/phishing.html) .

Kaspersky (2021). *All About Phishing Scams & Prevention: What You Need to Know*. [online] [www.kaspersky.com](https://www.kaspersky.com). Available at: <https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips> .

Zetter, K. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. [online] WIRED. Available at: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> .

Fazzini, K. (2019). *Google and Facebook got tricked out of \$123 million by a scam that costs small businesses billions every year — here's how to avoid it*. [online] CNBC. Available at: <https://www.cnbc.com/2019/03/28/how-to-avoid-invoice-theft-scam-that-cost-google-facebook-123m.html> .

NPR. (2019). *Man Pleads Guilty To Phishing Scheme That Fleeced Facebook, Google Of \$100 Million*. [online] Available at: <https://www.npr.org/2019/03/25/706715377/man-pleads-guilty-to-phishing-scheme-that-fleeced-facebook-google-of-100-million> .

Hickey, M. and Arcuri, J. (2020). *Hands on Hacking*. [online] John Wiley & Sons. Available at: <https://www.wiley.com/en-us/Hands+on+Hacking%3A+Become+an+Expert+at+Next+Gen+Penetration+Testing+and+Purple+Teaming-p-9781119561453> .

ACM Conferences. (2014). *Amandroid / Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. [online] Available at: <https://dl.acm.org/doi/10.1145/2660267.2660357> .

Trendmicro.com. (2023). *Spear phishing - Definition*. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing>.

Trendmicro.com. (2021). *Spear Phishing 101: What is Spear Phishing? - Wiadomości bezpieczeństwa*. [online] Available at: <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing> .

Proofpoint. (2022). *What Is CEO Fraud?* [online] Available at: <https://www.proofpoint.com/uk/threat-reference/ceo-fraud> .

Fortinet. (2022). *What Is a Whaling Attack? Examples and Statistics / Fortinet*. [online] Available at: <https://www.fortinet.com/resources/cyberglossary/whaling-attack> .

Radware (2022). *Security Research Center / Radware*. [online] Radware.com. Available at: <https://www.radware.com/security/> .

Gartner. (2021). *Best Practices for Implementing DMARC*. [online] Available at: <https://www.gartner.com/en/documents/3992242> .

Norton.com. (2022). *What is smishing + smishing attack protection tips for 2022 / Norton*. [online] Available at: <https://us.norton.com/blog/emerging-threats/smishing#> .

GET THE FULL REPORT Want to learn more? The 2021 State of the Phish report includes data from: Get the report for a detailed picture of today's phishing threat and steps you can take to build a people-centric cybersecurity strategy that helps enhance user awareness, reduce risk and make your people more resilient. [www.proofpoint.com/us/resources/threat-](https://www.proofpoint.com/us/resources/threat-)

reports/state-of-phish. (n.d.). Available at:

<https://www.proofpoint.com/sites/default/files/infographics/pfpt-us-sotp-infographic.pdf> .

Tessian. (2023). *Data Loss Prevention in Financial Services 2021 - DLP Research -*

*Tessian*. [online] Available at: <https://www.tessian.com/research/the-state-of-data-loss-prevention-in-financial-services/> .

Norton.com. (2020). *Beware of these coronavirus scams*. [online] Available at:

<https://us.norton.com/blog/online-scams/coronavirus-phishing-scams> .

FBI (2021) '2020 Internet Crime Report Released', Federal Bureau of Investigation.

Available at: <https://www.fbi.gov/news/stories/2020-internet-crime-report-released-021721> .

Hadnagy, C. and Fincher, M. (2015). *Phishing Dark Waters*. [online] John Wiley & Sons.

Available at: <https://www.perlego.com/book/997226/phishing-dark-waters-the-offensive-and-defensive-sides-of-malicious-emails-pdf>.

ACM Conferences. (2023). *Why phishing works / Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. [online] Available at:

<https://dl.acm.org/doi/10.1145/1124772.1124861> .

Rose, S., Larson, M., Massey, D., Austein, R. and Arends, R. (2005). *RFC 4033: DNS Security Introduction and Requirements*. [online] IETF Datatracker. Available at:

<https://datatracker.ietf.org/doc/rfc4033/> .

Mehrdad Bagheri-Sanjareh, Mohammad Hassan Nazari and Gharehpetian, G.B. (2020). A Novel and Optimal Battery Sizing Procedure Based on MG Frequency Security Criterion Using Coordinated Application of BESS, LED Lighting Loads, and Photovoltaic Systems. *IEEE Access*, [online] 8, pp.95345–95359.

doi:<https://doi.org/10.1109/access.2020.2995461>.

Kumar, P., & Sachdeva, M. (2020). A comprehensive survey on email spam detection and filtering techniques. *Journal of Ambient Intelligence and Humanized Computing*.

Liu, H., Li, J., Yang, Y., & Zou, D. (2021). A comprehensive survey on phishing attacks and defenses. *IEEE Communications Surveys & Tutorials*.

Mishra, D., Sharma, A., Singh, R., & Joshi, G. P. (2020). A comprehensive review on content-based spam filtering. In *Advances in Data and Information Sciences*. Springer, Singapore.

Nikiforakis, N., Balduzzi, M., & Van Acker, S. (2021). A decade of malvertising: A longitudinal study of the malicious advertising ecosystem. *ACM Transactions on Privacy and Security*.

Ramachandran, A., & Feamster, N. (2019). Understanding the network-level behavior of spammers. *ACM SIGCOMM Computer Communication Review*.

Raff, E., Nicholas, C., & McLean, M. (2020). Malware detection by eating a whole exe. In *Proceedings of the AAAI Conference on Artificial Intelligence*.

A., & Thabtah, F. (2021). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*.

Alam, M. M., Rahman, M. S., & Rahman, M. M. (2021). A survey of deep learning techniques for email spam classification. *Expert Systems with Applications*.

Chen, X., & Guo, Y. (2020). Adaptive spam email detection based on deep learning. *Computers, Materials & Continua*.

Dey, S., Roy, S., & Das, A. K. (2020). A survey on various email spam filtering techniques. In *Advances in Communication, Devices and Networking*. Springer, Singapore.



