A Study of AIOT in Detecting Social Engineering Attacks: Phishing and Identity Theft

Ateefa Rehan Siddiqui [1], Nor Azlina Abd Rahman [2] and Khalida Shajaratuddur Harun[3]
[2]Forensic and Cyber Security Research Centre
[123]Asia Pacific University, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1] TP 066244@mail.apu.edu.my, [2]nor_azlina@apu.edu.my, [3]khalida@staffemail.apu.edu.my

***Abstract*— With the advancement of technology, the Internet is becoming ubiquitous and available to everybody. There is a plethora of websites that provide various advantages. Despite their large quantity, not all these websites are genuine. Phishing sites are websites that trick people into serving their objectives. Phishing assaults, which have been around for ages and are still a huge issue today, pose a severe threat to the cyber world. Attackers are using a variety of innovative and inventive tactics to carry out phishing assaults, which are on the rise. Web browsing's pervasiveness in our everyday lives, however, is not without security hazards. This standard web browsing habit, along with web users' poor situational awareness of cyber dangers, exposes them to Phishing, malware, and profiling, among other hazards. Furthermore, phishing assaults are frequently used as an attack vector or the first stage in a more complex attack in today's security climate. The usual method of comparing websites by using a blacklist and a whitelist is ineffective. As attackers have gotten more sophisticated in concealing and redirecting URLs, they may now fool users into phishing attacks without being caught. These Phishing attacks are used to commit all sorts of criminal activities like identity theft, whether in the form of Document theft, financial fraud, or medical fraud. As a result, new methodologies on machine learning algorithms (ML) are required to detect these phishing websites.**

***Index Terms*—AIOT, phishing, Machine Learning, Identity Theft**

1. Introduction

In numerous parts of the world, crimes are categorized into different categories, despite how exceptional law approval associations may be liable for disclosing explicit kinds of criminal (e.g., customs divisions may be blamed for battling pilfering and related offenses). Wrongdoing can be sorted into three detectable stages: the disclosure that misconduct has been completed, the distinctive verification of a suspect, and the grouping of sufficient evidence to summon the suspect under the watchful of a court. Just like customs officers are present at the airport to ensure passengers are not bringing illegal stuff into the country. Cyber security was made to ensure that people or organizations taking part in cyber-crimes are caught and punished. Cybercrimes are classified into different types as shown in figure 1. In today's world, technological advancement has made it possible for police power, customs, and specialists to distinguish any wrongdoings, such as drug dealing, sneaking firearms, mule account, and various violations. Nowadays, the Internet of Things (IoT) and Artificial Intelligence (AI) are comprehensively used in adventures and affiliations. The joining of these two developments will be astonishing advances called Artificial Intelligence of Things or AIoT.

Countless organizations are now using software that have AI, IoT or combining them both as AIoT to help them solve crimes.

Figure 1: Cyber - Crime Examples [1]

2. Literature Review

There are many types of Social Engineering attacks, but the focus of this research is on the Phishing attack and Identity Theft.

2.1 Phishing

The motivation of hackers behind this attack is to steal an individual's private information that may include financial details like credit or debit card information, account information, and login credentials. It happens when an assailant, taking on the appearance of a confided in substance, hoodwinks a casualty into opening an email, text, or instant message. The hackers convey something similar and make individuals enter their qualifications. These days this is done chiefly through messages [2]. Many phony locales are accessible and are utilized by phishers to extortion individuals by

- Sending counterfeit sends and taking their private information
- Making them a casualty of email phishing by sending any vindictive emails that the client will unconsciously open along these lines stalled out in their snare.

It is a type of misrepresentation where the assailant addresses himself to be certified substance and assault through correspondence channels. There are many types of Phishing as email phishing, smishing, HTTPS phishing, vishing, spear phishing and whaling/ CEO fraud [3].

2.1.1 Understanding Phishing

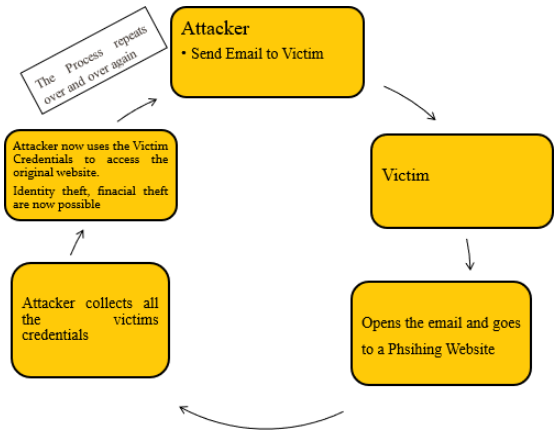

Figure 2: How Phishing Works [4]

Phishing can be viewed as a sort of online data fraud. It is typically directed through sending email messages to (a great many) expected casualties. These messages are commonly conveyed in mass to serve as an enticement", "professing to be from people or organizations that the beneficiary of the message might trust, requesting private and touchy data. The substance of these messages is consequently intended to attract the beneficiary into unveiling their subtleties. The phisher would then utilize these subtleties to get sufficiently close to the casualty's monetary records.

2.2 Understanding Identity Theft

Identity theft happens when the utilization of individual subtleties to acquire labor and products. The critical highlight note here is that fraud can be submitted for reasons other than monetary profit, and it very well may be submitted against individuals who are alive or dead.

Between 2019 - 2020, it is assessed that 3.7 million reports were made of individuals being the objective of false movement –wrongdoing which presently costs the UK public area between £31 billion and £48 billion every year. Besides these personal and public expenses, genuine worries about such wrongdoings are utilized to support coordinated wrongdoing and psychological oppression. Without a doubt, when we ponder 'fraud,' our considerations will generally zero in on the dread of somebody taking our investment funds. However, the truth can be more slippery than that [5].

The reasons for Identity fraud can include:

- Unlawful migration status
- Sidestepping loan bosses
- Acting like another person via web-based media
- Sidestepping capture for crime
- Protection extortion
- Financial Gain
- Taking Possession of Properties

There are three main types of Identity Theft

1. Medical Identity Theft
2. Financial Identity Theft
3. Online Identity Theft

3. Tools Used to Detect Phishing

Many different tools are currently present in the market for detecting Phishing. Nevertheless, before a company or an individual buys these tools, they must make sure that they have taken some precautions to minimize the risks from the attacks. Specific Protocols are present that can be implemented. The name of few of these protocols are:

- Sender Policy Frameworks
- Domain Keys Identified Mail (DKIM)
- Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

Although they might not be perfect when implemented, these protocols can save an individual from some of the malicious emails coming into their inbox [6].

3.1 BrandShield Anti-Phishing

It centers around brand security and corporate trust. Its toolset screens online media and other central focus to identify phishing locale (in any event, searching for your corporate logo) and reacting with takedown demands, and adding these vindictive destinations to a different enemy of phishing boycotts.

3.2 Ironscales

It increases an individual's current email security by consolidating AI-based ID and human cooperation (through warnings) to rapidly react to expected assaults while at the same time restricting bogus up-sides. Administrators likewise learn both the nature and extent of the danger, including the number of letter drops designated and the number of clients who announced the email.

3.3 Avanan

It is one of a few SaaS stages that improves the security of Office 365, G Suite, and others. Since Avanan is cloud-based and interfaces with each person's respective Office 365 or G Suite occasion utilizing APIs, it is efficient to set up and ensure something beyond email.

3.4 Sophos Email

It uses both strategy and AI-based location in its SaaS stage and elements a self-administration entryway to permit clients to deal with their isolations securely. Sophos can likewise distinguish clients who show hazardous conduct and appoint reproduction-based preparing to alleviate further danger from these clients.

4. Tools used to detect Identity Theft

Below are some of the tools that are used for detecting Identity Theft [7];

4.1 SolarWinds Identity Monitor

It is a simple but effective tool that helps monitor email and websites for data breaches. It will inform the person if their credentials have leaked and through forced password rests for

those accounts, making the credibility of stolen information zero.

4.2 Soniq Identity Force

This service might not be as cost-effective, but it is a demonstrated protection, personality, and credit security arrangement, with cutting-edge location innovation. It utilizes five steps to identify theft monitoring which are Monitor, Alert, Control, Recover and Credit

4.3 IdentityIQ

It is another data fraud observing project great at offering all-around insurance. It joins credit announcing and score conveyance, credit observing, dim web checking, personality security, application checking, character rebuilding, and family insurance utilities to give a set-up of assurance instruments intended to provide an individual inner serenity

4.4 LifeLock

LifeLock, by Norton, is a well-known decision among individuals searching for powerful character observing administrations. Norton 360 with LifeLock mix gives an across-the-board insurance arrangement covering web-based protection gadgets. This instrument can obstruct cyberthreats by utilizing Norton innovation, which impedes a normal of 142 million dangers consistently

4.5 Shufti Pro

It is an AI-powered technology that provides identity verification over several services in 200+ countries around the globe. The main goal of this software is to provide a safe online place that's is void of identity theft.

5. Methodology

5.1 Vulnerabilities and Risk Management

In a recent report directed by TNS Global for Halon, an email security administration, 30% of the overviewed people included 1,000 grown-ups in the US, unveiled that they would open an email regardless of whether they knew it contained an infection or was dubious [8]. According to research done by Sophos Email, it was seen that overall, 41% of organizations had been a daily phishing attack target while 77% faced monthly attacks [9].

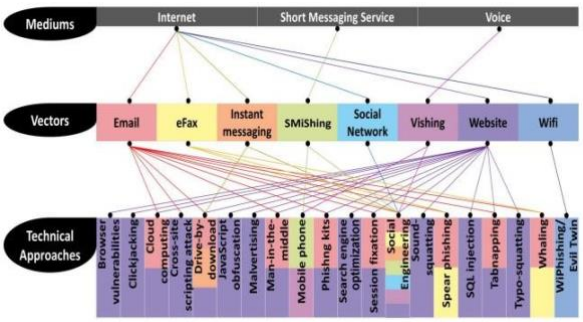

Figure 3: A Structure Detailing The Principle Parts Of A Phishing Assault And The Connections Among Them [10]

5.2 Criminal Activities Using Phishing

Since we all know that hackers or cyber-criminals are using Phishing attacks to perform criminal activities like:

5.2.1 Identity Theft or Fraud

Hackers will send mass spam messages to people's email account. These emails usually ask people to enter their confidential information by replying to this email. Usually, these emails come with some warning. For example, if the user does not reply to this email, their record will be obliterated.

These emails also have fake promises, like if the person clicks on the link provided in the email, he/ she can win a ticket for a trip to Moscow.

5.2.2 Spear Phishing

These types of emails usually are made to look like they are from a trusted source. For example, they can be from a website that a person has subscribed to do, or it can look like the email came from the company CEO or the IT Manager asking the individual to transfer money to a said account. For example:

According to a Senior Contributor [11] of Forbes Magazine. Google announced that after 2017 its email would use AI technology for detecting Phishing emails. In March of 2016, John Podesta's account was hacked using a phishing email. A fake mail from google was sent to his account asking him to change his password promptly. The person at the help desk had known that it was a spear-phishing tactic and warned Podesta chief of staff to change his password, but due to a typo error (saying it was a legitimate email), he wanted to write that it was an illegitimate email. Moreover, the person who changed his email clicked on the shortened phishing URL that led to his account being hacked by Russian hackers. His emails were leaked starting November of the presidential election.

A lot of these phishing attacks were successful because weakness was found in end-users. Thus, it makes humans the weakest link in the security chain.

5.3 Humans Vulnerability to Phishing That Led to Identity Theft

Experiments have investigated the connection between socioeconomics, e.g., age and sexual orientation, and weakness to phishing assaults. It is observed that ladies are more powerless against Phishing than men and that clients in the 18-25 age bunch were bound to succumb to Phishing than clients of different ages [12].

5.3.1 Psychological Variables

To look for establishments of the premium to open conceivably harming messages, [13] noticed the variety of purposes to take part in such conduct is explicit among men and women. Ladies are captivated to open messages showing up from interpersonal organizations, while men succumb to messages imparting influence, cash, and sex.

Further assessing the social-mental impacts, backup ways add influence to effective social designing assaults by affecting a casualty's feelings towards dread or hunger, which might adjust a capable activity. Also, in conclusion, impacting methods depend on fringe ways to influence that impact conduct and activity [8].

The recognized philological parts in a phishing assault are:

- Moment delight (ease freedom to save or procure cash)
- Notoriety (the assault depends on the standing of an organization to mislead beneficiaries)
- Unwanted outcomes (the victims are cautioned that their record will be obliterated if they do not do what is inquired) [10]

5.4 Vulnerabilities of System/ Tools

If we talk about Security at Airports a decade back. The technology at that time was not that advance. The Airport Security staff were the only ones present that checked the passports and documents of the passengers. These said teams were on duty for long periods, which led to exhaustion. An exhausted human can make errors. Due to fatigue, it was possible to miss some fake passports. This allowed people to use someone's else Identity to board the plane and fly. With how advanced our system has become; it is still possible to trick the systems.

Utilizing AI to separate among great and terrible IDs is very productive. In any case, without oversight, the rationale created by the calculation might prohibit IDs that are not fake. There are many reasons why an ID may not pass despite being substantial: mileage, other actual harm, fabricating blunders or imperfections, minor plan changes, or even varieties underway relying upon where and how the card was delivered.

A PC should be instructed that IDs that are worn or harmed are as yet legitimate. Getting to a program that permits the assortment of functional and execution measurements for the product helps work on the acknowledgment and validation of reports upheld by the record library of the supplier.

5.4.1 Vulnerability in SolarWinds

In December of 2020, SolarWinds software faced a supply chain attack. FireEye first reported this attack on December 8 and then by the US treachery on December 13. These departments used SolarWinds software. These attacks were performed by an attack group APT29 (Cozy Bear/ Russian SVR)[11]. According to the organization, an intern had chosen a weak password, "SolarWinds123," which caused this attack [15].

The malware was conveyed as a feature of an update from SolarWinds' servers and was carefully endorsed by a substantially advanced declaration bearing their name.

This exceptionally modern identity-based inventory network assault was executed by employing an "indirect access" into a SolarWinds update server, probably supported by secret word splashing.

The assailants could sidestep multifaceted confirmation and move alongside the organization, acting like ordinary clients.

Data from those frameworks and malware left behind by the programmers will probably be utilized for follow-on assaults, including account takeover.

Given the designated, careful nature of this assault, no single security arrangement might have forestalled it. Nonetheless, witness declarations during the Senate hearing featured the significance of character and secret phrase security.

The strategies these assailants used to sidestep multifaceted validation were refined. Nonetheless, lawbreakers have numerous techniques for avoiding MFA available to them, including SIM-trading, social engineering, addressing security questions utilizing uncovered PII, and scanning other taken records for TOTP seeds.

MFA is a layer of assurance – a significant initial step –, yet extra layers are needed to defend the characters of the workers, shoppers, and providers signing into your frameworks. If a client signs in with legitimate accreditations (also known as record takeover), the association has no real way to decide whether the client is a criminal because the login doesn't 'trip a sensor.'

With a north of 18,000 conceivably impacted clients, the extent of the SolarWinds assault is phenomenal. Senate declarations stressed that more casualties would arise over the long haul, and we can hope to see follow-on assaults. Other danger entertainers might take advantage of a similar injector instrument, SUNSPOT, to think twice about advancement processes later [11].

6. Combining AI with the Existing Tools

With the advancement in technology, organizations have made profound changes in their Software. Many different companies have incorporated AI or IoT in their current Software. Simulated intelligence will be turning out to be more crucial for handling digital dangers in the space of network protection: reality, the market is projected to extend. Simultaneously, the utilization of AI is not without risks: more than 60% of AI organizations perceive that AI makes the main online protection concern. Being a universally helpful, double reason innovation, artificial intelligence can be both a help and a curse for network protection [16].

Personality records, like driver's licenses and identifications, are checked to test different components of an ID, either on-premises or from a distance with cell phones. A few verification tests include affirmation of accurate microprint text and security strings, approval of uncommon paper and ink, examination among OCR and scanner tags and attractive strips, information legitimacy tests, and biometrics or facial acknowledgment to interface the person to the ID qualification.

6.1 Utilizing AI

The archive makes a more effective and exact cycle than depending on an undeveloped human. These arrangements ought to contain an unknown interior information assortment system fit for putting away data about the activity and execution of the product. Then, at that point, the information is naturally sent to the supplier consistently. This cycle—whenever mechanized—saves time and works on the nature of the outcomes. Information mining, semi-regulated learning, and relapse investigation in the input circle [17].

There are different models of ID validation to look over:

- Information Mining
  We are examining enormous data sets to transform crude information into valuable data. For more proficiency,

make sure to separate clean information to save time with this cycle.

- Semi-Regulated Picking Up
  Relying on totally computerized AI can bring about "coming up short" reports for things that have encountered mileage or ones with record-producing blunders.
- Relapse Examination
  This strategy persistently tests and breaks down the results to work on the calculation. This interaction is frequently called the criticism circle. As new information is taken into the analysis, the input circle tests predict and improve the results.
- Authenticity Checks
  Computer-based intelligence and AI models ensure that the report submitted for confirmation is real/legitimate.
- Arrangement Identification
  AI-based arrangements can distinguish the specific configuration of the archives. For example, Shufti Pro can confirm records from 3000+ archive formats from 230 nations and domains in 150+ dialects.
- Verifying MRZ code
  Artificial intelligence takes a look at the validness of the machine-coherent zone (MRZ) code by assessing if this field has been altered or altered inside the report. After guaranteeing the report's legitimacy, it disentangles the MRZ and matches it against the data on the record.
- Distinguishing Folded/Collapsed Edges
  As the archives are made of paper, hence they are inclined to mileage. AI-based intelligence, the framework performs checks to recognize collapsed/folded edges on the archive that may influence their genuineness.
- Recognizing Indications of Treating/Fabrication/Photoshop
  After preparing the exact information, AI models can precisely recognize any indications of fabrication regardless of whether it is a minor change in a solitary pixel. These sorts of manufactured records are hard to recognize with the bare natural eye.
- Affirming Multi-Dimensional Images/Rainbow Prints
  Officially sanctioned character archives contain explicit 3D images and rainbow prints. AI-based record check arrangements can distinguish any change or treat in these 3D images and rainbow prints.
- Checking Special Paper and Ink
  Govt-gave ID archives utilize uncommon paper and inks to go up against character fakes. Artificial intelligence can confirm the extraordinary paper and ink on the archives.
- Looking at The Miniature Prints
  Government-provided ID records have microprint as an extra security layer to forestall extortion. The AI checks microprinting for verifying reports.

7. **Proposed Framework** [18]

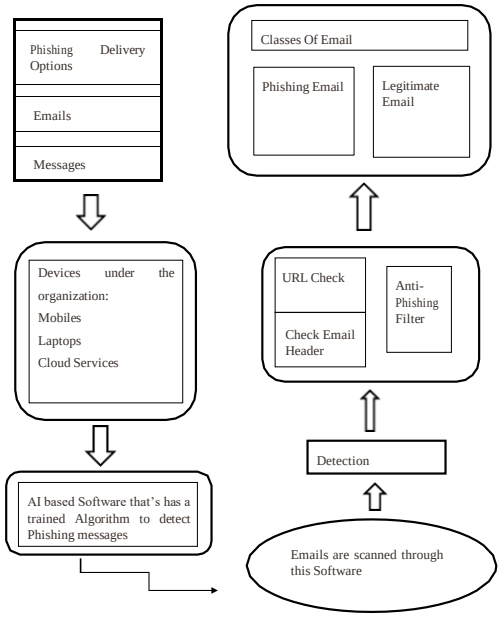

Figure 4. Proposed framework in detecting and preventing from phishing attacks

The proposed framework as shown in figure 4 shows that any suspicious email, messages, or files received by the devices that attached to the organization network will be filtered by AI based software that has a trained algorithm to detect phishing attacks. Any email or messages that detected as phishing further checking need to be done that involve in URL check, checking on email header and anti-phishing filter. Then finally the emails or messages will be classed based on phishing email or legitimate email categories.

8. Conclusion

This paper study Phishing and the different types of Phishing. Identify how Identity Theft is possible through Phishing and a brief description of tools used to detect them. It was seen how devastating it is for a company or an individual if their personal information is stolen through any form of a phishing attack.
Many different types of Softwares are available to help the company or the individuals from Phishing. Suppose the measures, i.e., software put in place to prevent these attacks, have a vulnerability that might have catastrophic destruction towards the company's daily operations. In that case, need to make use of AI-based Softwares to detect these attacks as well. If these types of attacks happen, it is indispensable to ensure that the organization has an adequately maintained business continuity and disaster plan. Proper training of employees is essential, so the employees know what to do and who to report in case these attacks occur. Along with adequate training, security measures should also be present in the company to avoid these attacks.

References

[1] Upadhyay, I. (2020). 20 Important Types of Cyber Crimes To Know in 2021. https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/

[2] Doke, T., Khismatrao, P., Jambhale, V., & Marathe, N. (2020). Phishing-Inspector: Detection & Prevention of Phishing Websites. ITM Web of Conferences, 32, 03004. https://doi.org/10.1051/itmconf/20203203004

[3] Prabadevi, B., Jeyanthi, N., Udzir, N. I., & Nagamalai, D. (2019). Lattice structural analysis on sniffing to denial of service attacks. International Journal of Computer Networks and Communications, 11(4), 101–119. https://doi.org/10.5121/ijcnc.2019.11406

[4] Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. In Human-centric Computing and Information Sciences (Vol. 10, Issue 1). Springer Berlin Heidelberg. https://doi.org/10.1186/s13673-020-00237-7

[5] PIQUÉ, J. (2021). How to Protect Yourself Against Identity Theft. In Handbook of Zoonoses (p. 229). https://doi.org/10.1016/b978-0-323-04478-3.50056-7

[6] Ferrill, T. (2020). 9 top anti-phishing tools and services | CSO Online. https://www.csoonline.com/article/3575080/9-top-anti-phishing-tools-and-services.html

[7] Contributor, S. (2020). 5 Best Identity Theft Monitoring Services - DNSstuff. https://www.dnsstuff.com/identity-monitoring-services

[8] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

[9] Sophos. (2019). Don't Take the Bait 2 A Sophos Whitepaper.

[10] Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. In ACM Computing Surveys (Vol. 54, Issue 8). https://doi.org/10.1145/3469886

[11] Winder, D. (2020). Google Confirms New AI Tool Scans 300 Billion Gmail Attachments Every Week. https://www.forbes.com/sites/daveywinder/2020/02/28/google-confirms-new-ai-tool-scans-300-billion-gmail-attachments-every-week/?sh=4af0fc1a3edd

[12] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security. https://doi.org/10.1145/1572532.1572536

[13] Steve Ragan, & Writer, S. (2013). Social engineering: study finds Americans willingly open malicious emails. CSO. https://www.csoonline.com/article/2133877/social-engineering--study-finds-americans-willingly-open-malicious-emails.html

[14] Kisielius, J. (2021). Breaking Down the SolarWinds Supply Chain Attack | SpyCloud Blog. https://spycloud.com/solarwinds-attack-breakdown/

[15] CISOMAG. (2021). solarwinds123: Did a Weak Password Result in SolarWinds Hack? https://cisomag.eccouncil.org/solarwinds123-did-a-weak-password-result-in-solarwinds-hack/

[16] Mohammed, I. A. (2020). NOVATEUR PUBLICATIONS INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]. NNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY, VOLUME 7,(ISSUE 9).

[17] Fighting identity fraud with AI-enabled ID document verification. (n.d.). Retrieved November 11, 2021, from https://shuftipro.com/blog/fighting-identity-fraud-with-ai-enabled-id-document-verification/

[18] Patayo, C. (2021). A Preventive and Detective Model for Phishing Attack in Small and Medium Size Businesses. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3777065