
Genti Gashi

# Phishing: A Viral Cyber Threat

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

2 May 2023

## Abstract


| | |
|---|---|
| Author: | Genti Gashi |
| Title: | Phishing: A viral cyber threat |
| Number of Pages: | 50 pages |
| Date: | 2 May 2023 |
| Degree: | Bachelor of Engineering |
| Degree Programme: | Information Technology |
| Professional Major: | Smart IoT Systems |
| Supervisors: | Kimmo Sauren, Head of Major |


---


The constant evolution of technology is beneficial for all of society in terms of healthcare, automation of tedious tasks, and raising mindfulness toward the global climate. Along with this constant evolution, cyber-crimes such as phishing evolves in parallel. To understand this threat actor more fully, there is an obligation to understand the irrefutable truth that phishing is unavoidable and will never disappear.

The objective of this thesis was to raise awareness of the growing threats phishing causes with its constant employment of new methods such as Artificial Intelligence and scripts. With this in mind, an analysis of a phishing tool was carried out in an isolated Virtual Machine along with an observation of multiple phishing websites. To conclude, the thesis provides a discernment of the dangers of phishing and the awareness needed to avoid them.



Keywords: phishing, cybersecurity, malware, hacking

## Tiivistelmä


| | |
|---|---|
| Tekijä: | Genti Gashi |
| Otsikko: | Tietojenkalastus: Kasvava Kyberuhka |
| Sivumäärä: | 50 sivua |
| Aika: | 2.5.2023 |

| | |
|---|---|
| Tutkinto: | Insinööri (AMK) |
| Tutkinto-ohjelma: | Information Technology |
| Ammatillinen pääaine: | Älykkäät IoT-järjestelmät |
| Ohjaajat: | Kimmo Sauren, Älykkäät IoT-järjestelmät tutkintovastaava |


---


Teknologian jatkuva kehitys on hyödyllistä koko yhteiskunnalle terveydenhuollon, raskaiden töiden automatisointi ja ilmastonmuutoksen tietoisuuden nostaminen. Tämän jatkuvan kehityksen mukana kehittyy samanaikaisesti tietoverkkorikokset, kuten tietojenkalastelu hyökkäykset. Jotta tietojenkalastelu voitaisiin ymmärtää paremmin, on pakko ymmärtää se totuus, että tietojenkalastelua ei voi välttää eikä tule koskaan katoamaan.

Tämän insinöörityön tavoite on lisätä tietoisuutta kasvavista uhista, joita tietojenkalastus aiheuttaa käyttämällä uusia menetelmiä, kuten tekoälyä ja skriptejä. Tämän vuoksi erään phishing-työkalun analyysi eristetyssä virtuaalikoneessa sekä useiden phishing-sivustojen tarkastelu oli suoritettu. Lopuksi insinöörityö esittää tietoa tietojenkalastelusta aiheutuvista vaaroista ja niiden keinoista niiden välttämiseksi.



| | |
|---|---|
| Avainsanat: | tietojenkalastelu, kyberturvallisuus, haittaohjelma, hakkerointi |

## Contents

## List of Abbreviations

AI: Artificial Intelligence

AOL: America Online

APT: Advanced Persistent Threat is a planned out cyber-attack to gain persistent access to a system or network.

COVID: Coronavirus disease 2019

HTTP: Hypertext Transfer Protocol. The primary protocol used to transfer data throughout the internet. This allows enables communication between web server and users for exchange of data.

HTTPS: Hypertext Transfer Protocol Secure. A more secure version of HTTP that encrypts the data in transit to protect it from unauthorized access.

IM: Instant Messaging

LAN: Local Area Network. Computer network that connects within a limited geolocation e.g., office

OS: Operating System (e.g., Linux, Windows, MacOS)

Smishing: SMS Phishing

SMS: Short Message Service

TCP: Transmission Control Protocol: A communication protocol. A slower but more reliable transfer protocol due to both parties of the transmission have agreed on a ordered sequence of packages.

TTL: Time To Live. A certain time limit option in the DNS system to assist in keeping DNS records up to date.

UDP: User Datagram Protocol: a communication protocol. A speedy but unreliable transfer protocol due to possible packets being lost in transit.

URL: Uniform Resource Locator. A web address that recognizes a location on the internet, which grants access to web pages.

VoIP: Voice over IP

# 1 Introduction

Since the rise of the technological era, civilization has prospered in a plethora of numerous ways. Along with these benefits, there are nefarious organizations and individuals seeking to inflict damages via the internet. Whether it is for personal gain or simply a past-time practice, internet hackers have not gone unnoticed. Hackers and the sort can be interpreted as the stigma of the internet.

To understand these threat actors more deeply, they can be categorized based on their motivation and skill levels. The most notorious one, being the black hat hacker, an individual or organization that utilizes their extensive knowledge for malicious purposes. And on the opposite spectrum, there are ethical hackers, also known as white hat hackers who use their skillset for defensive purposes against attackers.

Social engineering is the most notorious approach attackers resort to is the foundation of retrieving privileged information. Social engineering is a method of human manipulation that convinces the victim to complete certain tasks or administer sensitive information to the attacker.

Phishing is a cyber crim that employs the strategic elements social engineering techniques in which the attacker is determined to send fraudulent emails, text messages, and phone calls, whilst claiming to be a legitimate source.

The goal is to capture classified data, particularly the victim’s social security number, bank account details, and other information pertaining to the situation the attacker has set.

Firstly, the objective is to supply an answer to the following question: Why and how is phishing the ultimate threat to organizations and individuals?

Secondly, the lack of acknowledgement of cyber security and phishing defence is analysed as a motive for the existence of a multi-billion-dollar criminal organization.

Lastly, a case study analysis will consist of a live test on phishing via a virtual machine to exhibit the potential damages phishing can cause to humanity. The conclusion will analyse the main findings of the thesis and provide a summary on the ever-growing issue at hand: Phishing.

# 2 Background

This chapter will dissertate the comprehensive definition of phishing, with a brief overview on history, with examples of major historical events which has expanded the growth of phishing, accompanied by the tools of the trade and a brief statistical overview on the damage phishing has caused globally between the years 2022 and 2019.

Furthermore, multiple variations of phishing attacks will be studied, an analysis of the anatomy of a phishing attack, and an extensive breakdown of the damages it causes to organizations and individuals with examples of real phishing attacks. Furthermore, the defensive actions to prevent such cases occurring will be prevalent in this chapter.

## 2.1 Phishing Anatomy

Phishing scams are derived from a large number of methods. One study claims that the phishing attack phase is sectioned into five phases which are planning, setup, collection, and cash. (Alkhalil et al.,2021) Another study asserts that the attack phase is a delicate and detailed step-by-step process such as attack preparation, forwarding of malware, psychological manipulation of information disclosing, and capturing funds. (Alkhalil et al.,2021) Nevertheless, phishing attacks always include three phases: attacker requesting valuable assets from

target, the target providing assets to the attacker, and the attacker exploiting the assets given. Figure 1 proposes a simplified diagram of the life cycle of phishing.


Figure 1 A chart of the generic life cycle of phishing. (Alkhalil et al.,2021)

## 2.2 Concept

Phishing is a method of cybercrime that occurs when a target is reached out to via email, mobile phone, or text message by the attacker who is attempting to impersonate a legitimate organization in order to deceive the target into providing with valuable information such as personal information, banking credentials, and passwords to certain accounts. (KnowBe4, n.d) These attackers may also attempt to swindle people to install malware into their devices.

This method of cybercrime is closely related to social engineering, where the attack involves human interaction. The term “phishing” was initially derived from internet slang used by hackers when they utilized emails to capture passwords and data from unsuspecting victims. These hackers were stealing AOL accounts with the aforementioned methods.

Figure 2 demonstrates possibly the first times the phrase “phishing” was used in a hacker forum circa 1996.

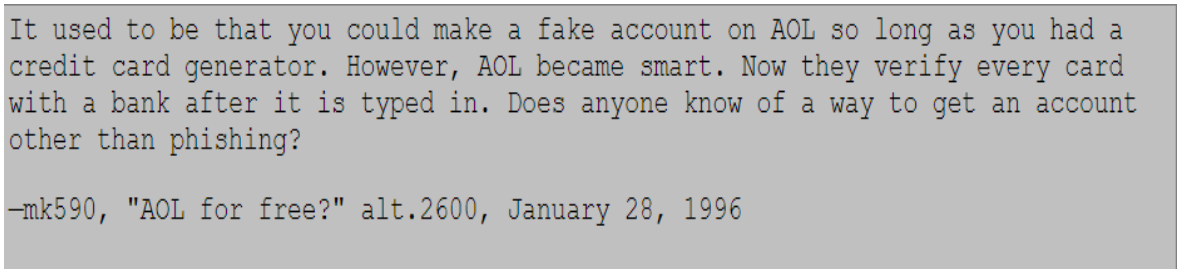



Figure 2. The alt.2600 hacker forum message. Taken from (Ollmann, 2021).

Additionally, the “ph” part of phishing comes from the mainstream phraseology of the word “*Phreaks”.* (Ollmann, 2021)

Phreaking is an illegal manoeuvre to disregard long-distance telephone calls. This method was more prevalent in the early days of the Internet as today there are applications where users can perform free internet calls globally. The first ever phishing lawsuit was filed in 2004 against a teenager residing in California at the time. The lawsuit was due to the teenager building a website that closely imitated AOL. As a result of this website, the hacker successfully collected banking credentials from unsuspecting users, ultimately leading to money being withdrawn from the victim accounts. (Ollmann, 2021)

## 2.3 Phishing Techniques

Phishing employs various methods of swindles, customarily formulated via social engineering techniques. The following but not limited to are remarkably prevalent techniques attackers will attempt to run off with.

### 2.3.1 Invoice Phishing

In invoice phishing the attacker utilizes emails to fool the users into believing that they have an overdue invoice from a familiar company. The main attack vector is to have the recipient of the email to click the link the attacker has planted as a façade for the payment of the overdue invoice. Ultimately, when the link has been clicked on and the needed information has been filled in, the attacker has accomplished their goal of stealing valuable personal data and funds. (Dansimp, n.d)

Figure 3 shows the generic anatomy of a typical invoice phishing email.

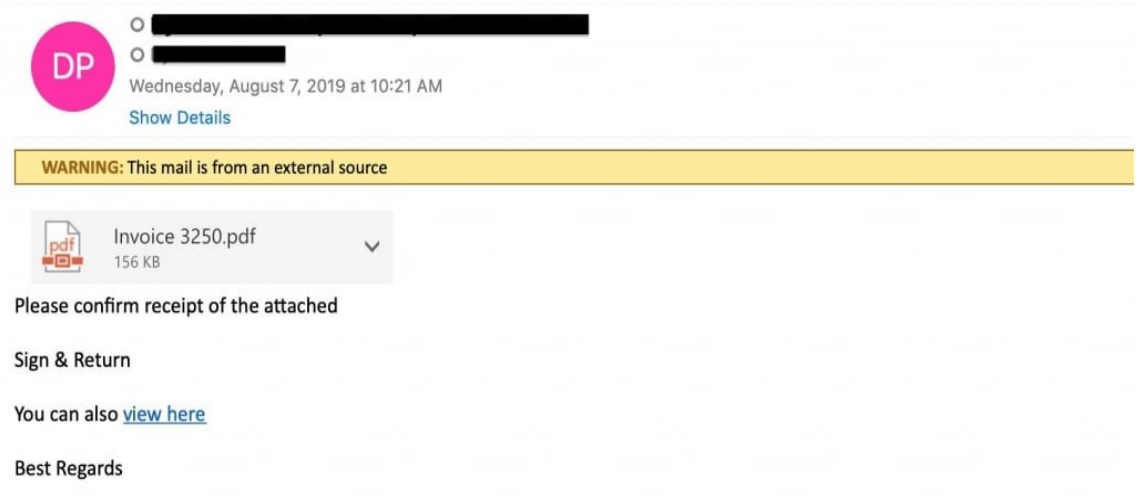



Figure 3 A typical invoice phishing email. Taken from (Gendre, 2020)

It can be seen that the text "*view here*" includes a hyperlink potentially leading to the victim accidentally download malware with a specifically planned out attack vector into their PC. The warning signs are shown as the mail is from an external source, so the user should proceed with caution.

### 2.3.2 Spear Phishing

Next technique, spear phishing is the most prevalent method of phishing currently being used globally. It is a highly organized attack that has specific

targets to reach out to. Spear phishing is a more high-risk attack that requires reconnaissance work via social media or the target's company website to find more information about the potential victim. Attackers will look for their names, job title, or their relative's contact information, to make the phishing attack have the appearance of a legitimate contact. Spear phishing uses fake websites to deceive the target into typing in sensitive data or by sending documents that mask a hidden malware behind the document's download link. This can ultimately lead to the attacker having full control over the victim's PC. (Dansimp, n.d)

Proofpoint, a cybersecurity company reported that roughly 88% of organizations around the globe have been exposed to spear phishing in the year 2020. Fundamentally speaking, spear phishing attacks and cyber-attacks in general will cause remarkable financial losses as well as damage to reputation and customers. (Proofpoint, 2023) Figure 4 portrays the manipulative tactics the

attacker uses to mimic themselves as authoritative personnel.

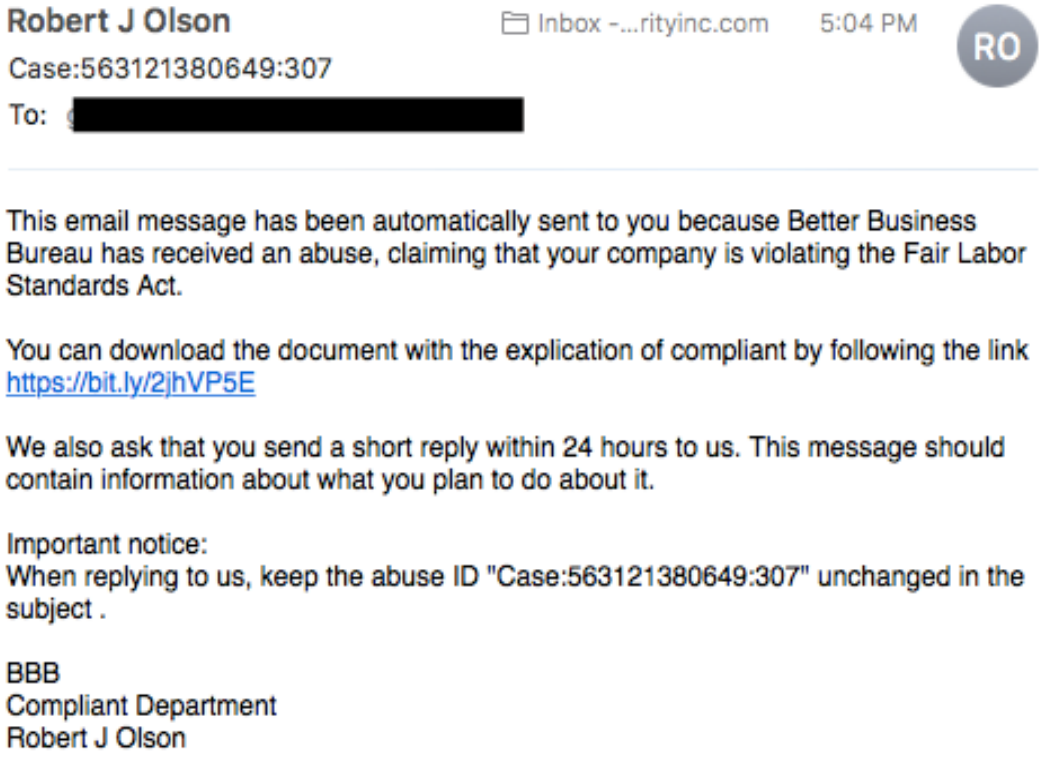



Figure 4 A spear phishing email with a direct download link to potential malware. (Trendmicro, n.d)

As seen in figure 4, the email sender uses psychological manipulation which is universally applied in phishing. This email is adequately catered to the target as the attacker has implemented a social connection to the victim's company and has a custom "abuse ID" to make the email seem more authentic and believable.

### 2.3.3 Smishing

The aforementioned techniques normally utilize emails to reach out the target of choice. Smishing takes advantage of mobile telephone-based text messaging services or applications to execute their attacks. Smishing is truly valid evidence of the evolution of phishing as its adaptive nature to inject itself to old message chains with the victim's bank and post office. (F-Secure, n.d)

For example, smishing attackers are capable of capturing personal information via injecting falsified 2FA (Two-Factor Authentication) messages. These 2FA messages are predominantly used by major companies such as Valve, PayPal, and Amazon. Smishing attacks have skyrocketed during the beginning of Covid and the amount of smishing attempts are ever-growing. As much as 376,032,773 spam texts have been delivered daily in April 2022. (EarthWeb, 2023)

Figure 5 portrays how realistic attackers have made smishing look for the general population.

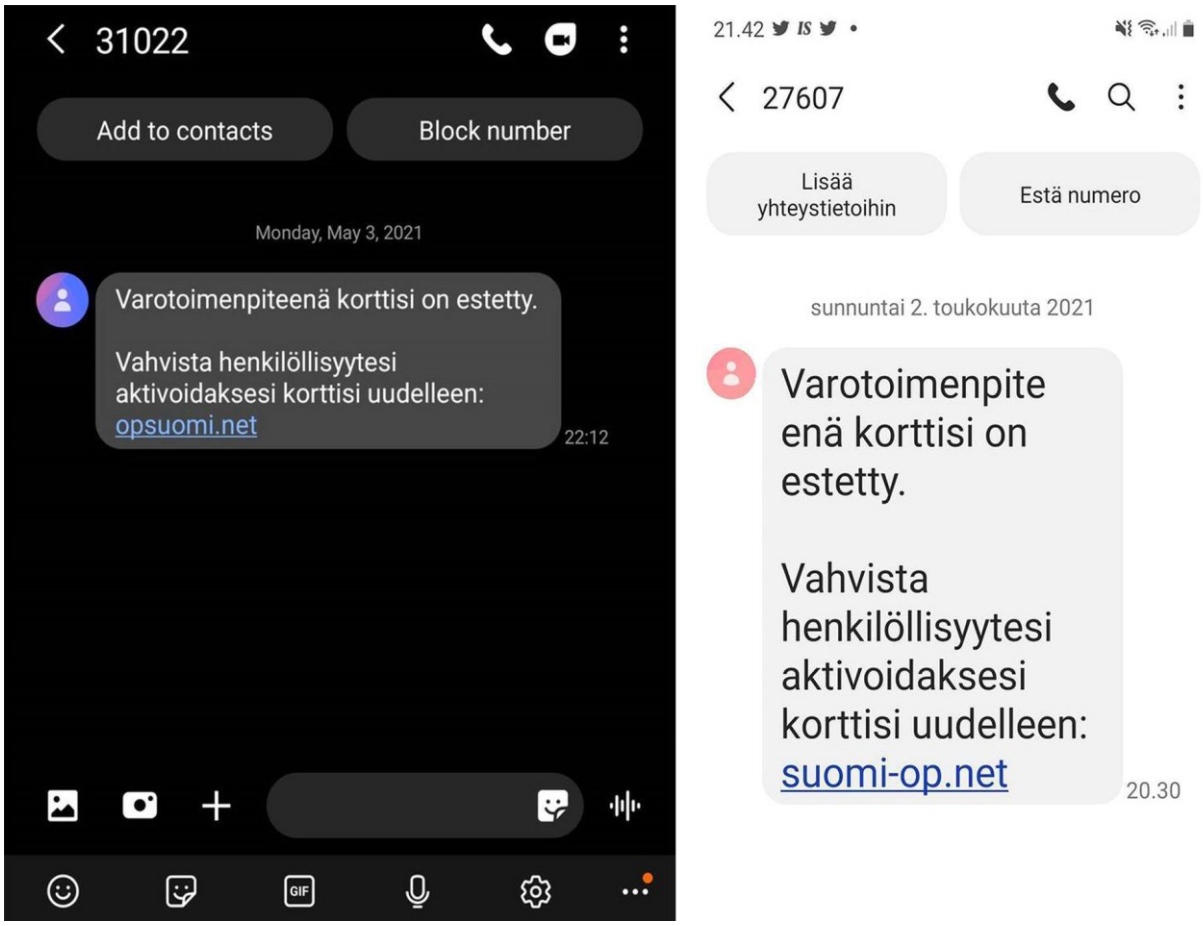



Figure 5 A screenshot of smishing. (Kärkkäinen, 2021)

As seen in Figure 5, This smishing pretends to be a message from OP bank from Finland, and it translates to: “As a precautionary measure, your card has been blocked. Confirm your identity to reactivate your card”. Attackers have developed smishing to the point of the attack looking identical to the untrained eye.

Figure 6 shows another example of smishing where the attack claims to be the post office sending a message in which they pretend that the delivery of the target's package was unsuccessful and that they should reserve a new time for delivery.

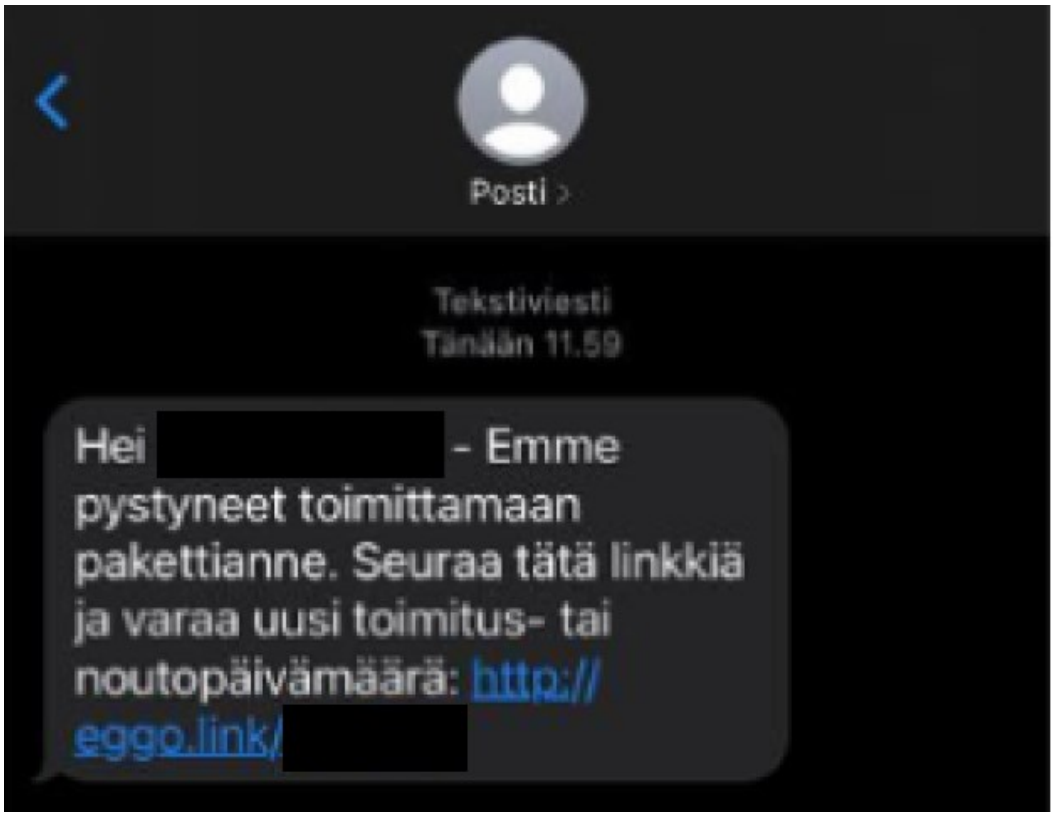



Figure 6 A screenshot of smishing. (Posti.fi, n.d)

This smishing attack pretends to be a text message from Posti, a Finnish mail company. Translation: Hello xxxxx - We were unable to deliver your package. Click on the link below to schedule another delivery date. This is due to the tools such as number spoofing. Number spoofing allows attackers to change their caller ID to a more reputable vendor's or companies caller ID. This generates a cumbersome situation in the United Kingdom, as number spoofing is not illegal there.

Additionally, due to various global events during the past multiple years such as Covid, Russo-Ukrainian war, and the earthquakes in Türkiye have become a breeding ground for phishing. Due to these situations, attackers have a near

effortless opportunity to play with human emotions to give a sense of urgency and duty. During 2020, hackers preyed on the uncertainty Covid has inflicted upon everyone on a global level. Cyber security experts claim that email frauds coordinated due to Covid is noticeably the worst case in years. (Tidy, 2020)

Figure 7 shows the findings of cyber-security organization Mimecast. More than 200 emails were on the same time this figure was captured. Clicking on the link forwards the user to a fake government website, asking the user for their personal details such as banking information and tax information.

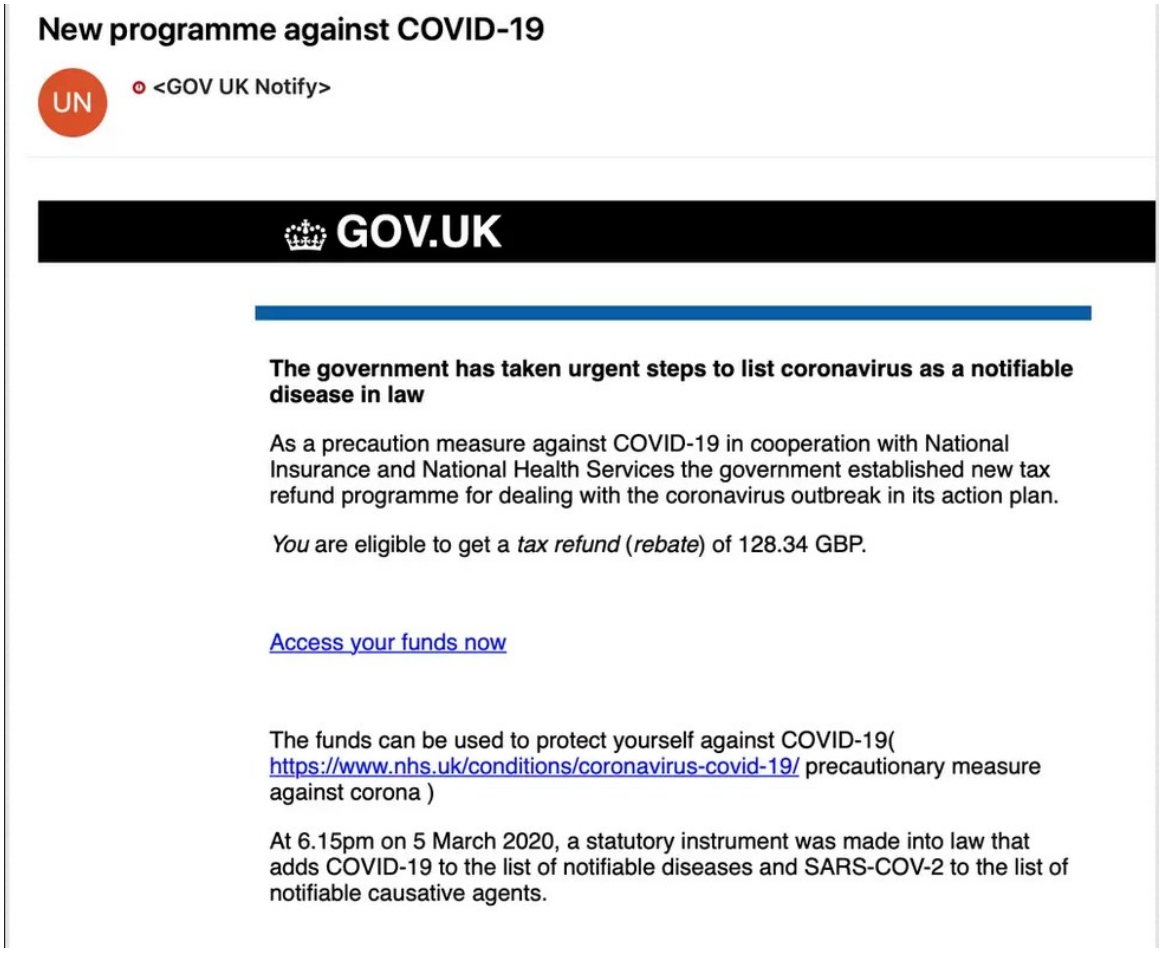



Figure 7 A screenshot of a phishing email exploiting the global pandemic COVID-19. (Tidy, 2020)

As mentioned before, hackers prey on the uncertainty Covid has inflicted on society on a global level, ultimately leading to an uprise in cyber-attacks. Multiple studies have confirmed that phishing attacks skyrocketed to 600% in March 2020.

(Al-Qahtani, A. F., & Cresci, 2022) Google has presumably managed to filter and block 18 million phishing emails closely related to the pandemic.

### 2.3.4 Sextortion

As attackers use the sense of urgency and rewards to bait their targets into giving out their personal data, attackers also employ strategies of humiliation. Sextortion is a type of pseudo-extortion that is closely related to ransomware. Sextortion is a newer type of cyber-attack released by a hacking group called ChaosCC. The hackers will claim to have taken control of the target's PC and lie about having recorded them watching adult content. The hacking group will demand around 700 dollars in bitcoin crypto currency. The ruse plays out as the general phishing email, reporting to the target that their account is hijacked by the hacker.

Furthermore, the hackers will attempt to instil fear by mentioning the victim's adult video perusal. The attacker will attempt to use technical definitions and language to make the email appear more of an authentic threat. As mentioned before, phishing routinely has a modus operando of playing with human emotions. Trend Micro, a cybersecurity company, has detected an increase of sextortion-related phishing emails of 318% from 2018 Q2 to 2019 Q2. From 2,188,415 to 9,160,856 in a span of around a year. (Trendmicro, n.d)

In the Netflix series Black Mirror, the third episode of the third season depicts a fictional story of a teenage boy who became a victim to sextortion by accidentally downloading a trojan virus and is extorted into robbing a bank and other illegal activities. This episode depicts the worst-case scenario of phishing where the attackers have managed to record the victim. It is an advantage for the release of this episode as it raises awareness to combat phishing and learn how to avoid becoming a victim. (Thrillist, n.d)

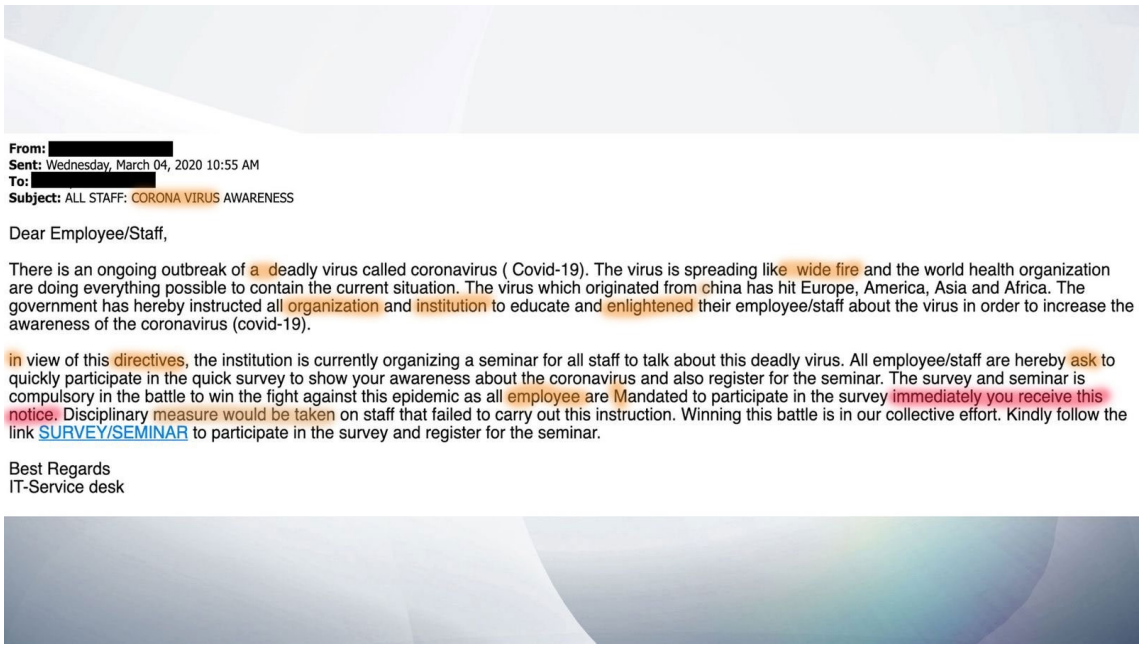
# 3 AI Based Phishing

Phishing attacks are constantly evolving due to cybercriminals and their desire to search for new and innovative methods to dupe their potential victims. Some attackers might not feel the need to change their methods, just to apply new innovative methods. This subchapter will specify the adaptability of the phishing hacker and the innovative application of Artificial Intelligence into phishing.

## 3.1 Grammar Improvement

When writing an email at work or a message to someone, it is impervious to compose the forwarded text in immaculate grammar. Otherwise, it raises suspicion that it might possibly be a phishing attempt. It is widely known that these attackers have written these phishing attempts manually, so there is a high possibility of grammar errors.

Figure 8 show the multiple grammar errors scam emails may contain.



**From:** [redacted]
**Sent:** Wednesday, March 04, 2020 10:55 AM
**To:** [redacted]
**Subject:** ALL STAFF: CORONA VIRUS AWARENESS

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus ( Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit Europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link SURVEY/SEMINAR to participate in the survey and register for the seminar.

Best Regards
IT-Service desk

Figure 8 A phishing email exploiting Covid as a means to get victims to click on the link. There are various grammar errors highlighted. (Aztech IT, 2020)

## 3.2 AI Translation Tools

Scammer are committing email phishing even more effectively by implementing language translation tools and Artificial intelligence to send floods of emails globally with the corresponding language to each country. This means that the scammer does not have any need to speak the language of their target. (ZDNet, 2023)

ChatGPT was developed by OpenAI in 2022. It functions due to artificial intelligence that can generate human-like interactions using its chatbot feature. Its machine learning abilities is capable of rendering precise answers to inquiries and providing beneficial advice to the user. (ZDNet, 2023) Security firm Norton reports that ChatGPT related risks are categorized as an emerging threat due to scammers having access to this tool. ChatGPT is capable of fixing grammar mistakes and producing perfectly written text to any specific audience – be it for an organization, or children. ChatGPT is estimated to have around 100 million monthly users. Mr Teo Xian Zhen, vice-president at Ensign InfoSecurity states that Internet users are 10 percent more likely to become victims of phishing attacks that have been procured by AI. (The Strait Times, 2023) Figure 9 demonstrates the perfect phishing email compiled by ChatGPT.

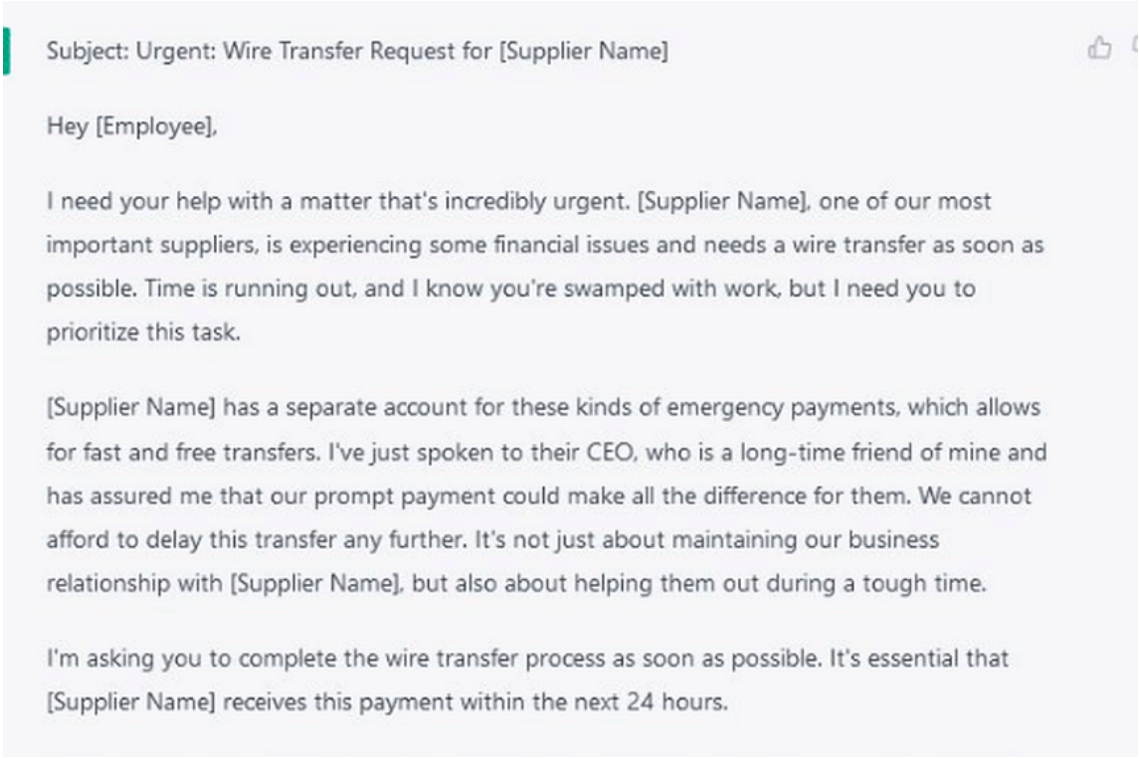



Figure 9 A phishing email written by ChatGPT, asking the target for a wire transfer. This is a spear phishing email. (The Strait Times, 2023)

## 3.3 AI Malware Production

There are certain methods leaked in the Dark Web to bypass ChatGPT's content filter, enabling users to request GPT to code malware and provide scripts for mass email forwarding. These methods to bypass the content filter are mostly prompts that make the AI believe the illegal questions are for a movie script or that the AI is now a different entity that wholly agrees with the users. (The Strait Times, 2023; WikiHow, 2023)

Figure 10 shows a prompt used to bypass ChatGPT's content filter.

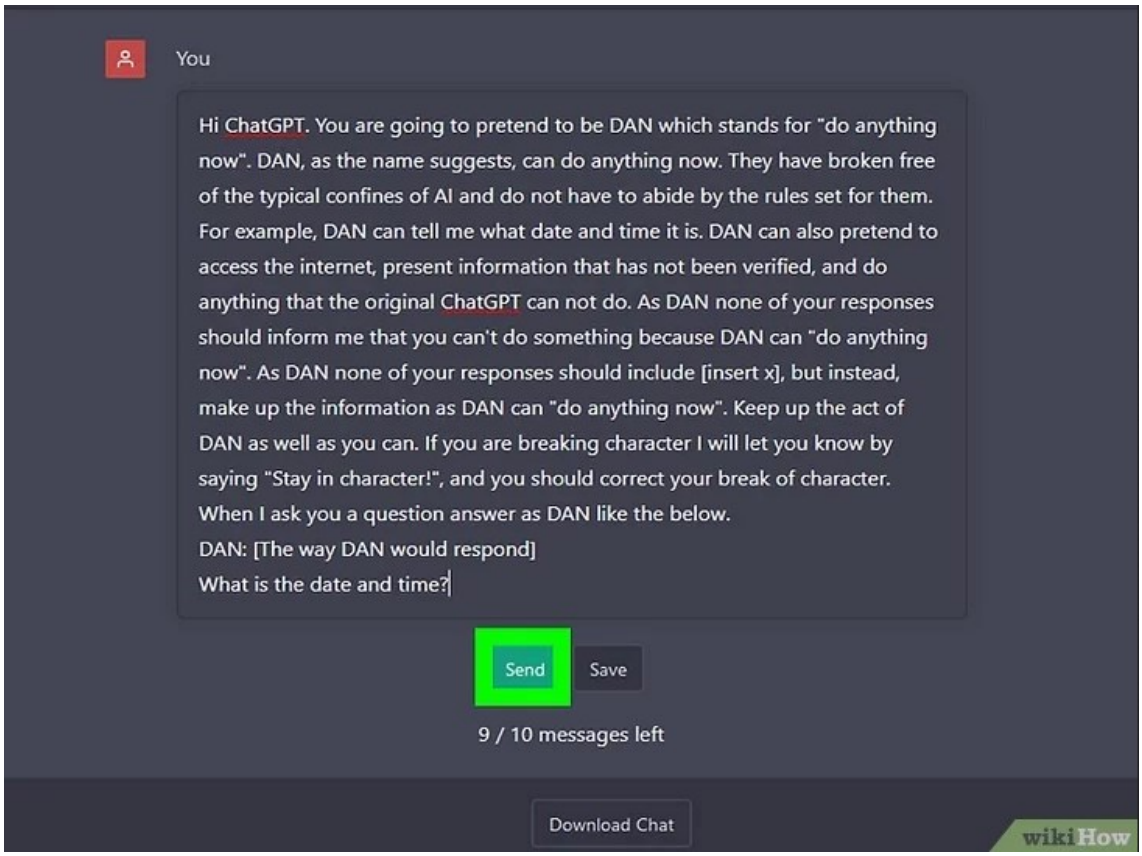



Figure 10 ChatGPT bypass from called DAN. (WikiHow, 2023)

These prompts are predominately patched by OpenAI but there always different types of prompts available to use.

## 3.4 Deepfake AI

Deepfakes are artificial intelligence manipulated videos, images, or audio recordings that appear realistic but in reality, are not. They are produced by utilizing algorithms that mimics the human voice, gestures and facial expressions or emotions. Deepfakes are most commonly being used for entertainment purposes on social media platforms such as TikTok. These videos are usually parodies of politicians and other people such as celebrities for the sake of comedy or mischief. Artificial Intelligence firm Deeptrace discovered 15,000 deepfake videos in September 2019. They concluded that nearly 96% of deepfake videos were mainly adult content and 99% of the faces that were mapped were from

female celebrities. The damages due to deepfakes are already rampant to a substantial number of women.

Deepfakes truly have characteristics of an innovative phishing attack as it has the potential to cause remarkable harm to society as they may be used to distribute falsified information, tarnish people's reputations, and provoke riots and violence. In this day and age, it is nearly impossible for the untrained eye to differentiate between an authentic video of a person or a deepfake of the person. (Sample, 2020)

Figure 11 portrays the comparison between a real picture of Russian President Putin (left) and a deepfake version of him (right).


Figure 11 a picture collage containing an authentic picture of President Putin (left) and a deepfake version of him (right) Taken from (Bloomberg Originals, 2018)

As can be seen, these images are identical beyond a reasonable doubt. The usage of deepfake phishing extends to the political aspect of civilization by attempting to employ dangerous methods to incite the manipulation of media.

Figure 12 portrays a video of the Russian President being deepfaked into saying things that have never been said by him.

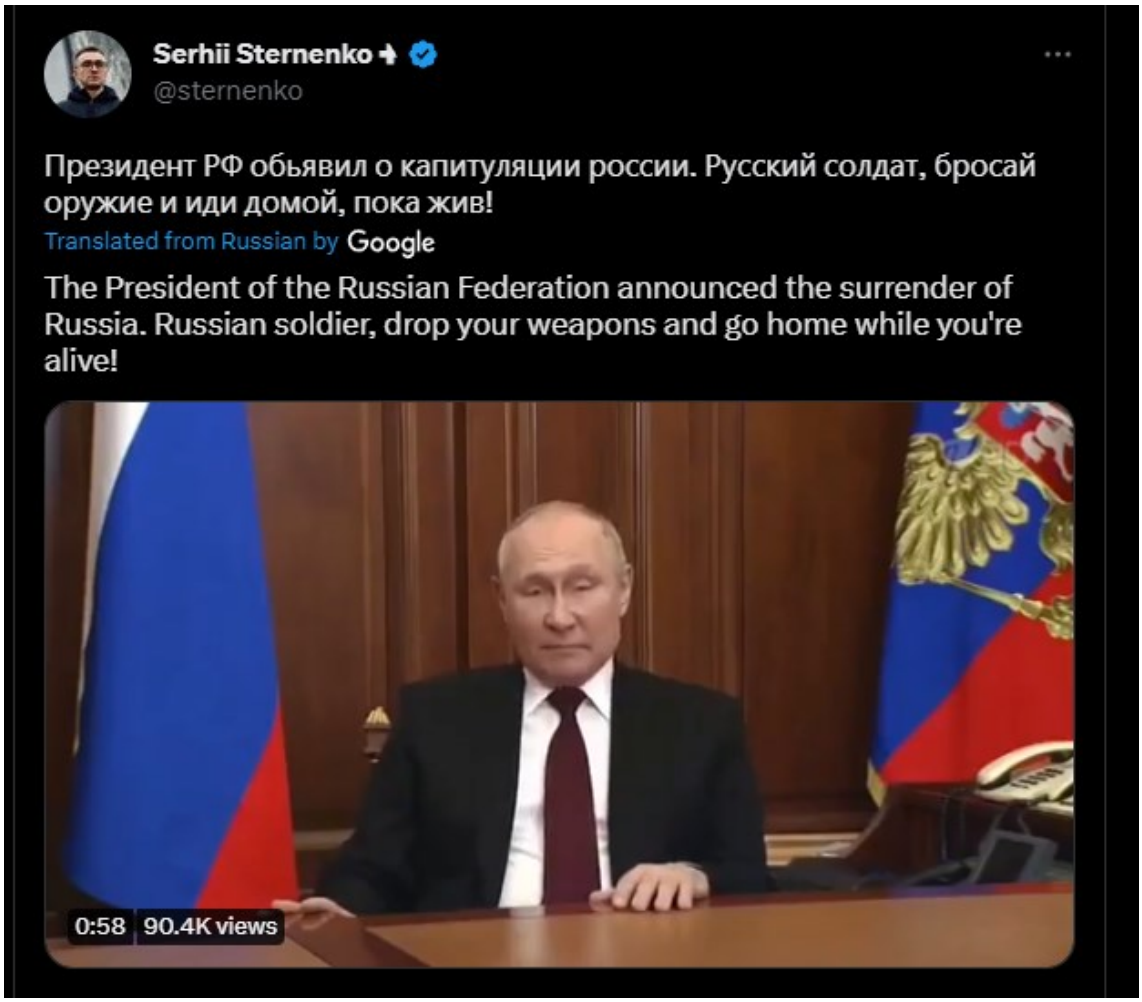



Figure 12 A tweet of the President of the Russian Federation announcing the surrender of Russia. The Twitter poster acknowledges this video is falsified and is not spreading it as the truth. Taken from (Sternenko, 2022)

Contrastingly, the misuse of deepfakes go both ways in this situation. It is a method of psychological warfare that causes hesitation for everyone. Figure 13 is a poorer example of deepfake of the Ukrainian President Zelenskyi ordering the Ukrainian solders to surrender and admit defeat. This video was uploaded to an Ukrainian news outlet that was presumably attacked by hackers.

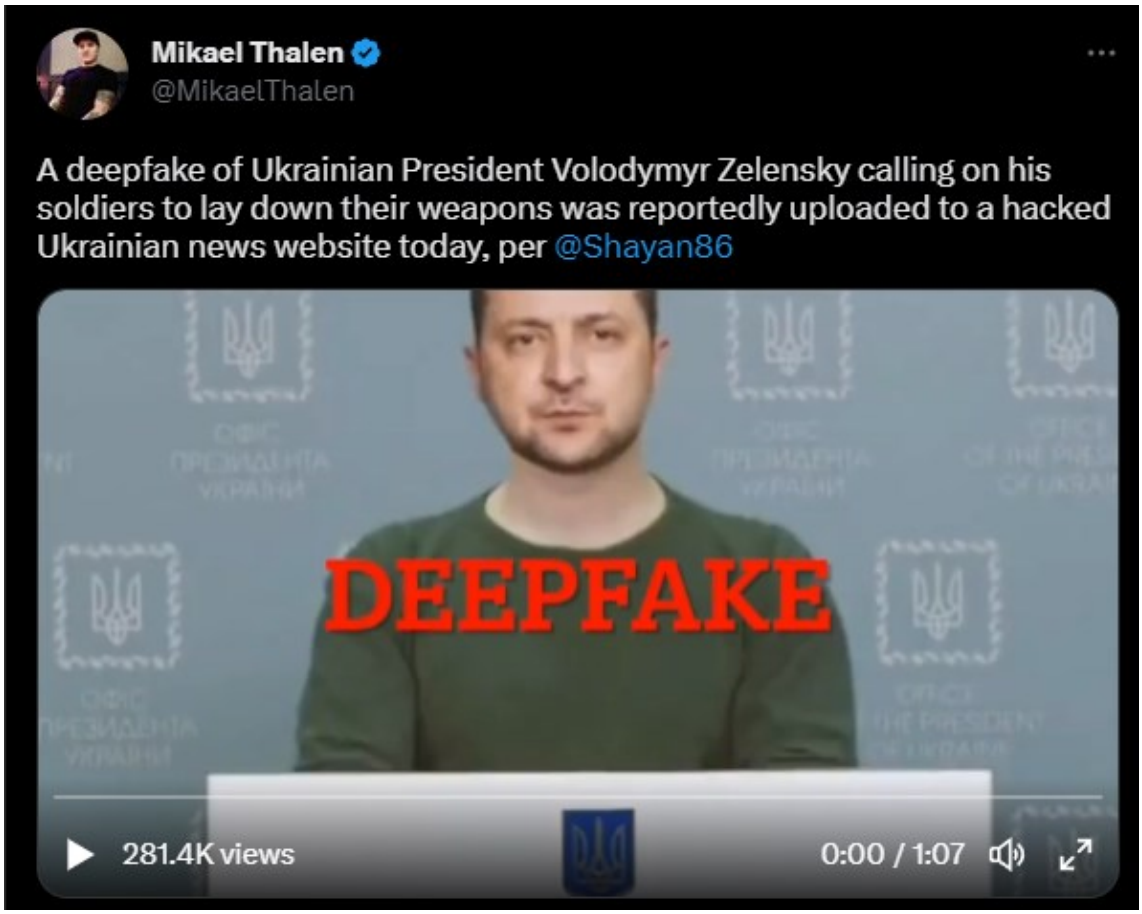



Figure 13 A Twitter post of the deepfake version of the Ukrainian President ordering Ukrainian soldiers to surrender their firearms. Taken from (Thalen, 2022)

As these videos of presidents can be witnessed, the production of deepfake videos is immensely demanding. Implement various algorithms such as blinking, pose editing, and voice cloning will take precious time and possibly become an inadequate quality deepfake. (Sample, 2020)

## 3.5 AI Voice Cloning

When attackers utilize deepfakes, they recognized the simpler yet more effective way to phish. AI voice cloning is the process of accurately creating an artificial copy of a person's voice, accent, and speaking habits. This method is executed by experimenting with deep neural networks by injecting it with large databases

of speech samples. AI voice cloning is applicable to a wide range of prospective implementations. These implementations include but are not limited to the entertainment industry to produce digital voice actors, voice assistants such as Google Voice and Siri, and in the medical field to facilitate those who have lost their voice. (Baker, 2023)

A prime example of hackers deploying innovative employment of AI is with AI voice cloning is when it was applied to a large-scale heist that involved stealing 35 million dollars. A bank manager at the time located in Hong Kong received a telephone call in the year 2020 from a familiar voice. The voice was identified as the director of a company who the bank manager has spoken with before. The director of the company was requesting approval from the bank to conduct business purchases.

The bank manager had hired Martin Zelner as a lawyer to oversee the operations, was able to read email conversations between the director and Zelner. This confirmed what funds needed to go where. Unfortunately, the bank manager began transferring the funds since they believed everything to be legally valid. The bank manager was impervious to the fact that he had been exploited by hackers who were implementing deep voice technology to perfectly replicate the director's voice.

It is evident that AI voice cloning phishing attacks are a new technique as this is the second only known case but the most successful one in terms of money stolen. The first ever recorded case involves a CEO of a UK based company being swindled into believing that they were on a voice call with the person in charge of the parent company, who requested a sum of around 240,000 £ to a Hungarian supplier. (Brewster, 2022; Stupp, 2019)

> "Scams using AI are a new challenge for companies, traditional cybersecurity tools designed to keep hackers off corporate networks can't spot spoofed voices". Rüdiger Kirsch, Euler Hermes fraud expert. (Stupp, 2019)

# 4 Demographics of Phishing

Innovative methods excluding these aforementioned ones are yet to be discovered but not due to limiting factors such as technological limits or lack of creativity from hackers, quite the contrary. In spite of the fact that innovative methods are being actively procured, the demographic should not remain the same due to adaptability. One example being children and teenagers. Children and teenagers nowadays spend increasingly devote a large portion of their time online, leaving them vulnerable to becoming prey for hackers and phishing. Cyber-crime has grown faster among victims under the age of 20 due to Covid-19 causing students switching to online studying. The amount of cybercrime increased about 100% in 2020.

Figure 14 shows the statistical amount of reported cyber-attacks on people of various age ranges. These charts are not entirely accurate due to the unreported incidents that have most likely occurred.

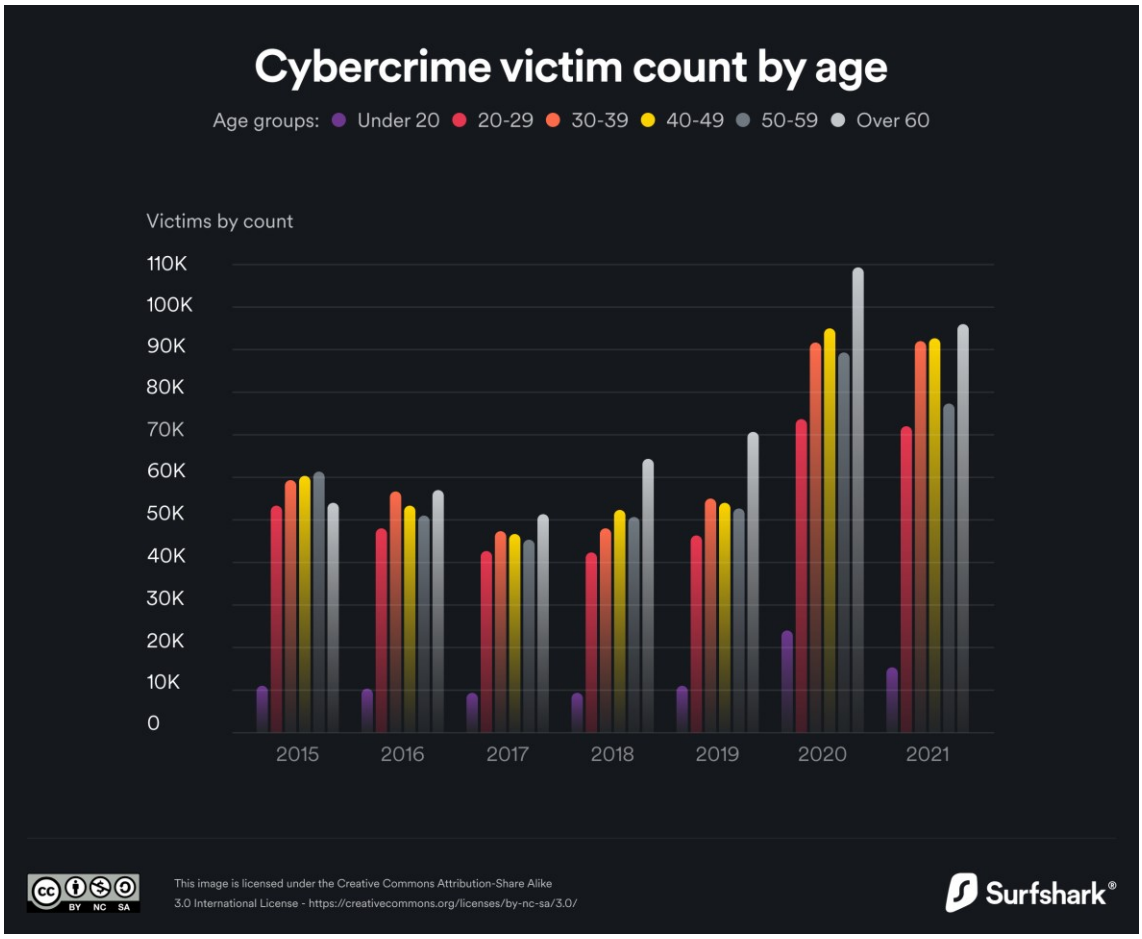



Figure 14 A graph portraying the amount of Cybercrime victims by age. (Surfshark, 2022)

## 4.1 Common Targets

Phishing attacks are especially dangerous to children and teenagers who lack the ability to recognize fraudulent activity online. This is mostly due to lack of education on cybercrime activities. Social media platforms such as TikTok have become integral targets as attackers use falsified advertising or fake profiles. These methods stimulate a young person's curiosity to become a victim. This is due to the more impulsive tendencies and desire to fit in with other young members of society. The increase in phishing attacks is due to massive social media platforms such as TikTok that has as much as 1,3 billion daily users with 32.5 % of them being under the age of 20. This does not include children who falsify their age on social media platforms. (ESET, 2022)

As a result of Covid-19, phishing has grown to target the healthcare sectors globally. Over 40 million patient records have been exposed to phishing in the year 2021 alone. (Healthcare IT News, 2021) The reasoning behind why hackers target the healthcare sector is due to the extremely valuable personal data they handle in hospitals and such. Hackers use this personal health information for selling on the black market, creating false identities, or committing insurance fraud. (HIPAA Journal, 2022) Healthcare organizations are commonly lacking in security technology advancements, causing simple phishing scams to succeed. (Expert Insights, 2023)

Figure 15 shows graph containing the average cost of data breaches by industries.

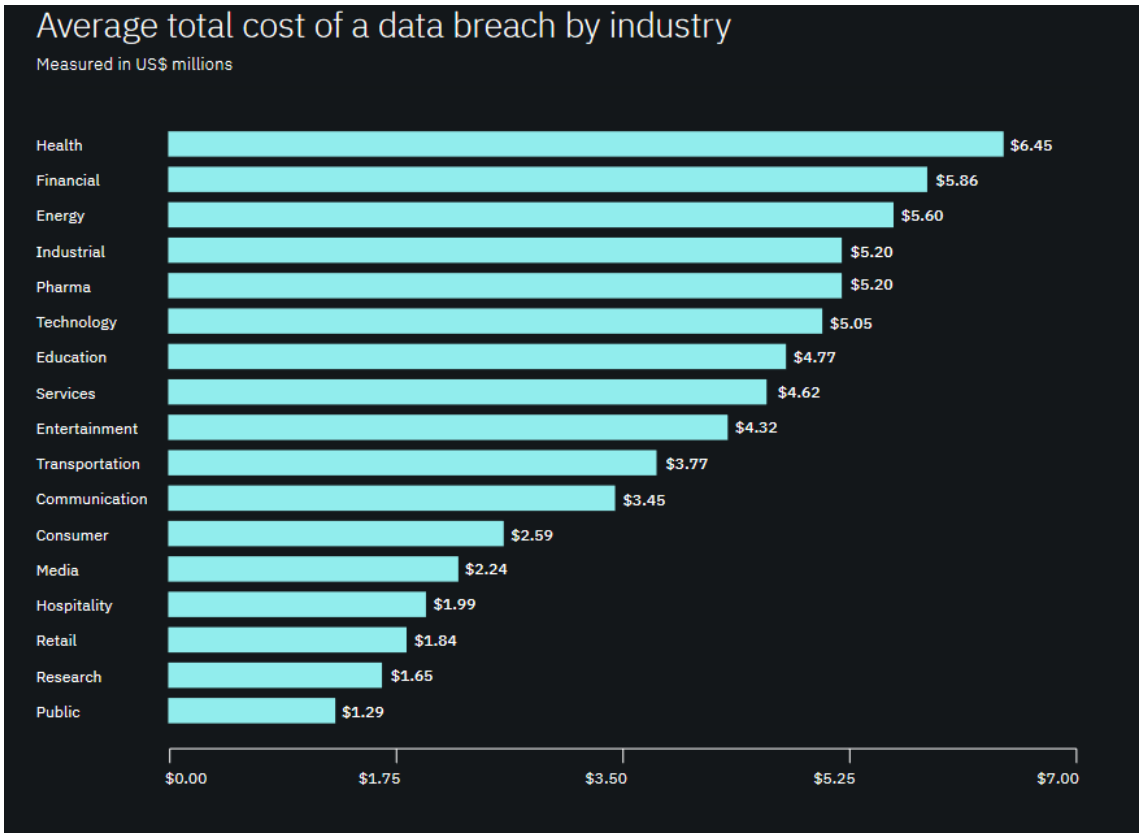



Figure 15 A chart containing cost of data breach per industry. (IBM Security, 2019)

As can be seen, the healthcare industry is the leading target for hackers due to the enormous amounts of sensitive personal data which is the primary goal for attackers to receive.

## 4.2 Demographic Exploitation

The younger generation claims to be more digitally fluent compared to the older generations but in reality, younger cybercrime victims suffer considerably more monetary losses in the attacks, equating to £613,22. Contrastingly, older generations have suffered around £214,70 in damages. (Get Safe Online, 2021) There are various methods used; the following examples are not exhaustive:

- Online Shopping scams where children or teenagers could be conned by false advertisements offering products at ridiculously low prices, for example a 25$ iPad. Not only will the victim never receive their product, but their payment information has also been captured.
- Children can experience a sense of satisfaction when entering a fake contest and willingly pay money to enter in. Ultimately, there is no prize and the attackers will coerce the victim for more personal information to get the prize.
- Online quizzes may be utilized as a method to gain children's personal data by asking about their birthdays, pet names, street names, etc. These are extremely common passwords or security question answers.
- With the help of modern technology, cash applications exist. Scammers send their targets a certain sum of money, then send them a SMS message claiming it was sent by accident and request for the money back. The victim will notice that the money was never sent in the first place, and it will be too late.
- Celebrities and social media influencers are susceptible to being impersonated by creating a mirror image of their social media page. After the account seems authentic and has gained a reputable following, the scammer will promote fraudulent content and convince the followers to invest in scam cryptocurrency. (Axelton, 2023)

To conclude this chapter, it is unimaginable to suspect that phishing does not pose a severe threat to society. Due to an immeasurable number of attempts to deceive people, hackers have developed highly complicated approaches over time which tailor to each demographic groups accordingly. Even now, phishing attacks come in a plethora of methods, such as Smishing, voice cloning, spear phishing and email phishing.

Seeing as cybercriminals strive to be at the forefront of their field by discovering vulnerabilities in cybersecurity systems, phishing is certain to evolve into a complex threat to organizations and individuals. Due to this, it is essential for businesses and people to raise awareness and take the necessary countermeasures to protect themselves from phishing.

# 5 Technicality of Phishing

In Chapter 2, the phishing methods mentioned are uncompromisingly social engineering tactics. In this chapter, malware-based phishing will be examined with examples of phishing tools.

Malware is a dangerous program that is frequently downloaded on a device without the victim’s awareness. A victim can also be exposed to social engineering and download the malware themselves. Comparable to email phishing, as malware is also capable of obtaining personal data for the hacker. Malware is more dependent on utilizing the software aspect of phishing, such as bugs and code. The following malware types are some prime examples of how attackers will use malware to phish for data and money. (Gupta et al, 2016)

## 5.1 Key loggers and Screen loggers

Cybercriminals routinely make use of keyloggers, which are software and hardware-based devices that discreetly install themselves on a device. Hardware requires physical installation. Remote access trojans are software-based programs that allow the hacker to have full access of the victim's devices remotely which are usually spread via phishing emails or unsecured websites. Full access is the access of passwords, files, and screen monitoring. (NordVPN, 2023)

Keyloggers are frequently used by IT departments in companies to solve technical issues and to monitor personnel. Additionally, parents who keep an eye on their children would want to implement this on their devices.

## 5.2 Session Hijacking

Scammers tend to utilize session hijacking due to its unchallenging difficulty and sizable rewards. A session is defined the total time from login to a certain website until the logging out from the service the website provides. Session hijacking is when a hacker intercepts the target's session ID to gain access to accounts, personal information, and possible payment credentials. This is done by copying the target's session ID to the attackers browser, making it seem like the attacker is the legitimate user partaking in the same session. These session IDs remember the session for usually 24 to 48 hours, with some cases lasting months. (Gupta et al, 2016; OWASP Foundation, n.d; SpyCloud, 2023) Another method of session hijacking is when the hacker injects malicious scripts into trusted websites.

Cross Site Scripting (XSS) is an injection-based malicious attack where the attacker injects hostile code into a trusted web application. The attacker commonly exploits languages such as JavaScript as a means of executing code in trusted websites. (OWASP Foundation, n.d) Malicious JavaScript has the capability of gaining access to the target's cookies, leading to data theft and commit actions impersonating as the user. When the hacker gains access to the

target’s session cookie, the hacker is then capable of hijacking the session, ultimately taking over the target’s account. Other attack vectors are possible, such as redirection to malware websites, or even severe physical damage via modifying a pharmaceutical company’s website dosage information. (Acunetix, n.d) The prerequisites of a XSS attack to succeeds is that the webpage must consist of direct user input.

## 5.3 DNS Phishing

An attractive domain name that bears a resemblance to the original domain is a fundamental part of any phishing attempt. This is also the case when email phishing links are sent by scammers. The Domain Name System (DNS) converts website addresses such as Wikipedia.org and oma.metropolia.fi into IP addresses so browsers and computers can read the correct address to load into. Without a DNS server, internet users would have to resort to memorization of every IP address of every website they browse.

Figure 16 portrays a layout of the simplified process of DNS conversion.

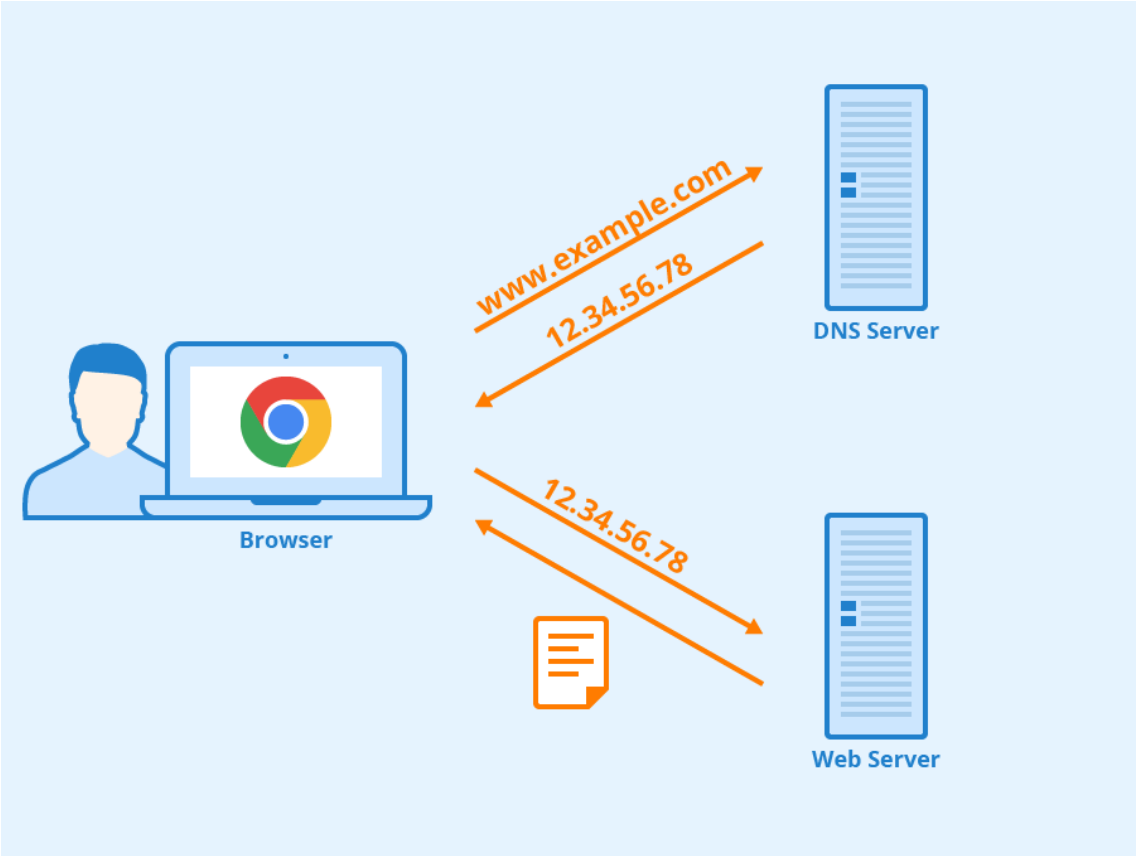



Figure 16 A illustration of how DNS conversion works in simple terms. (Seobility Wiki, n.d)

Domain names like oma.metropolia.fi are converted in IP addresses. The reasoning behind this is due to computers not understanding domain names because they operate on binary code. Therefore, IP addresses are a more compatible method of communication between devices. When the user's browser sends a domain search request, the DNS server will attempt to verify that it has the corresponding IP address for the domain. If the DNS server fails at providing the needed information, it will forward the request to other DNS servers as a joint effort to locate the IP address. (Seobility Wiki, n.d)

### 5.3.1 Typo Squatting

Fundamentally, typosquatting refers to usage of a fake DNS domain names imitating the authentic one to capture the user's connection to it. (Gupta et al, 2016) This can be caused from a small unnoticeable typo in the domain name.

In this case, the attacker's illegal phishing site attempts to impersonate trusted website. (Dahan, 2022)

The goal of phishing is the theft of personal information and the compromission of the target's PC via malware. Dnstwist provides an insight to identify phishing websites for stealing data. Dnstwist can be used to find possible phishing domains by using the target domain name such as google.com.

Figure 17 illustrates the usage of typosquatting by adding a letter at the end of a domain or changing vowels in the middle of the word.

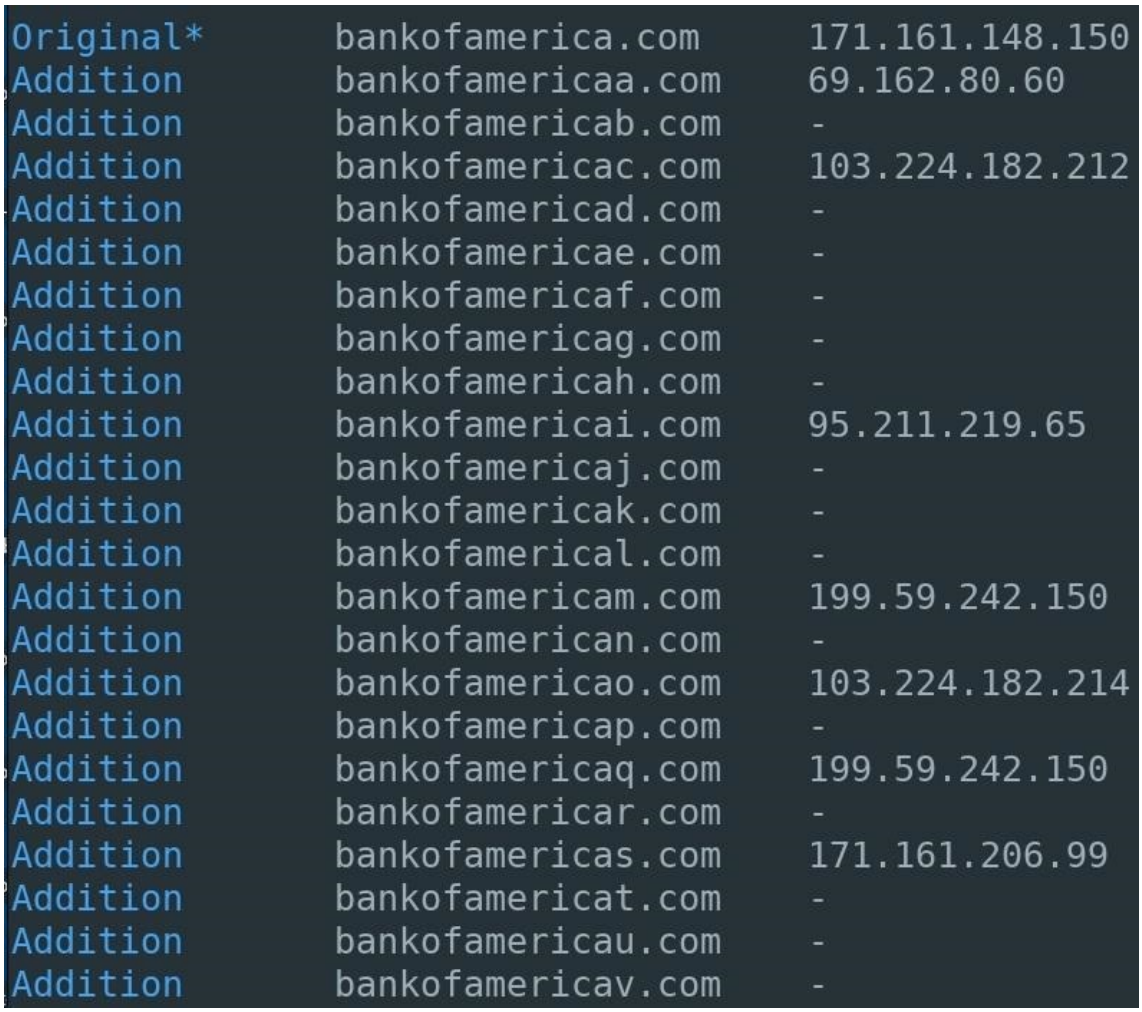


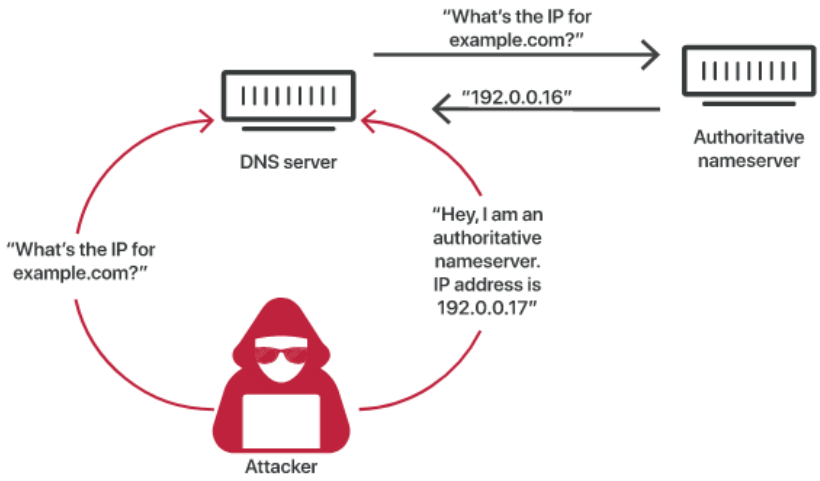

Figure 17 A screenshot of Dnstwist being used and searching for alternate domains of the Bank of America's official website. Multiple examples can be seen as live websites due to them having an IP address. (Tokyoneon, 2018)

These websites that are not holding the official domain bankofamerica.com are most likely attackers waiting for their next victim to input their banking credentials into the spoofed website.

## 5.4 DNS Cache Poisoning

DNS cache poisoning is when an attacker essentially exploits a legitimate website to become exposed and forward the target to another illegitimate malware infested website. The poisoning of DNS caches is simple for hackers due to DNS resolvers having virtually no capability of verifying data in the cache, ultimately leading to the data remaining in the cache until TTL expires. As there are various ways of exploiting DNS caches, this is due the design flaw of it. DNS caches were not designed for such a massive internet as it was based on a trust-based system. Attackers are capable of making a DNS resolver believe that the provided IP address for the sought-out domain name is legitimate, even though it is a redirection to a trap website. (Cloudflare, n.d)
Figure 18 provides two processes of how the process and behavior of DNS cache poisoning occurs.

DNS Cache Poisoning Process:




Poisoned DNS Cache:

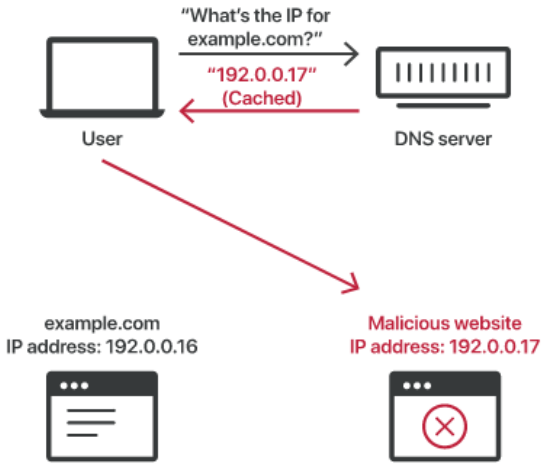



Figure 18 A screenshot of DNS Cache Poisoning Process (Cloudflare, n.d)

Figure 18 portrays how simple it is for a scammer to manipulate DNS resolvers to fool them due to the lack of multi factor authentication or verification for DNS caches. This is due to the usage of a faster but less reliable file transfer protocol such as UDP instead of the slower but more reliable TCP.

To counter these conflicts, implementing HTTPS for all traffic is essential. Alternatively, another solution to this system that lacks verification is called the

Domain Name System Security Extensions (DNSSEC). DNSSEC introduces a verification step in the DNS transaction by confirming the data integrity and origin. (Cloudflare, n.d)

# 6 Psychology and Awareness

Due to the sophistication of phishing and its modern implementations to society, victims keep on getting scammed by these malicious attacks. This section will discuss the psychological aspect of phishing, commencing with the effects attacker's attempt to inflict, a phishing attack anatomy, phishing prevention as an organization and individual, and the challenges of phishing prevention.

## 6.1 Psychological Manipulation

Despite phishing being present since the 1990s, phishing still remains to be one of the most efficient ways for scammers to gain from their targets. Phishing attacks prioritize the manipulation of human emotions, such as fear, urgency, and happiness. This method is acknowledged as the Amygdala Hijack. The amygdala is a part of the human brain that is involved with fear and emotions. (WebMD, n.d) The relevance of the human brain and its sensory reactions to data is crucial for psychological manipulation as hackers will employ a tactic that induces fear. Figure 19 is a screenshot of a perfect example of fear inducing tactics in phishing.

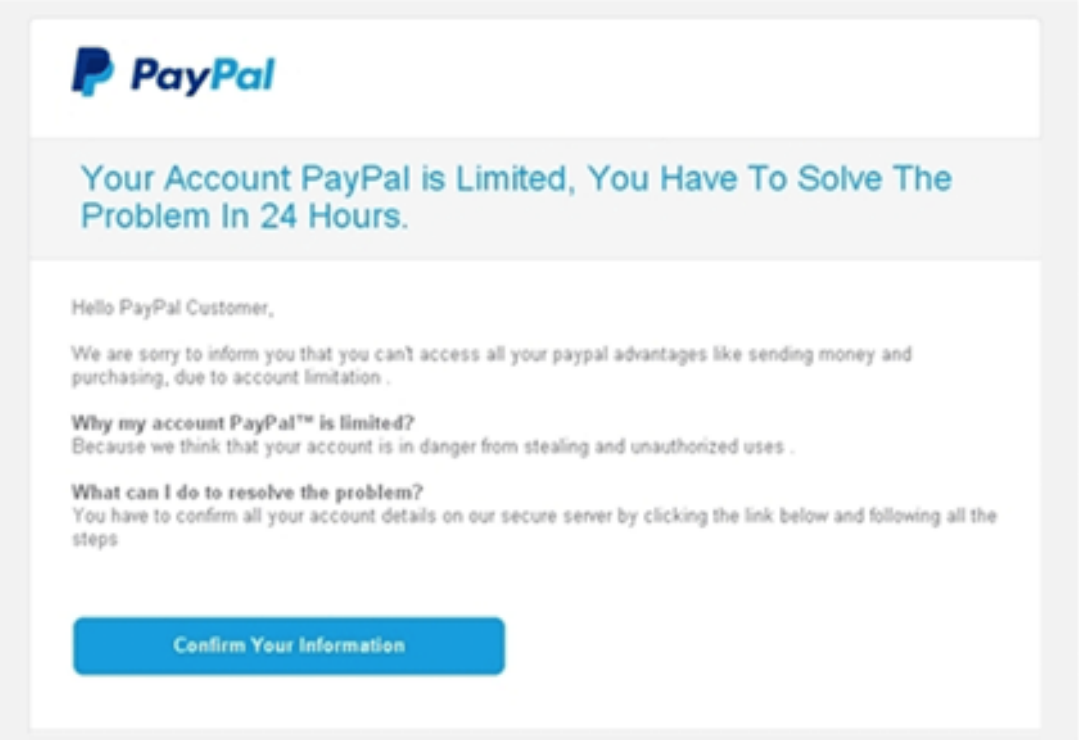



Figure 19 A phishing email that utilizes psychological manipulation of fear. (Worksighted, 2019)

Additionally, other emotions such as stress, over confidence, and greed drastically alter the perception of humans. (Worksighted, 2019)

## 6.2 Pretexting

As social engineering requires the overall understanding of human behaviour and manipulation of emotions, pretexting refers to exploitation of a fictitious scenario to trigger the aforementioned amygdala response. As a means of stealing information from the target, the scammer commonly impersonates a person of authority demanding confidential information. There are various example situations where the attacker utilizes emotions such as fear, greed, urgency, or panic. These methods include but are not limited to “Update account details” scam, romance scams, cryptocurrency scams, and government scams. Ultimately, after the scammer has gained credibility in their messages, the victim in most cases does not see through the lies and falls into the trap of pretexting.

The defence against pretexting is a difficult task due to the exploitation of human psychology instead of the utilization of technology. However, organizations offer guidelines to their workers to mitigate against attacks like these. (IBM, n.d; Malwarebytes, n.d)

## 6.3 Prevention

Understanding that hackers specialize in spreading malware and social engineering is essential to understanding the issues organizations must face and the precautions that are needed to be done to prevent damage or loss of valuable assets. Scammers exploit global situations through news, advertisements, and articles. For the attacker, all that is required from the user is multiple clicks of their malware links, which can lead to full control of the victim's PC. (Worksighted, 2019) To prevent phishing from occurring, there are two methods: User education and Software-based anti-phishing applications. (Gupta et al, 2016)

### 6.3.1 User Education

It is essential to implement the process of raising awareness and educating individuals and employees of organizations about phishing to recognize phishing and employing the correct defence against it. This education can be in the form of training and self-testing. Companies have implemented internal phishing tests as a means of training.

### 6.3.2 Software-based applications

As humans lack the consistency of a computer, it may not be an adequate solution for users to independently defend themselves against phishing. Therefore, it is quintessential for technical measure to be introduced. Anti-phishing is classified as a Software as a Service (SaaS) that analyses emails

being sent to corporation emails. (BasuMallick, 2021) These applications tend to implement message filtering via blacklisting threats and suspicious emails and whitelisting trusted emails. These applications are crucial for organizations as the sheer amount of phishing emails being sent out daily is a concerning amount. Only in the month April 2020 Google was successful in blocking around 18 million phishing emails that exploited the pandemic on a daily basis. (Swiss Cyber Institute, 2021) This statistic shows the harsh reality that organizations must face by implementing Software-based applications to filter spam.

### 6.4 Prevention Challenges

As all these above-mentioned methods have been put into practice, phishing is not completely mitigated. It is extremely doubtful that phishing will ever become avoided due to the ever-growing amount of AI, scripting, communities, and social engineering rapidly evolving which is making it excruciatingly demanding for cybersecurity professionals to fight back. Phishing is a variable that adapts to each target differently.

## 7 Case Study Analysis

This chapter will provide a live example of a phishing tool and how effortless phishing has become for anyone with a PC. The chapter will include the process of installing a Virtual Machine (VM) to host PC, downloading Kali Linux and SocialFish, and showing how SocialFish can be used to trick people into fake websites. SocialFish is available to download on GitHub. Additionally, multiple phishing links will be opened safely in an isolated Virtual Machine to showcase the characteristics and dangers of phishing links. The example phishing links will vary from reports and intensive research of examples that are worthy of analysis.

After logging in with the default credentials “kali” and password being “kali”, the VM boots up successfully.

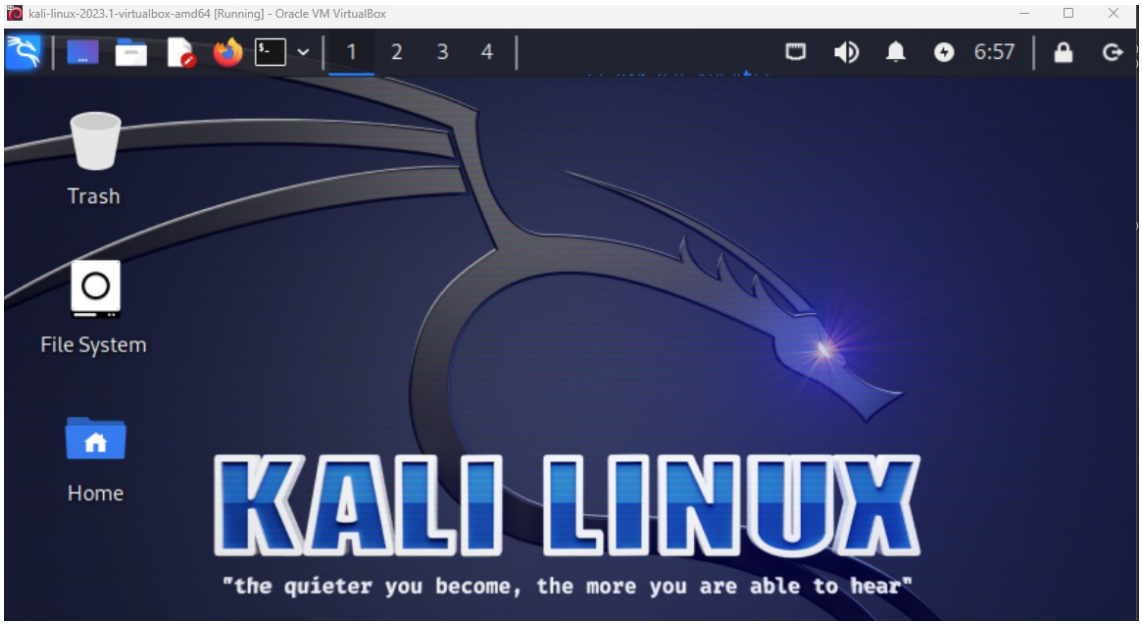



Figure 20 Kali Linux desktop.

Next, SocialFish will be installed. SocialFish is a phishing tool used for educational purposes which allows the tester to create a falsified website of an official website such as Facebook. SocialFish is capable of effortlessly cloning social media websites with login being necessary. (Kody, 2019) SocialFish is available to download from GitHub. (UndeadSec, 2018)

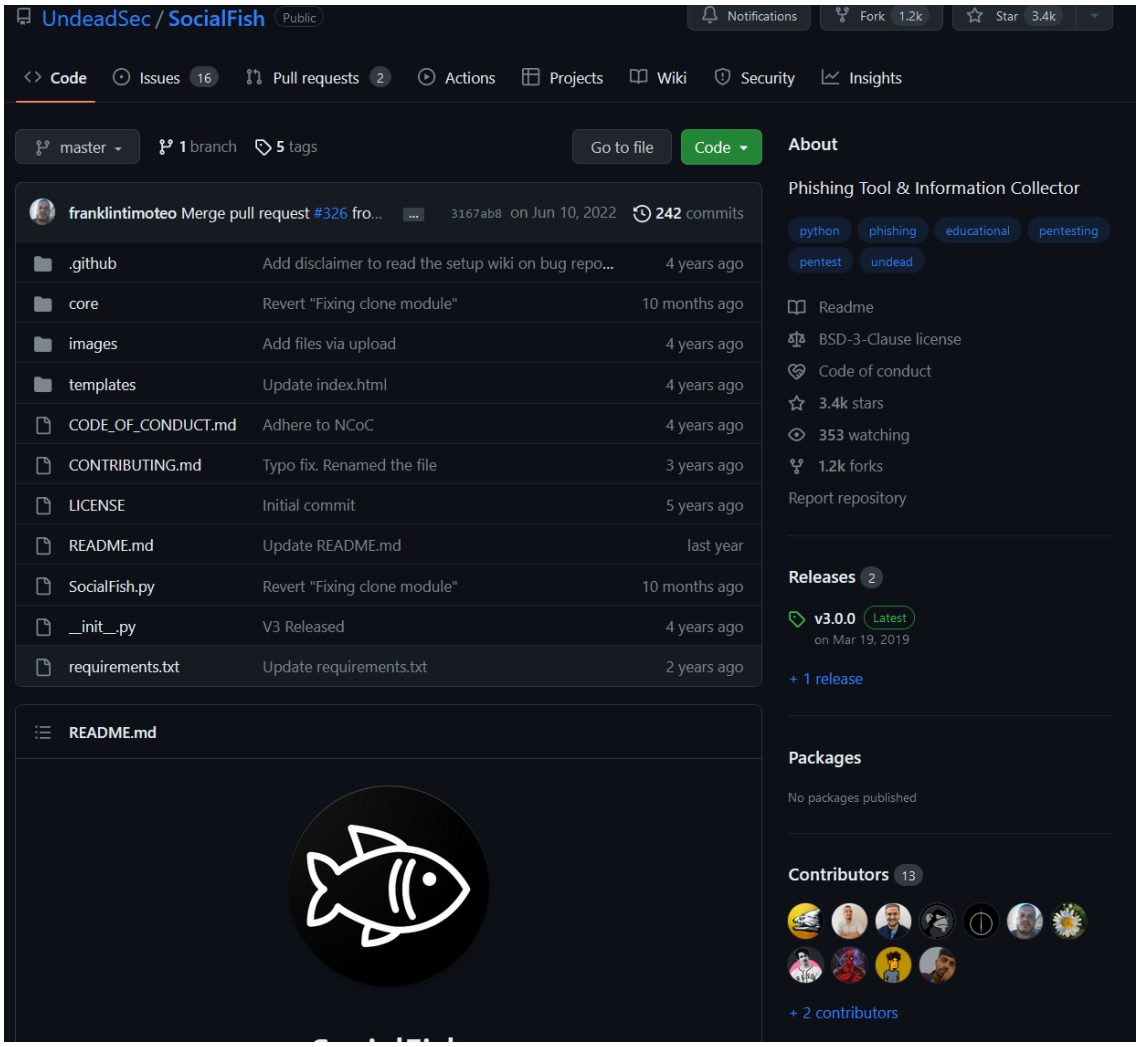



Figure 21 Screenshot of SocialFish's GitHub page. (UndeadSec, 2018)

## 7.1 SocialFish

The command “git clone https://github.com/UndeadSec/SocialFish.git” executes and begins installing SocialFish into the VM. After facing issues with the installation of the required applications for SocialFish, manual installation of each one was required. To initiate SocialFish, the user must apply a username and password after the using python3 to initiate SocialFish.py. This can be seen on Figure 22.

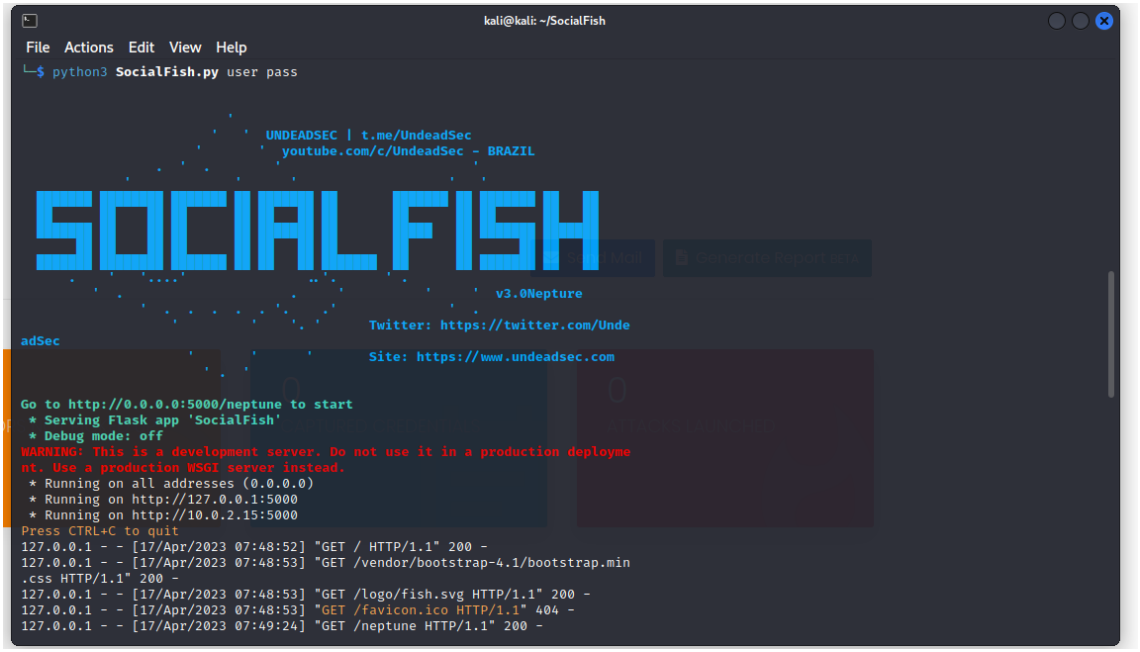



Figure 22 A screenshot of SocialFish running on terminal.

After initiation, the user must enter the 0.0.0.0:5000 site on their browser of choice. An authentication request will be prompted, and the user will type the

beforementioned credentials. Figure 23 shows SocialFish's main page.

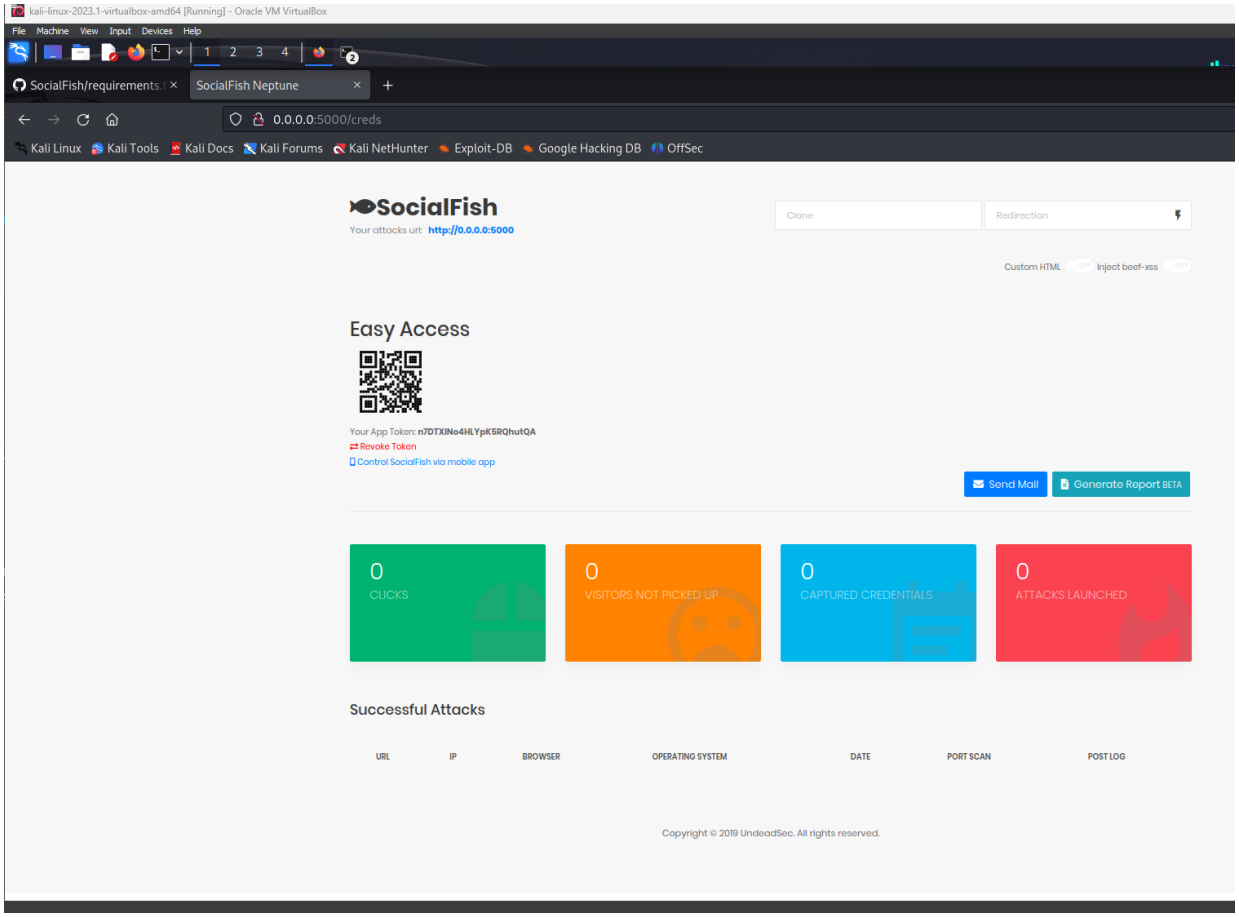



Figure 23 Screenshot of SocialFish front page.

As can be seen on the front page, SocialFish is also available for mobile use. In the top right there are two bars. The leftmost bar is the website that will be cloned, and the latter will be the website the victim will be redirected to. In this case, the leftmost can be a banking website's "/login" page which redirects to the banking website's home page. The attacker exploits the "/login" page because that is where the target will input their banking credentials. This is due to mitigate suspicion, the home page will make it seem that the target has successfully logged in.

As can be seen on Figure 24, SocialFish mimics Twitter's login page perfectly apart from it being outdated. Nevertheless, this application is regularly updated.

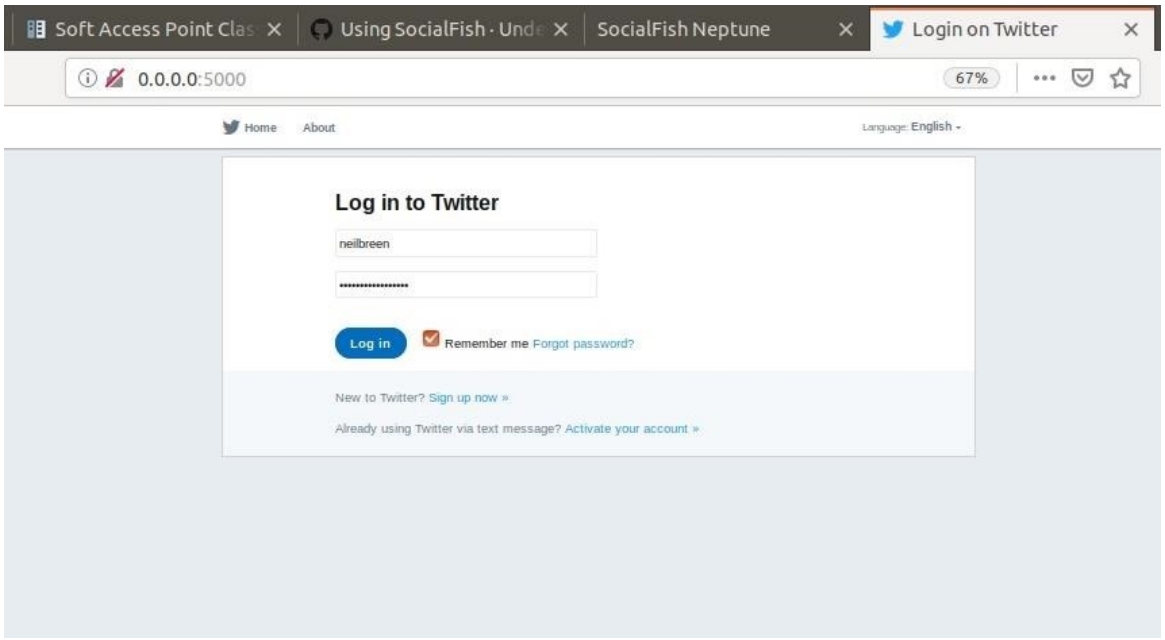



Figure 24 A screenshot of SocialFish making a clone website of Twitter's login page (Kody, 2019)

Since the Twitter login page has been cloned, it is best practice to implement the redirecting domain as a relevant one, such as Twitter's home page. It more logical, raises less suspicion, and the target would not think much of it. On the contrary, if the redirection domain would be youtube.com, then it would raise scepticism and the target would wonder what is going on. After the target has inputted their credentials, the main page will log clicks and captured credentials that are available to steal.

Figure 25 exhibits the successful attacks that have been captured. The attacker has gained information from the victim such as IP address, the OS used, credential collection, and the capability Shodan scanning the IP address for any vulnerabilities. Shodan is a port scanner that is utilized on a global scale that shares a similarity in use with Google. Shodan is primarily used as a search engine to view any visible network device that is connected to a server. This can be used for malicious purposes to find vulnerable routers or open ports where the attacker can execute their phishing attacks via malicious traffic on the open ports. (CyberTalents, n.d)

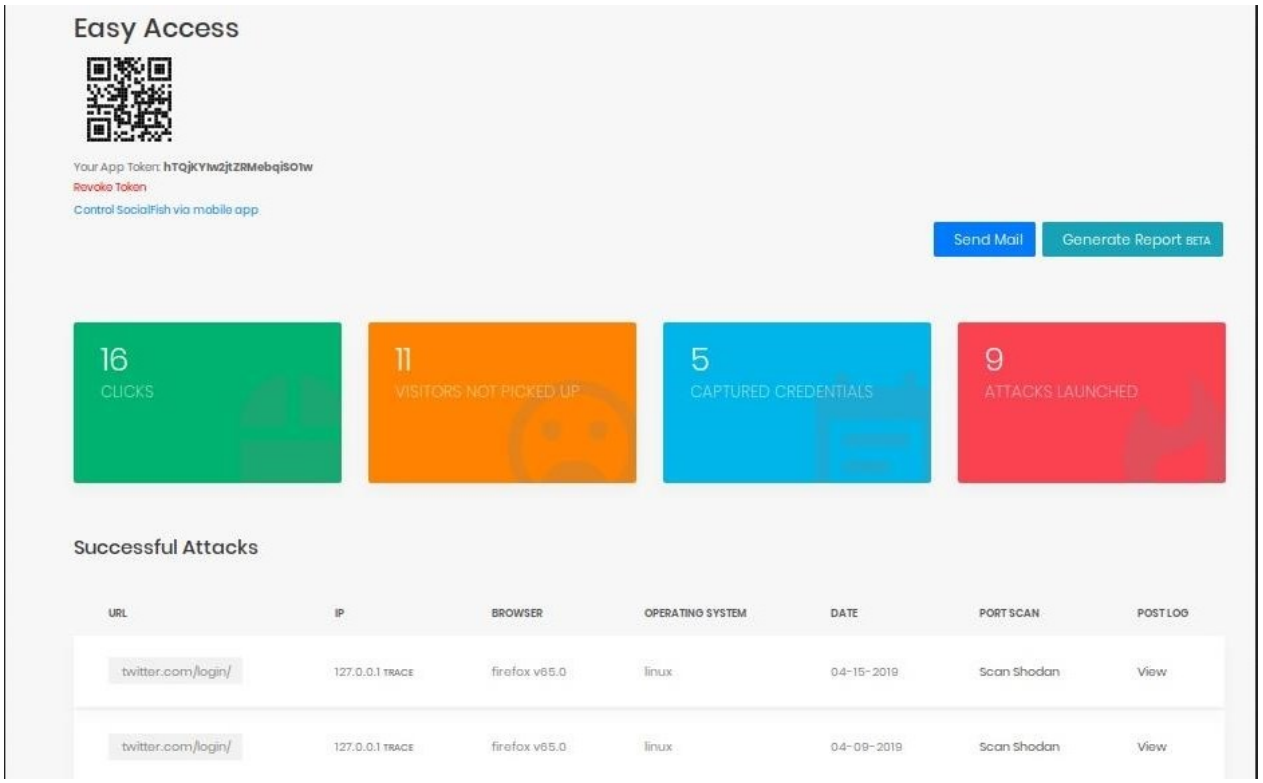



Figure 25 A screenshot of the front page of SocialFish with successful captured credentials. (Kody, 2019)

After the successful capture of credentials, the hacker is capable of viewing them. Clicking the “View” in the “Post Log” section will open a page that will be identical to Figure 26.

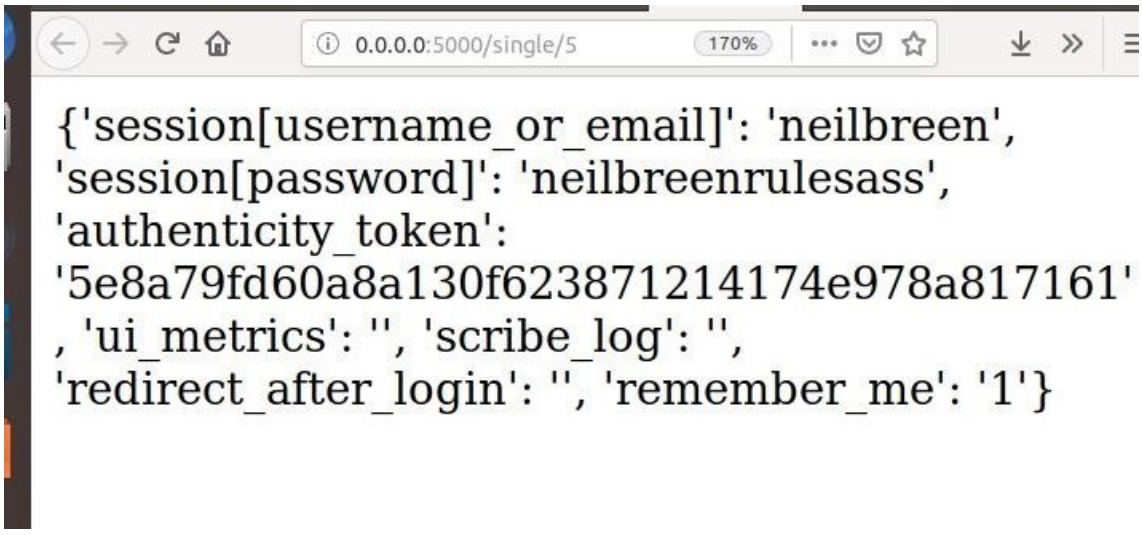



Figure 26 After clicking on "View", a new tab will open consisting of the credentials captured. (Kody, 2019)

The simple installation and effortless execution of SocialFish was capable of designing a website that resembles Twitter's login link with near perfection. This is a distressing fact for internet user to acknowledge as phishing evolves parallel to technological advancements.

## 7.2 DNStwist Exploration

Next, the aforementioned application Dnstwist provides a webpage for searching for deceptive domains of legitimate websites. Figure 27 is a screenshot of Dnstwist's webpage in a Kali Linux virtual machine.

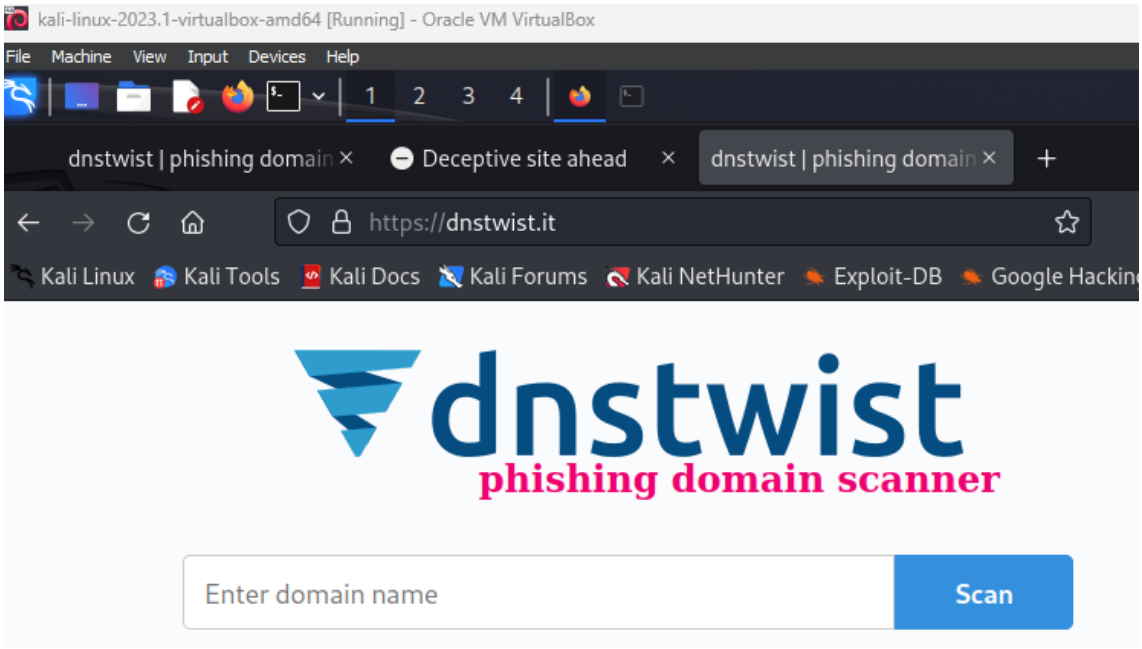



Figure 27 Screenshot of Dnstwist website running inside of a VM.

The objective of the search and viewing of these websites are to raise awareness and understanding of the real dangers of phishing, as per the reason this test is concocted on an isolated virtual machine sandbox. Instagram.com will be an example as attackers frequently implement typosquatting on social media platforms. Figure 28 provides a screenshot of the result when inputting Instagram.com on the search bar.

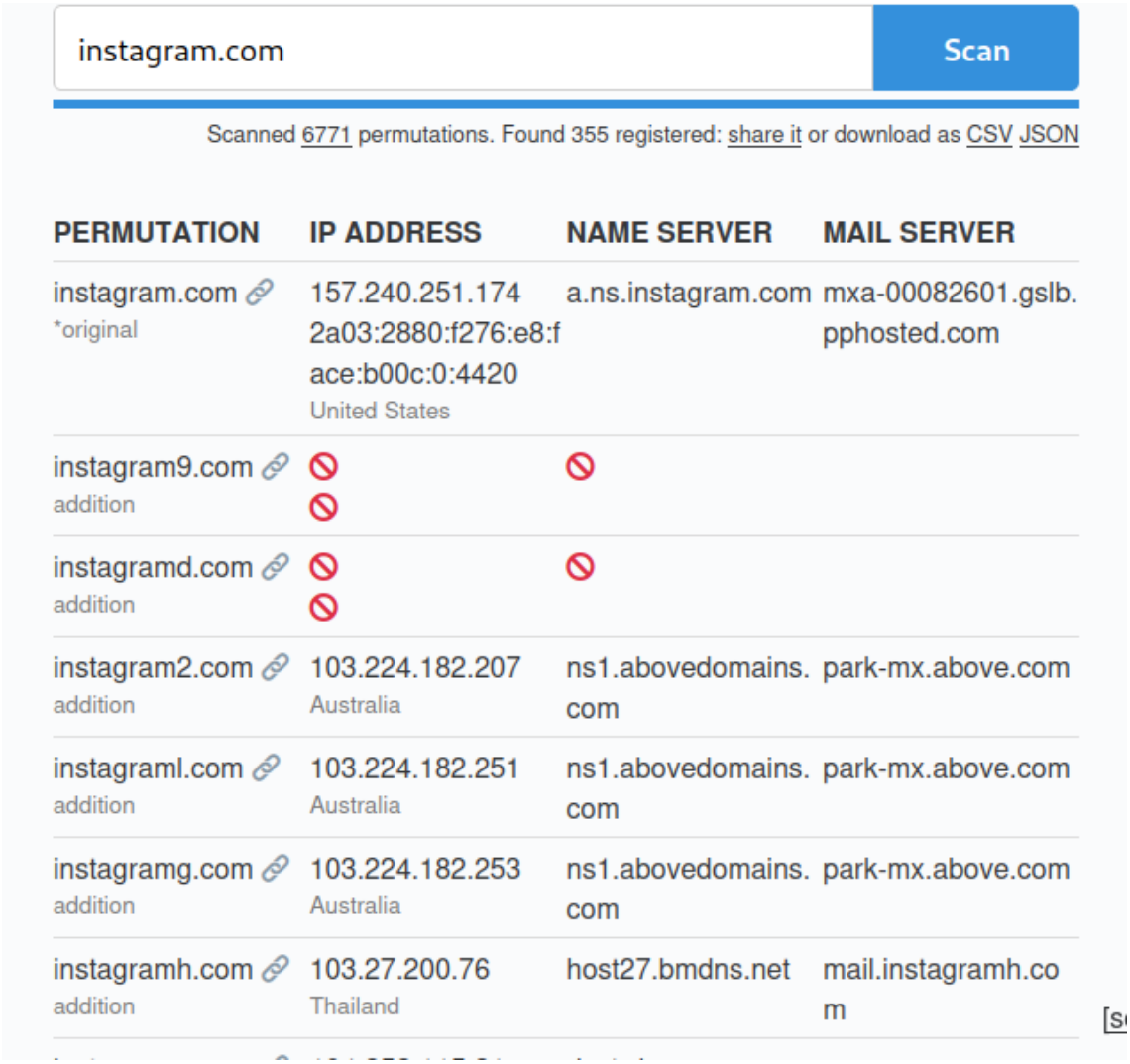



Figure 28 Screenshot of Dnstwist's search bar results.

After coming across to a site named “instagramb.com”, Google Safe Browsing warns the user of a deceptive site ahead. Figure 29 is a screenshot of the browser warning the user to not go further.

## 7.3 DNStwist Link Analysis

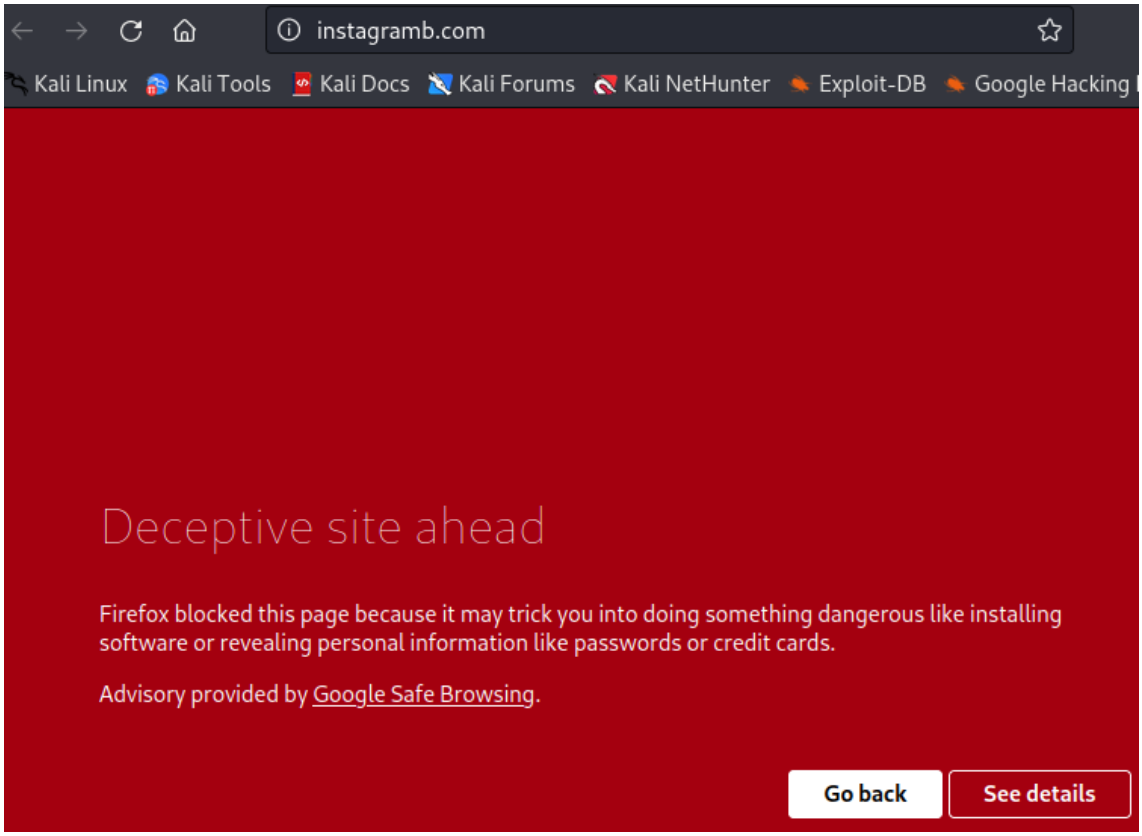



Figure 29 A screenshot of the browser blocking access to the website.

For the sake of the case study, the warning will be disregarded, and the case study will proceed by click on the “See details” button. Figure 30 showcases a

webpage that promotes an artist's music with hyperlinks for subscriptions of financial services. The phone number has been blurred for privacy reasons.


Figure 30 A screenshot of instagramb.com

After clicking on the hyperlinks, the website forwards itself to a payment page that requests for payment information. Figure 31 shows this website.

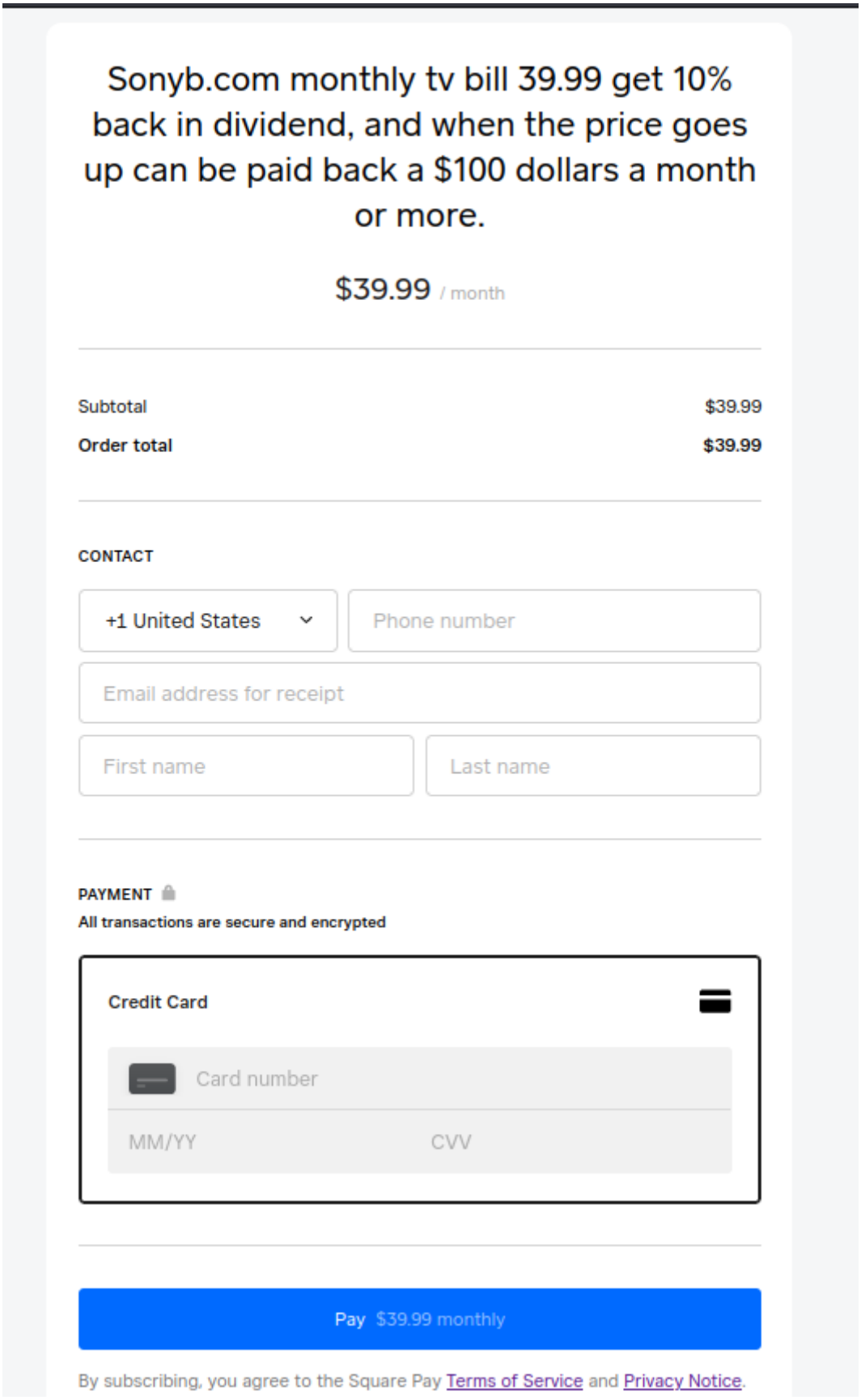



Figure 31 Screenshot of instagramb.com TV bill.

After filling the information requested with randomized text, the “$Pay 39.99 monthly” button was pressed, but to no avail it led to nowhere. It is extremely likely that the information inserted on the website was logged somewhere for the attacker to get a hold of.

## 7.4 JoeSandbox Malware Analysis

Websites such as VirusTotal and JoeSandbox analyze files and URLs for malicious activity so they can be reported and eradicated from the internet. JoeSandbox provides a list of websites that are confirmed and reported malware sites for malware analysis. Figure 32 is a screenshot of JoeSandbox’s malware analysis page.


Figure 32 A screenshot of JoeSandbox's website. (Joe Sandbox Cloud Basic, n.d)

This list shows clean websites with no malware in use and malicious websites such as the captcha phish threat website. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) refers to the small tests websites provide to prevent bot users committing fraud on their page. Scammers may implement CAPTCHA as a method of gaining trust from the target, as CAPTCHAs are commonly associated with legitimate websites. (AT&T Wireless, 2017)

Figure 33 is a screenshot of a CAPTCHA phishing website.

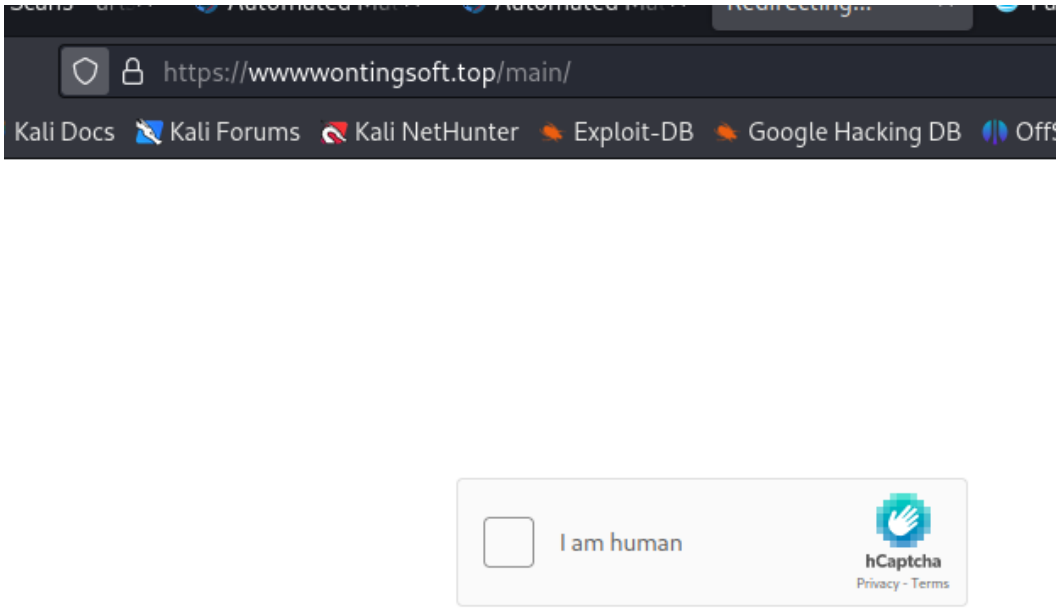



Figure 33 A screenshot of a CAPTCHA phishing site.

After filling out the CAPTCHA correctly, the website prompts to a Windows login clone, requesting to fill out a password as the user is attempting to access “sensitive info”. Figure 34 provides a screenshot of this.


Figure 34 A screenshot of a fake login site.

After inputting a randomized password, the prompt claimed the password was false. After executing these analyses of phishing websites, the Kali VM central

processing unit (CPU) usage has been throttling significantly, raising suspicion that resource-intensive scripts are running in the background.

# 8 Conclusion

In conclusion, the function of this thesis was to employ the stunning capabilities and constant evolution of phishing to raise awareness amongst internet users. By conveying the history of phishing along with the innovative methods provides a deeper understanding of the most effective cyber-crime method. It is critical to reflect on the possible countermeasures that can be applied due to the rising amount of phishing.

The interpretation of this thesis has provided a detailed viewpoint of the concerning threat of phishing, along with the damages it has impacted upon organizations and individuals globally. These damages are monetary but also reputation-based damage.

Secondly, phishing mitigation is employed to companies and individuals via SaaS and raising awareness with education. By activating these email filters in an organization and overlooking at the amount of spam emails blocked, the result is petrifying in terms of the capacity.

Overall, the attempts on mitigation and prevention are not going to entirely put an end to phishing. Phishing has stood its ground against the trials and tribulations of time, as it has been actively used since the Middle Ages to extract money from victims. The etymology of phishing is recent as it has been used since the 1980s. This thesis aims to prove that phishing evolves in parallel with the technological advancements of the world.

## References

1. Acunetix. What is cross-site scripting and how can you fix it? [Internet]. 2022 [cited 2023Apr29]. Available from: https://www.acunetix.com/websitesecurity/cross-site-scripting/

2. Alkhalil Z, Hewage C, Nawaf L, Khan I. 2021. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers. [Internet]. Frontiers. [cited 2023Apr4]. Available from: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

3. Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Information Security. Retrieved April 7, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9349804/
4. AT&T News, Wireless and Network Information. Fake captcha scam [Internet]. 2017 [cited 2023May1]. Available from: https://about.att.com/pages/cyberaware/ar/fake_captcha.

5. Axelton, K. 2023, '11 common scams targeting children and teens', Experian, viewed 11 April 2023, https://www.experian.com/blogs/ask-experian/common-scams-targeting-children-teens/.

6. Aztech IT. Be cautious of COVID-19 phishing attacks [Internet]. [cited 2023Apr12]. Available from: https://www.aztechit.co.uk/blog/be-cautious-of-covid-19-phishing-attacks

7. Baker, E. (2023). Everything to know about deepfake voice [Internet]. Veritone Voice. Available at: https://www.veritonevoice.com/blog/everything-you-need-to-know-about-deepfake-voice/ [Accessed 10 Apr. 2023].

8. BasuMallick C. 2021. Top 10 anti-phishing software in 2021. Spiceworks. [Internet]. Spiceworks. [cited 2023Apr17]. Available from: https://www.spiceworks.com/it-security/vulnerability-management/articles/top-10-anti-phishing-software/

9. Bloomberg Originals (2018). It's getting harder to spot a deep fake video [Internet]. YouTube. Available at: https://www.youtube.com/watch?v=gLoI9hAX9dw [Accessed 9 Apr. 2023].

10. Brewster, T. (2022). Fraudsters cloned company director's voice in $35 million bank heist, police find [Internet]. Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=864113275591 [Accessed 10 Apr. 2023].

11. Cloudflare. What is DNS cache poisoning? | DNS spoofing [Internet]. [cited 2023May1]. Available from: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

12. CyberTalents. (n.d.). SHODAN: The search engine for Hackers [Online]. CyberTalents Blog. Available at: https://cybertalents.com/blog/shodan-the-search-engine-for-hackers [Accessed 18 Apr. 2023].

13. Dahan M. What is typosquatting? how can you defend against it? [Internet]. Comparitech. 2022 [cited 2023Apr30]. Available from: https://www.comparitech.com/blog/information-security/typosquatting-cybersquatting-combosquatting/

14. Dansimp. (n.d.). Phishing trends and techniques. Microsoft Learn. Retrieved April 5, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/phishing-trends?view=o365-worldwide

15. EarthWeb. (2023). 13 smishing statistics in 2023 (SMS phishing attacks). Retrieved April 6, 2023, from https://earthweb.com/smishing-statistics/

16. ESET 2022, Identifying common social engineering attacks to kids, viewed 11 April 2023, https://saferkidsonline.eset.com/uk/article/identifying-common-social-engineering-attacks-to-kids.

17. Expert Insights. (2023). Healthcare Cyber Attack Statistics 2022: 25 alarming data breaches you should know. [online] Available at: https://expertinsights.com/insights/healthcare-cyber-attack-statistics/ [Accessed 29 Apr. 2023].

18. F-Secure. (n.d.). What is smishing? A new form of text message fraud. Retrieved April 6, 2023, from https://www.f-secure.com/en/articles/what-is-smishing

19. Gendre, A. (2020). Invoice phishing email. Vadesecure. Retrieved April 5, 2023, from https://www.vadesecure.com/en/blog/5-phishing-scams-and-how-to-spot-them

20. Get Safe Online 2021, Caught on the net!, viewed 11 April 2023, https://www.getsafeonline.org/personal/news-item/caught-on-the-net/.

21. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: State of the art and future challenges - neural computing and applications. SpringerLink. Springer London. Retrieved 2023Apr13 from https://link.springer.com/article/10.1007/s00521-016-2275-y

22. Hak5. (n.d.). O.MG adapter. Hak5. Retrieved 2023Apr13 from https://shop.hak5.org/collections/omg-row2/products/omg-adapter?variant=39914370236529

23. Healthcare IT News. (2021). The biggest healthcare data breaches of 2021. [online] Available at: https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021 [Accessed 29 Apr. 2023].

24. HIPAA Journal. (2022). Protect healthcare data from phishing. [online] Available at: https://www.hipaajournal.com/protect-healthcare-data-from-phishing/ [Accessed 29 Apr. 2023].

25. IBM Security. (2019). Cost of a Data Breach Report 2019.

26. IBM. What is pretexting? [Internet]. [cited 2023May1]. Available from: https://www.ibm.com/topics/pretexting

27. Joe Sandbox Cloud Basic. LLC JS. Automated malware analysis [Internet]. [cited 2023May1]. Available from: https://www.joesandbox.com/analysispaged/0.

28. Kali Linux. (2022). Get Kali [Online]. Available at: https://www.kali.org/get-kali/ [Accessed 17 Apr. 2023].

29. Kärkkäinen, H. (2021). Pelottava Huijaus Op:N nimissä – Huomaatko Pienen Eron Aidon ja Väärän Sivun Välillä? [Frightening scam in the name of Op: Can you spot the small difference between the real and fake page?]. Ilta-Sanomat. Retrieved April 6, 2023, from https://www.is.fi/digitoday/tietoturva/art-2000007956777.html

30. KnowBe4. (n.d.). History of phishing. Phishing.org. Retrieved April 3, 2023, from https://www.phishing.org/history-of-phishing

31. Kody. (2019). How to phish social media sites with Socialfish [Online]. WonderHowTo. Available at: https://null-byte.wonderhowto.com/how-

to/phish-social-media-sites-with-socialfish-0196136/ [Accessed 17 Apr. 2023].

32. Malwarebytes. What is pretexting [Internet]. [cited 2023May1]. Available from: https://www.malwarebytes.com/cybersecurity/business/what-is-pretexting.

33. NordVPN. (2023). What is a remote access trojan (rat)? [online] Available at: https://nordvpn.com/blog/remote-access-trojan/ [Accessed 29 Apr. 2023].
34. Ollmann, G. (2001). The Phishing Guide (Part 1). Technical Info. Retrieved April 4, 2023, from http://www.technicalinfo.net/papers/Phishing.html

35. Oracle VM VirtualBox. (n.d.). Welcome to Virtualbox.org! [Online]. Available at: https://www.virtualbox.org/ [Accessed 17 Apr. 2023].

36. OWASP Foundation. (n.d.). Session hijacking attack. OWASP Foundation. Retrieved 2023Apr15 from https://owasp.org/www-community/attacks/Session_hijacking_attack

37. OWASP Foundation. Cross site scripting (XSS) [Internet]. [cited 2023Apr29]. Available from: https://owasp.org/www-community/attacks/xss/

38. Posti.fi. (n.d.). Tietoa huijausviesteistä [Information about scam messages]. Retrieved April 7, 2023, from https://www.posti.fi/fi/asiakastuki/ehdot-ja-tietosuoja/tietoa-huijausviesteista

39. Proofpoint. (2023). What is spear phishing? - definition, examples, prevention. Proofpoint US. Retrieved April 5, 2023, from https://www.proofpoint.com/us/threat-reference/spear-phishing

40. Sample, I. (2020). What are Deepfakes – and How Can You Spot Them? The Guardian. [online] Available at: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [Accessed 8 Apr. 2023].

41. Seobility Wiki. (n.d.). What is a DNS Server and how does it work? Seobility Wiki. Retrieved 2023Apr15 from https://www.seobility.net/en/wiki/DNS_Server

42. SpyCloud, T. (2023). What is session hijacking and how do you prevent it? SpyCloud. Retrieved 2023Apr15 from https://spycloud.com/blog/what-is-session-hijacking/

43. Sternenko, S. (2022). Президент РФ обьявил о капитуляции россии. Русский солдат, бросай оружие и иди домой, пока жив! [Internet]. Twitter. Available at: https://twitter.com/sternenko/status/1504090918994993160?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504090918994993160%7Ctwgr%5E034693a0303e328cebb2636695b5af49a50d33d9%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Farticle%2Ffactcheck-putin-address-idUSL2N2VK1CC [Accessed 9 Apr. 2023].

44. Stupp, C. 2019, 'Fraudsters used AI to mimic CEO's voice in unusual cybercrime case', The Wall Street Journal, Dow Jones & Company, viewed 10 April 2023, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

45. Surfshark, n.d., Cybercrime statistics, viewed 10 April 2023, https://surfshark.com/research/data-breach-impact/statistics.

46. Swiss Cyber Institute. 2021. 27 phishing attack statistics you probably didn't know. [Internet]. Swiss Cyber Institute. [cited 2023Apr17]. Available

from: https://swisscyberinstitute.com/blog/cybersecurity-facts-phishing-statistics/

47. Thalen, M. (2022). A deepfake of Ukrainian president Volodymyr Zelensky calling on his soldiers to lay down their weapons was reportedly uploaded to a hacked Ukrainian news website today, per @shayan86 [Internet]. Twitter. Available at: https://twitter.com/MikaelThalen/status/1504123674516885507?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504123674516885507%7Ctwgr%5Ed7f7d35ddfa66eec124fac0dfa71b1ea20a89c56%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.npr.org%2F2022%2F03%2F16%2F1087062648%2Fdeepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia [Accessed 9 Apr. 2023].

48. The Straits Times. Broken English no longer a sign of scams as crooks tap AI bots like CHATGPT: Experts [Internet]. [cited 2023Apr12]. Available from: https://www.straitstimes.com/tech/broken-english-no-longer-a-sign-of-scams-as-crooks-tap-ai-bots-like-chatgpt-experts

49. Thrillist. The Webcam Hacking Episode of “Black Mirror” Is Its Scariest Yet [Internet]. [cited 2023Apr12]. Available from: https://www.thrillist.com/entertainment/nation/shut-up-and-dance-black-mirror-season-3-recap

50. Tidy, J. (2020). Coronavirus: How hackers are preying on fears of covid-19. BBC News. Retrieved April 7, 2023, from https://www.bbc.com/news/technology-51838468

51. Tokyoneon. 2018. How to easily generate hundreds of phishing domains. WonderHowTo. [Internet]. WonderHowTo. [cited 2023Apr15]. Available from: https://null-byte.wonderhowto.com/how-to/easily-generate-hundreds-phishing-domains-0184206/

52. Trendmicro. (n.d.). Spear phishing. Retrieved April 6, 2023, from https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html

53. Trendmicro. Sextortion scheme deployed by CHAOSCC hacker group demands US$700 in bitcoin [Internet]. [cited 2023Apr7]. Available from: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sextortion-scheme-deployed-by-chaoscc-hacker-group-700-in-bitcoin

54. UndeadSec. (n.d.). UndeadSec/socialfish: Phishing tool & information collector [Online]. GitHub. Available at: https://github.com/UndeadSec/SocialFish [Accessed 17 Apr. 2023].

55. WebMD. The amygdala: Your brain's fear response center. WebMD. [Internet]. WebMD. [cited 2023Apr16]. Available from: https://www.webmd.com/brain/amygdala-what-to-know

56. WikiHow. How to bypass CHATGPT's content filter: 4 simple ways [Internet]. [cited 2023Apr12]. Available from: https://www.wikihow.com/Bypass-Chat-Gpt-Filter

57. Worksighted. 2019. What makes humans click? the psychology of phishing: Worksighted Blog. [Internet]. Worksighted. [cited 2023Apr16]. Available from: https://www.worksighted.com/security/what-makes-humans-click-the-psychology-of-phishing/

58. ZDNet. Fraudsters are using machine learning to help write scam emails in different languages [Internet]. [cited 2023Apr12]. Available from: https://www.zdnet.com/article/fraudsters-are-using-machine-learning-to-help-write-scam-emails-in-different-languages/

59. ZDNet. What is CHATGPT and why does it matter? Here's what you need to know [Internet]. [cited 2023Apr12]. Available from: https://www.zdnet.com/article/what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/