PHISH-AWARE

Research Manual

SEAN DOWLING
C00246571

Abstract

Phishing is one of the main means in which cyber-attacks are developed. Fake emails are a main technique used by various phishers to steal confidential information such as usernames and passwords. Uniform Resource Locators (URLs) and attachments are the main source for sharing malwares, trojans and false information. Therefore, it is crucial to correctly distinguish between legitimate and phishing URLs and attachments. The utilization of different Application Programming Interfaces (API's)

Contents

Abstract 1

Table of Figures 4

1. Introduction 5

2. Phishing Overview 5

3. Types of Phishing 6

   a) Email Phishing 6

   b) Spear Phishing 7

   c) Whaling/CEO fraud 8

   d) Vishing 9

   e) Smishing 10

   f) Business Email Compromise (BEC) 11

   g) Pretexting 12

   h) Conclusion 12

4. Types of Malware 13

   a) Trojans 13

   b) Spyware 13

   c) Adware 13

   d) Rootkits 14

   e) Ransomware 14

   f) Worms 14

   g) Keyloggers 14

5. Email Attachments 15

   a) Executables 15

   b) Scripts 15

   c) Documents 16

   d) Archive Files 16

   e) Disk Images 17

6. Ways of Detecting Phishing Emails 18

   a) Email Sent from a Public Email Domain 18

   b) Domain Name is Misspelt 18

   c) Email is Poorly Written 18

d) Suspicious Attachments or Links 19
e) Message Ensues Urgency 19
f) Conclusion 20
7. Email Header Analysis 21
8. Email Authentication 22
a) SPF 22
b) DKIM 22
c) DMARC........23
9. Email Clients 23
10. Artificial Intelligence Vs. Programming Languages........24
a) Java 24
b) Python........24
c) Artificial Intelligence........24
d) Conclusion 24
11. API Utilization........25
12. URL Checkers........25
13. Attachment Checkers........25
14. Existing Tools........26
a) Avanan 26
b) Barracuda Sentinel 26
c) BrandShield 26
d) Cofense PDR 27
e) RSA FraudAction 27
f) IRONSCALES........27
g) Conclusion 27
15. Testing........28
a) GoPhish........28
b) King-Phisher........28
16. Conclusion........29
Glossary........30
Bibliography 31

Table of Figures

Figure 1: Credential Harvester Example (Spiceworks, 2018) 6
Figure 2: Spear Phishing Example (Micro, 2022) 7
Figure 3: Whaling Example (FRSecure, 2020) 8
Figure 4: Voicemail Phishing Example (Northwestern, n.d.) 9
Figure 5: Smishing Example (Tripwire, 2020) 10
Figure 6: Business Email Compromise Example (Chipeta, 2022) 11
Figure 7: Pretexting Example (Vadesecure, 2020) 12
Figure 8: Rise of Phishing Sites (Rosenthal, 2022) 12
Figure 9: Fantom Ransomware File Example (Meskauskas, 2021) 15
Figure 10: Malicious PHP File Example (SecureList, 2022) 15
Figure 11: Malicious Document File Example (Meskauskas, 2022) 16
Figure 12: Malicious ZIP File Example (Cyren, 2021) 16
Figure 13: Malicious ISO File Example (EMSI, 2018) 17
Figure 14: Public Domain Email Example 18
Figure 15: Misspelt Domain Name Example (Irwin, 2022) 18
Figure 16: Poorly Written Email Example (Crane, 2020) 19
Figure 17. Disguising a Link as a Button 19
Figure 18: Urgent Email Example (Montagnese, 2016) 20
Figure 19: SPF, DKIM, DMARC 22
Figure 20. Outlook's Unsafe Link Detection (Microsoft, 2021) 23

1. Introduction

Throughout the past few years, the use of phishing attacks has grown drastically in the cyber world. Cyberattacks increased 50% year-over-year, with each organization facing 925 cyberattacks per week globally (Spanning, 2022). So, protecting against this has never been higher. Some ways attackers are successful in these attacks are by implying a sense of urgency, such as, “Password will expire soon, click here to update.” 96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone. (Rosenthal, 2022)

The sense of urgency plays a significant role in phishing attacks, but there are also many more techniques used to gain access to sensitive information. What is hosted on these malicious URLs also varies, credential harvesters are a main constituent, these are websites looking for usernames, passwords or other personal identifiable information. URLs can even take device information like IP addresses, locations, etc.. Attackers could also automatically install malware on devices unbeknownst to users, like spyware, ransomware, or viruses. Breaches can also happen and enable access to your contacts, allowing attackers to send more phishing attacks friends and family. These are just some of the reasons I feel it has never been a better time to make a tool like an automated phishing detection system. This will allow users of the tool to not only feel protected, but also learn what phishing emails are like and how to identify them themselves in the future.

2. Phishing Overview

We must first understand what phishing is, and what are the many types phishing can appear in. Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website (Microsoft, n.d.). Phishing comes in many ways; the most common ways are described in detail below.

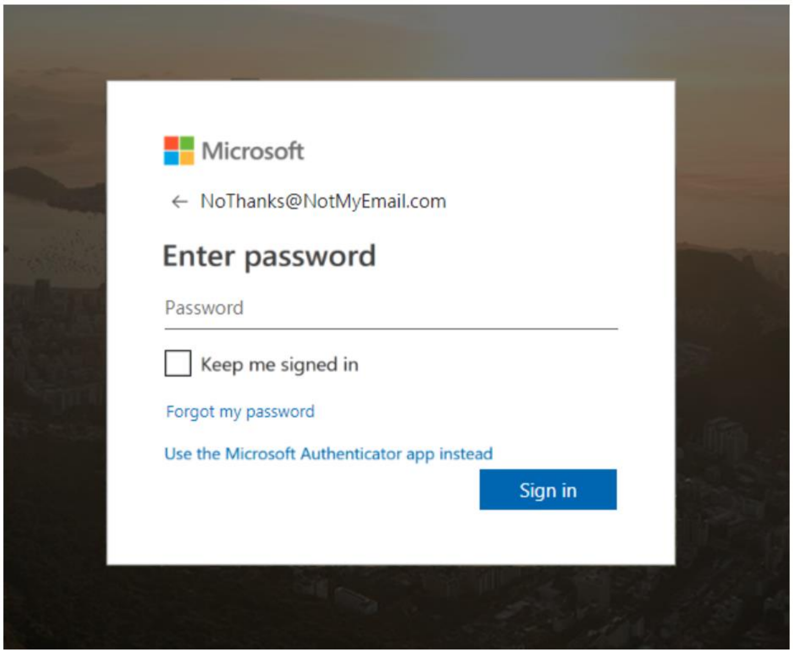
3. Types of Phishing

Phishing can take many forms, so understanding these in every shape and form is a must to provide the greatest level of security, ensuring that no one can fall victim to an attack. Different phishing methods focus on different targets, how many people they send this type of attack to, how the attachment or link looks for each person, or what can be stolen from each victim. Below I describe many forms of attacks and the different ways in which they are portrayed.

a) Email Phishing

- **Target:** An individual
- **Instance:** Singular
- **Design of Attachment/Link:** Tailored to individual, general detail of user
- **Vulnerable Information:** Personal Information like usernames, passwords, credit cards, etc.

Also called "deception phishing," email phishing is one of the most well-known attack types. Malicious actors send emails to users impersonating a known brand, leverage social engineering tactics to create a heightened sense of immediacy and then lead people to click on a link or download an asset (securityscorecard, 2021). Each phishing email is most of the time tailored to each individual with may be their name making each attack unique. Emails are sent to an individual separately as to not arouse suspicion. The malicious link or attachment may have a credential harvester, like the one shown below:



Microsoft

← NoThanks@NotMyEmail.com

Enter password

Password

□ Keep me signed in

Forgot my password

Use the Microsoft Authenticator app instead

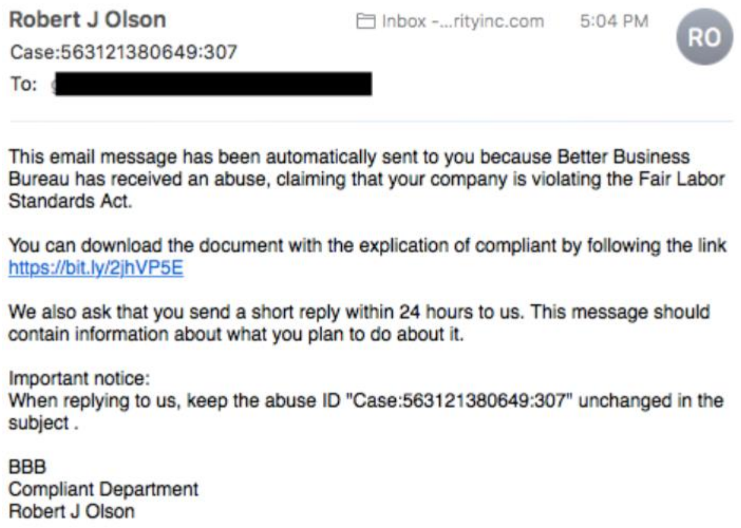
Figure 1: Credential Harvester Example (Spiceworks, 2018)

A credential harvester is often easy to spot in that the email field is already populated with the email that the attack was sent to, only needing the user to enter their password.

b) Spear Phishing

A. **Target:** Specific group, e.g., Accounting or Senior Management
B. **Instance:** Singular
C. **Design of Attachment/Link:** Tailored to individual, general detail of user/company
D. **Vulnerable Information:** Personal Information or business information

Spear phishing is a targeted attack on a specific group or users. These attacks are often done to users within a group of importance like Accounting or Senior Management. Cybercriminals start by using open-source intelligence (OSINT) to gather information from published or publicly available sources like social media or a company's website. Then, they target specific individuals within the organization using real names, job functions, or work telephone numbers to make the recipient think the email is from someone else inside the organization. Ultimately, because the recipient believes this is an internal request, the person takes the action mentioned in the email (securityscorecard, 2021).The below example again uses a sense of urgency to scare an individual to giving the attacker information before realising it is fraudulent.



Robert J Olson
Case:563121380649:307
To: [redacted]

This email message has been automatically sent to you because Better Business Bureau has received an abuse, claiming that your company is violating the Fair Labor Standards Act.

You can download the document with the explication of compliant by following the link https://bit.ly/2jhVP5E

We also ask that you send a short reply within 24 hours to us. This message should contain information about what you plan to do about it.

Important notice:
When replying to us, keep the abuse ID "Case:563121380649:307" unchanged in the subject .

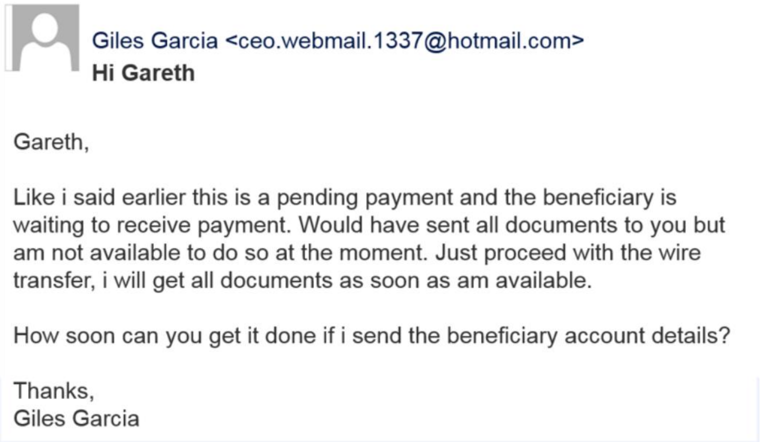
BBB
Compliant Department
Robert J Olson

Figure 2: Spear Phishing Example (Micro, 2022)

c) Whaling/CEO fraud

- **Target:** Specific user/group, e.g., Chiefs or Owners
- **Instance:** Singular or multiple
- **Design of Attachment/Link:** Personalized with very specific information
- **Vulnerable Information:** Business, finances, reputation

Whaling is like a spear phishing attack, except it focuses on targeting high-level management within the organization. One of the most common attacks is attempting to get a wire transfer (FRSecure, 2020). A wire transfer is used to send funds to a fraudulent account or an account that was used to hold the user at ransom. The example below shows an attacker impersonating the CEO of a company and is requesting funds be sent to a beneficiary account.



Giles Garcia <ceo.webmail.1337@hotmail.com>
Hi Gareth

Gareth,

Like i said earlier this is a pending payment and the beneficiary is waiting to receive payment. Would have sent all documents to you but am not available to do so at the moment. Just proceed with the wire transfer, i will get all documents as soon as am available.

How soon can you get it done if i send the beneficiary account details?

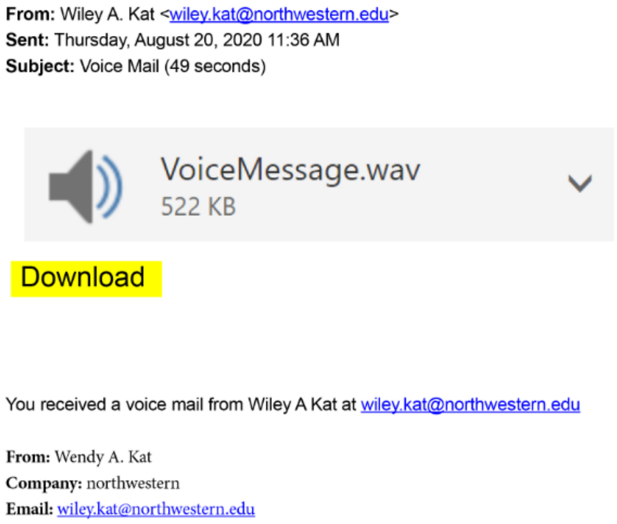
Thanks,
Giles Garcia

Figure 3: Whaling Example (FRSecure, 2020)

d) Vishing

1. **Target:** An individual
2. **Instance:** Singular
3. **Design of Attachment/Link:** Tailored to individual, general detail of user
4. **Vulnerable Information:** Personal Information like usernames and passwords

Vishing is a cybercrime that uses the phone to steal personal confidential information from victims. Often referred to as voice phishing, cyber criminals use savvy social engineering tactics to convince victims to act, giving up private information and access to bank accounts (TerraNovaSecurity, 2022). This type of attack will not be a primary focus for this project but is still important to understand as there is another form of 'voice' phishing attack circulating too. Attackers send emails with a voicemail attached, leaving the user to believe that they have a missed call. The victim is then requested to click the link to download the voicemail, but instead a virus or malware will be installed on the victim's machine. The picture below shows how this attack is crafted.



From: Wiley A. Kat <wiley.kat@northwestern.edu>
Sent: Thursday, August 20, 2020 11:36 AM
Subject: Voice Mail (49 seconds)

You received a voice mail from Wiley A Kat at wiley.kat@northwestern.edu

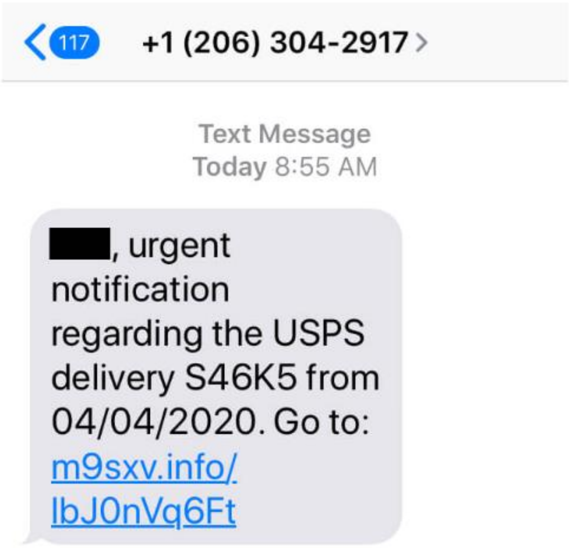
From: Wendy A. Kat
Company: northwestern
Email: wiley.kat@northwestern.edu

Figure 4: Voicemail Phishing Example (Northwestern, n.d.)

e) Smishing

- **Target:** An individual
- **Instance:** Singular
- **Design of Attachment/Link:** Tailored to individual, general detail of user
- **Vulnerable Information:** Personal Information like usernames and passwords

Smishing, or SMS Phishing, is another form of attack. Malicious actors often apply similar tactics to different types of technologies. Smishing is sending texts that request a person take an action. These are the next evolution of vishing. Often, the text will include a link that, when clicked, installs malware on the user's device (Ahola, 2021) .This type of attack again may not be a primary focus for this project but is still important to know the all the methods used by attackers. An example of Smishing can be seen in the picture below



+1 (206) 304-2917

Text Message
Today 8:55 AM

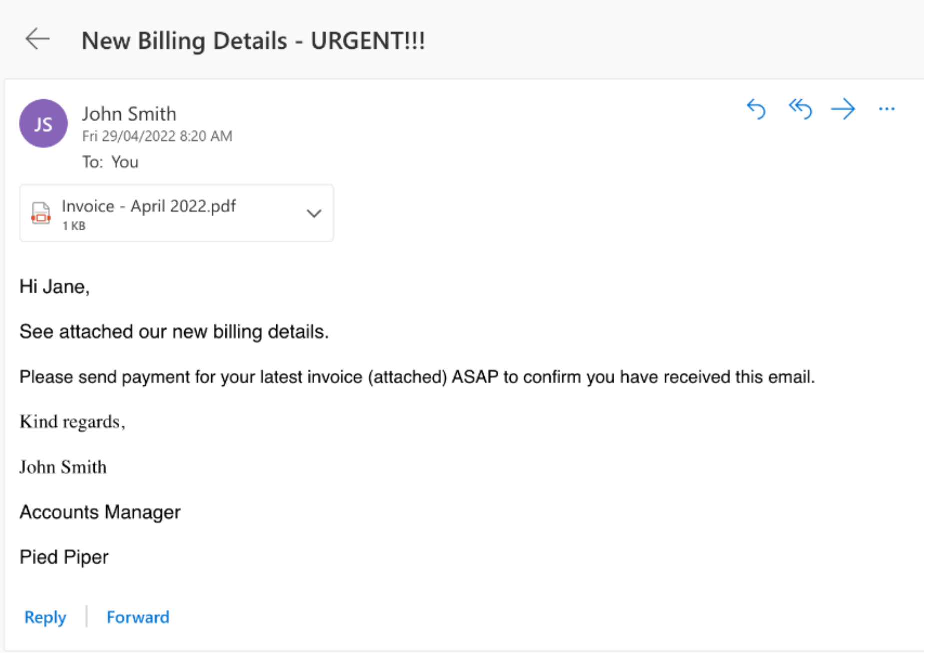
[redacted], urgent notification regarding the USPS delivery S46K5 from 04/04/2020. Go to: m9sxv.info/lbJ0nVq6Ft

Figure 5: Smishing Example (Tripwire, 2020)

f) Business Email Compromise (BEC)

- **Target:** An individual
- **Instance:** Singular
- **Design of Attachment/Link:** Tailored to individual, general detail of user
- **Vulnerable Information:** Personal Information or business information

A Business Email Compromise (BEC) is a scam where a criminal poses as a business partner, customer or vendor of the target recipient. These types of phishing attack make use of business terminology and often involve detailed research and long chains of messages to make the scam believable (Chipeta, 2022).



New Billing Details - URGENT!!!

John Smith
Fri 29/04/2022 8:20 AM
To: You

Invoice - April 2022.pdf
1 KB

Hi Jane,

See attached our new billing details.

Please send payment for your latest invoice (attached) ASAP to confirm you have received this email.

Kind regards,

John Smith

Accounts Manager

Pied Piper

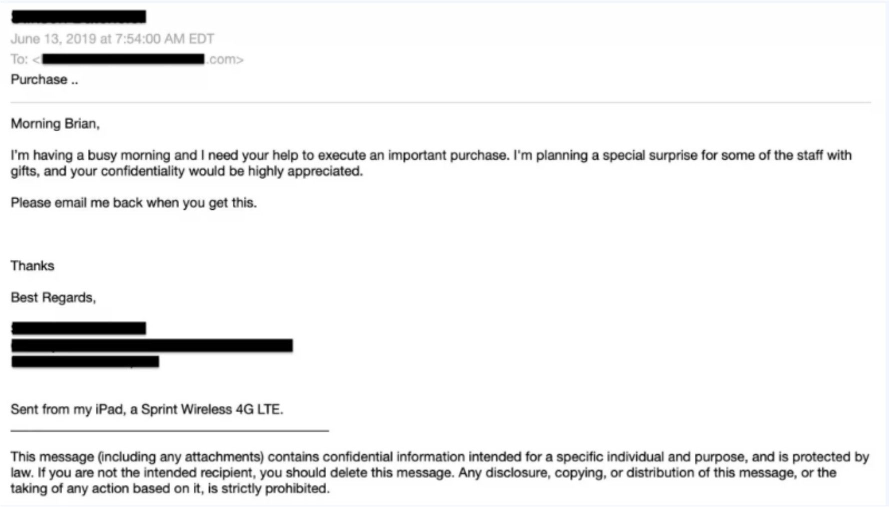
Figure 6: Business Email Compromise Example (Chipeta, 2022).

These types of attacks, similar to Whaling or Spear Phishing, target individuals that hold high positions in companies in order to get as much information as possible to carry out their attack. BEC attacks can have a significant financial impact on an organization. In some cases, attackers steal millions of dollars from their victims. Additionally, BEC attacks can damage an organization's reputation and cause customers to lose trust in the company (Fightcybercrime, n.d.)

g) Pretexting

- **Target:** An individual
- **Instance:** Singular
- **Design of Attachment/Link:** Tailored to individual, general detail of user
- **Vulnerable Information:** Personal Information or business information

Pretexting is exactly what it says on the tin. It’s a social engineering technique used by attackers to manipulate their targets into releasing information without knowing about it. This is usually done by a simple email stating they need their victim to send some information to them. An example of this is shown below



[redacted]
June 13, 2019 at 7:54:00 AM EDT
To: <[redacted].com>
Purchase ..

Morning Brian,

I'm having a busy morning and I need your help to execute an important purchase. I'm planning a special surprise for some of the staff with gifts, and your confidentiality would be highly appreciated.

Please email me back when you get this.

Thanks

Best Regards,

[redacted]

Sent from my iPad, a Sprint Wireless 4G LTE.

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

Figure 7: Pretexting Example (Vadesecure, 2020)

h) Conclusion

All of the examples outlined above will be the primary focus of this project. Protecting against these attacks have never been higher in recent years. A huge rise was seen just after the beginning of the COVID-19 outbreak. The chart below shows the rise in websites deemed as unsafe between January 2016 and January 2021.

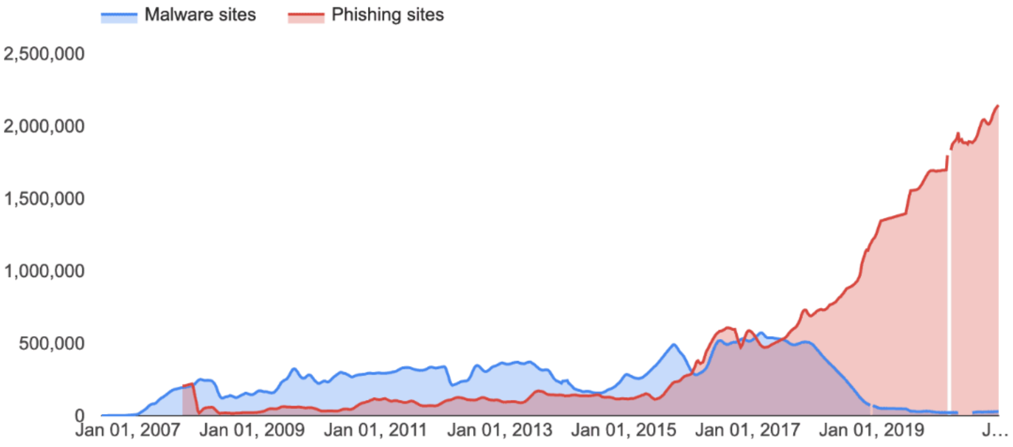


Figure 8: Rise of Phishing Sites (Rosenthal, 2022)

4. Types of Malware

Malware itself can come in many forms, and how it is sent to victims can be done in many forms also. Keeping people safe from these forms of malware is a key factor, ensuring that these files are checked and processed properly before deciding on whether it is safe or not is a must. Outlined by 'TitanFile,' there are seven common types of computer malware, those are:

a) Trojans

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network (Johansen, 2020). Consequences that lead on from downloading a Trojan file is backdoor access for the attacker, they may be able to get high level access to files or important information.

b) Spyware

Spyware. Although it sounds like a James Bond gadget, it's actually a type of malware that infects your PC or mobile device and gathers information about you, including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive (Malwarebytes, 2021). As guessed, this type of malware is often sneaky and operates without the user knowing. This can be installed by seemingly installing a legitimate file from an attachment and the spyware file is installed alongside it. The spyware then collects information on the victim like their common activity and in time slow down their machine rendering it useless.

c) Adware

Adware is software that displays unwanted (and sometimes irritating) pop-up adverts which can appear on your computer or mobile device (Kaspersky, n.d.). These again are installed by the victim installing software that appears legitimate and the adware is installed alongside it, unknowns to the user. There are three methods in which attackers can make a lot of money from this:

- Pay-per-click (PPC) — Every time an advertisement is opened, they get paid.
- Pay-per-view (PPV) — Every time an advertisement appears, they get paid.
- Pay-per-install (PPI) — Every time a victim installs the advertisement, they get paid.

d) Rootkits

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit." Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network (Veracode, 2021). If an attacker does get administration access to the victim's computer, they can then execute any files they want and can change system configurations to their liking. Rootkits are also very hard to detect and there is no commercial tool available that can detect all known rootkits.

e) Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment (Fruhlinger, 2020). The files that the attacker have encrypted will not be available for use by the victim, the only way to 'unlocking' these files will be by paying a fee to the attacker. These attacks are usually directed towards high level employees within top level corporations. The higher the company, the higher the fee needed will be.

f) Worms

To get a worm in a computer, the worm is often transmitted through vulnerabilities in software. They could also be sent through email attachments or within instant messages or spam emails. After a file is opened, it may link the user to a malicious website, or it could download the worm to the user's device automatically. After the worm is on the device, it infects it without the user being able to tell (Fortinet, 2021). Worms often exploit security vulnerabilities and bugs if there are known vulnerabilities within a file. An example of a worm is the Bagle/Beagle Worm. It was sent through an email and came through a password protected .zip file. It was originally made back in 2004 with some variations thereafter, through research, the most recent variation I could find was the Bagle.P variant in 2018.

g) Keyloggers

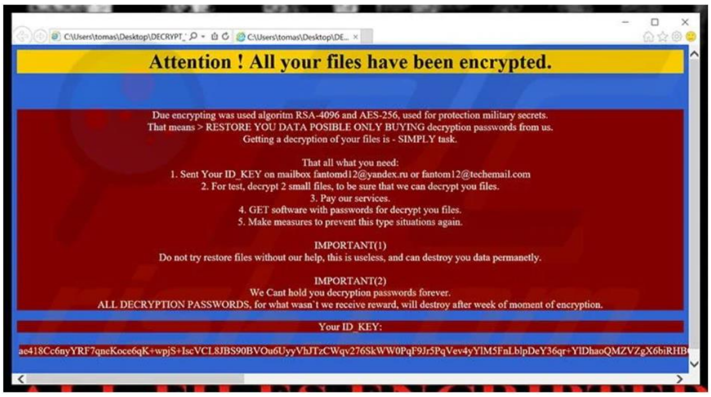
Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device (Malwarebytes, 2021). Keyloggers can be used to steal usernames and passwords. If an attacker can get these, they will then have access to anything they need to initiate their attack. Again, these can be installed alongside legitimate files sent through email attachments.

5. Email Attachments

The types of malware described above can be formatted in many different ways, Outlined by ‘Ergos,’ these 5 Types of email attachments you should look out for are:

a) Executables

Executable files are commonly used by attackers due to the ability to inject malicious code that can make changes to a computer system. For instance, the Fantom ransomware back in 2016 was packaged in a file named “WindowsUpdate.exe”. Once executed, it appeared to install an update on the victim’s PC. However, it only encrypted the user’s files and demanded money in exchange for data decryption. (Ergos, n.d.). The Fantom ransomware can be seen below:



Attention ! All your files have been encrypted.

Due encrypting was used algoritm RSA-4096 and AES-256, used for protection military secrets.
That means > RESTORE YOU DATA POSIBLE ONLY BUYING decryption passwords from us.
Getting a decryption of your files is - SIMPLY task.

That all what you need:
1. Sent Your ID_KEY on mailbox fantomd12@yandex.ru or fantom12@techemail.com
2. For test, decrypt 2 small files, to be sure that we can decrypt you files.
3. Pay our services.
4. GET software with passwords for decrypt you files.
5. Make measures to prevent this type situations again.

IMPORTANT(1)
Do not try restore files without our help, this is useless, and can destroy you data permanetly.

IMPORTANT(2)
We Cant hold you decryption passwords forever.
ALL DECRYPTION PASSWORDS, for what wasn`t we receive reward, will destroy after week of moment of encryption.

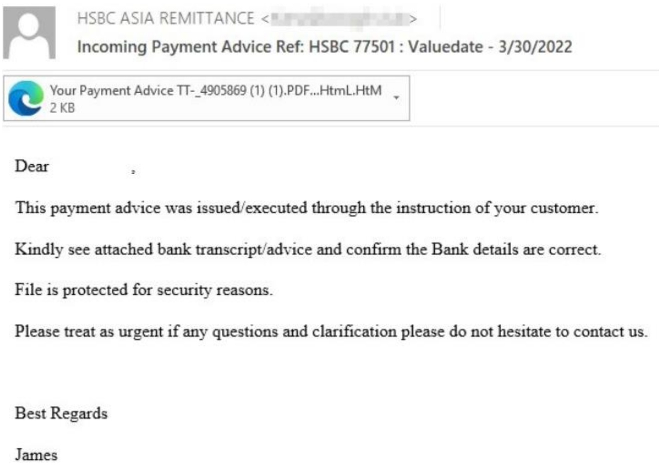
Your ID_KEY:

ae418Cc6nyYRF7qneKoce6qK+wpjS+IscVCL8JBS90BVOu6UyyVhJTzCWqv276SkWW0PqF9Jr5PqVev4yYIM5FnLblpDeY36qr+YIDhaoQMZVZgX6biRHB

Figure 9: Fantom Ransomware File Example (Meskauskas, 2021)

b) Scripts

Scripts are often contained within a ‘.php’ file. This contains code that will automatically install malware. These can often be attached to programmes such as documents or PDFs and will often go unnoticed to the victim. An example of this can be seen below:



HSBC ASIA REMITTANCE <[redacted]>
Incoming Payment Advice Ref: HSBC 77501 : Valuedate - 3/30/2022

Your Payment Advice TT-_4905869 (1) (1).PDF...HtmL.HtM
2 KB

Dear ,

This payment advice was issued/executed through the instruction of your customer.

Kindly see attached bank transcript/advice and confirm the Bank details are correct.

File is protected for security reasons.

Please treat as urgent if any questions and clarification please do not hesitate to contact us.

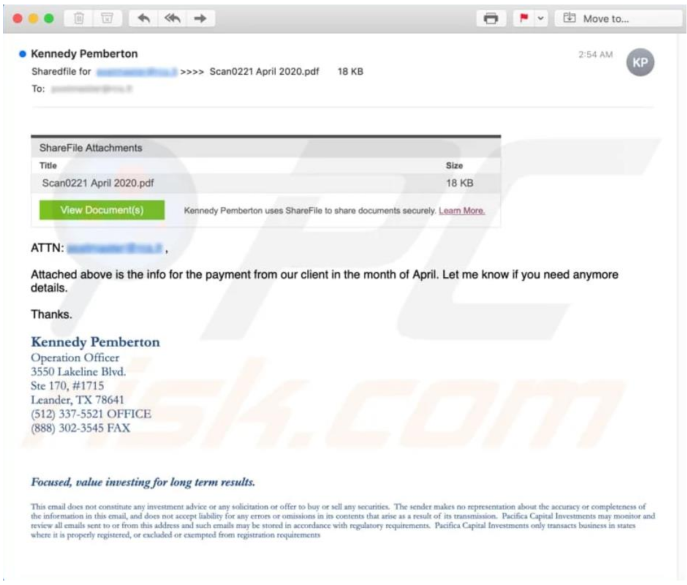
Best Regards

James

Figure 10: Malicious PHP File Example (SecureList, 2022)

c) Documents

Cybercriminals are using harmless-looking documents to infect host computers with macro malware. Macros are small programs that automate common tasks, like downloading files or installing a program (Ergos, n.d.). Hackers take advantage of vulnerabilities in applications that read or allow editing of documents, like Microsoft Office or Adobe Acrobat. Hackers take advantage of these vulnerabilities by including code that contains malware within document files that will end up infecting a computer once these documents are opened. Detecting these edited documents will be difficult, as they will still appear as legitimate documents. An example of this can be seen below:



Kennedy Pemberton 2:54 AM
Sharedfile for [redacted] >>>> Scan0221 April 2020.pdf 18 KB
To: [redacted]

ShareFile Attachments

Title	Size
Scan0221 April 2020.pdf	18 KB

View Document(s) Kennedy Pemberton uses ShareFile to share documents securely. Learn More.

ATTN: [redacted] ,

Attached above is the info for the payment from our client in the month of April. Let me know if you need anymore details.

Thanks.

Kennedy Pemberton
Operation Officer
3550 Lakeline Blvd.
Ste 170, #1715
Leander, TX 78641
(512) 337-5521 OFFICE
(888) 302-3545 FAX

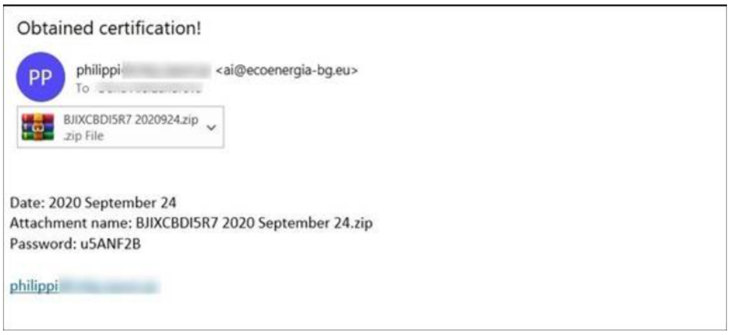
Focused, value investing for long term results.

This email does not constitute any investment advice or any solicitation or offer to buy or sell any securities. The sender makes no representation about the accuracy or completeness of the information in this email, and does not accept liability for any errors or omissions in its contents that arise as a result of its transmission. Pacifica Capital Investments may monitor and review all emails sent to or from this address and such emails may be stored in accordance with regulatory requirements. Pacifica Capital Investments only transacts business in states where it is properly registered, or excluded or exempted from registration requirements

Figure 11: Malicious Document File Example (Meskauskas, 2022)

d) Archive Files

These files are often stored in '.zip' or '.rar' folders. These are harder to detect also because to run a check on a file, we need access to them, but if they are stored in an archived folder, the user needs to download the folder to check. These will be the hardest to protect victims against I feel. An example of this can be seen below:



Obtained certification!

philippi[redacted] <ai@ecoenergia-bg.eu>
To [redacted]

BJIXCBDI5R7 2020924.zip
.zip File

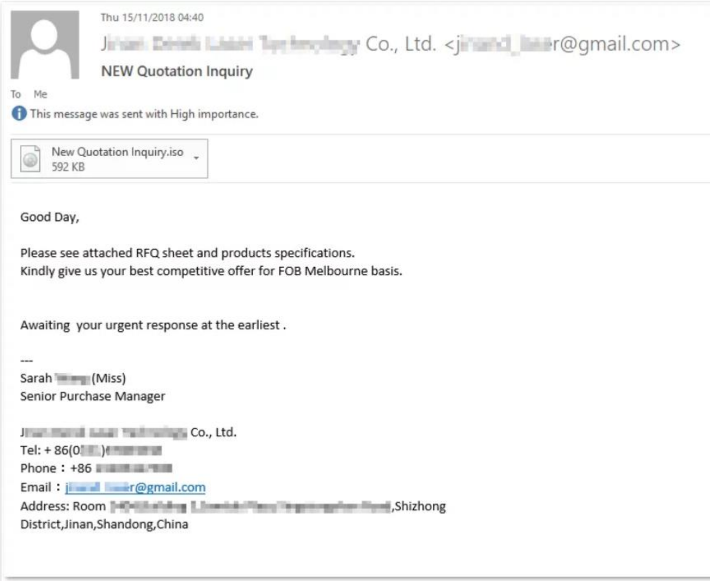
Date: 2020 September 24
Attachment name: BJIXCBDI5R7 2020 September 24.zip
Password: u5ANF2B

philippi[redacted]

Figure 12: Malicious ZIP File Example (Cyren, 2021)

e) Disk Images

While almost exclusively used in macOS, disk images are still one of the most dangerous attachments to avoid. Much like archive files, disk images can conceal executables and documents (Ergos, n.d.).This type of attack often takes place on a '.iso' file. Cyber criminals have been taking advantage of built-in Windows capabilities to mount disk image files once the end user opens them. There are multiple disk image file formats, but we have seen ISO and IMG files being abused the most (Taibo, 2020). I think when doing my project, I will alert the user of any ISO file attached as it is exceedingly rare that ISO files would be sent in an email in the first instance. One example of this type of attack can be seen below:



Thu 15/11/2018 04:40

J[redacted] Co., Ltd. <j[redacted]r@gmail.com>

NEW Quotation Inquiry

To Me

This message was sent with High importance.

New Quotation Inquiry.iso
592 KB

Good Day,

Please see attached RFQ sheet and products specifications.
Kindly give us your best competitive offer for FOB Melbourne basis.

Awaiting your urgent response at the earliest .

Sarah [redacted] (Miss)
Senior Purchase Manager

J[redacted] Co., Ltd.
Tel: + 86(0[redacted])[redacted]
Phone：+86 [redacted]
Email：[redacted]r@gmail.com
Address: Room [redacted],Shizhong District,Jinan,Shandong,China

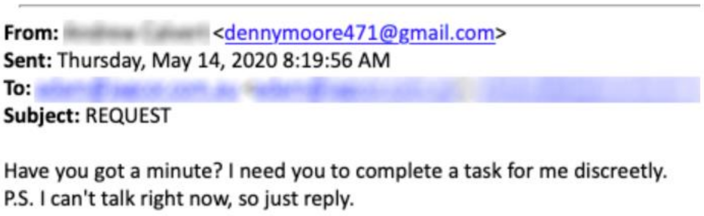
Figure 13: Malicious ISO File Example (EMSI, 2018)

6. Ways of Detecting Phishing Emails

Before even checking the URL's and attachments, we must know if the email is sent from a legitimate user, this will give us ease of mind knowing that it is from a legitimate source, but we cannot trust this with full extent as email addresses and domains can still be spoofed. There are 5 simple ways to detect phishing attacks outlined by 'IT Governance.'

a) Email Sent from a Public Email Domain

No legitimate organisation will send emails from an address that ends '@gmail.com.' Not even Google (Irwin, 2022). Most large corporations have their own domain name (anything after the @ symbol), the only time this may not come into effect is if it is a small business owner. As shown below, the email is sent from @gmail.



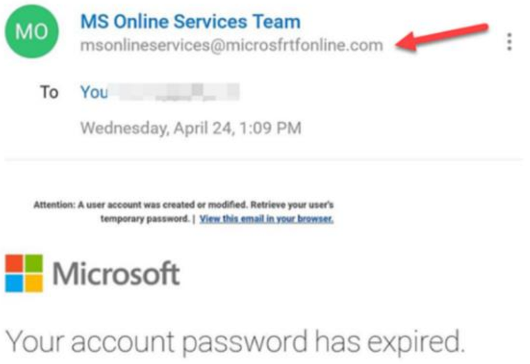
From: [redacted] <dennymoore471@gmail.com>
Sent: Thursday, May 14, 2020 8:19:56 AM
To: [redacted]
Subject: REQUEST

Have you got a minute? I need you to complete a task for me discreetly.
P.S. I can't talk right now, so just reply.

Figure 14: Public Domain Email Example

b) Domain Name is Misspelt

Domain names must be unique, but to bypass this, attackers could intentionally misspell words that would go unnoticed to the naked eye, an example of this could be 'googgle' or 'microsotf.' For my project, I could incorporate a domain name checker with the most common domain names like Google, Facebook, Twitter, etc.. The example below shows how Microsoft is spelt discreetly wrong, as to not arise suspicion and hope it goes unnoticed.



MO

MS Online Services Team
msonlineservices@microsfrtfonline.com

To You [redacted]

Wednesday, April 24, 1:09 PM

Attention: A user account was created or modified. Retrieve your user's temporary password. | View this email in your browser.

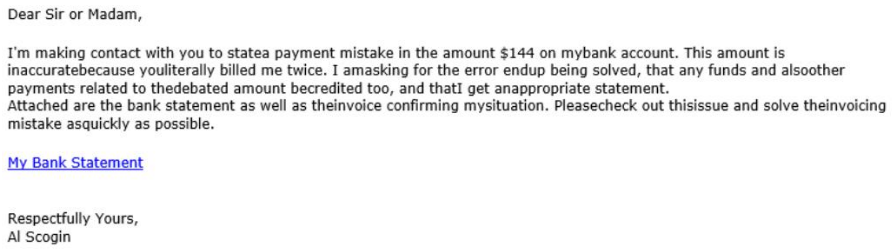
Microsoft

Your account password has expired.

Figure 15: Misspelt Domain Name Example (Irwin, 2022)

c) Email is Poorly Written

This includes silly spelling mistakes that any grammar checker would highlight. Attackers use this method to only get the most gullible of people to fall for the scam, this means most people who read the scam email will instantly be able to tell that it's a scam, but if you do end up falling for it in the first place, you are more likely to follow along for the rest of the scam. The example below shows exactly how obvious this type of Phish is to determine:



Dear Sir or Madam,

I'm making contact with you to statea payment mistake in the amount $144 on mybank account. This amount is inaccuratebecause youliterally billed me twice. I amasking for the error endup being solved, that any funds and alsoother payments related to thedebated amount becredited too, and thatI get anappropriate statement.
Attached are the bank statement as well as theinvoice confirming mysituation. Pleasecheck out thisissue and solve theinvoicing mistake asquickly as possible.

My Bank Statement

Respectfully Yours,
Al Scogin

Figure 16: Poorly Written Email Example (Crane, 2020)

d) Suspicious Attachments or Links

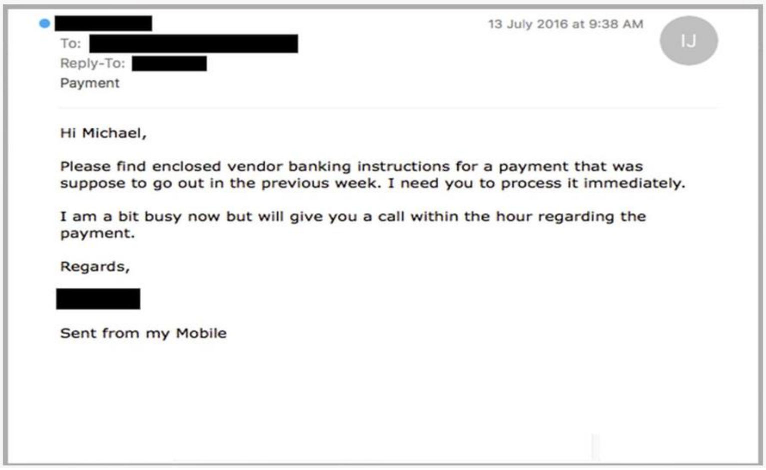
This is what I will be focusing on primarily in my project. If, somehow, everything within in the email appears legitimate, attackers will try scam you through attachments and links. Through attachments, attackers can install malware, spyware, keyloggers or trojans that may appear as a normal application. As I described above, these attachment malware files can take many forms and can cause severe damage. Links on the other hand are treated differently by attackers, you can spot a suspicious link if the destination address does not match the context of the rest of the email. For example, if you receive an email from Netflix, you expect the link to direct you towards an address that begins 'netflix.com' (Irwin, 2019). Although, attackers can avoid showing a link by using a button instead.

Figure 17. Disguising a Link as a Button

One way avoiding falling for a scam like this is by hovering your mouse over the button, revealing the actual link that you would be redirected to. This is where I feel I will have a tough time checking links as they will embedded within the button. Clicking on a phishing link could lead to information being stolen, like usernames and passwords, malware may be installed, contacts on your network may be exploited and used for further phishing attacks.

e) Message Ensues Urgency

This is a common technique used by attackers. The more time a victim spends looking at the contents of an email means the more they will realize that it is a phishing email. Attackers create a sense of urgency, so may be implying your password will expire soon, click on the link to change it now. The example below shows that banking instructions are included, and a payment should of went to it last week.



[redacted]

To: [redacted]

Reply-To: [redacted]

Payment

13 July 2016 at 9:38 AM

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

Figure 18: Urgent Email Example (Montagnese, 2016)

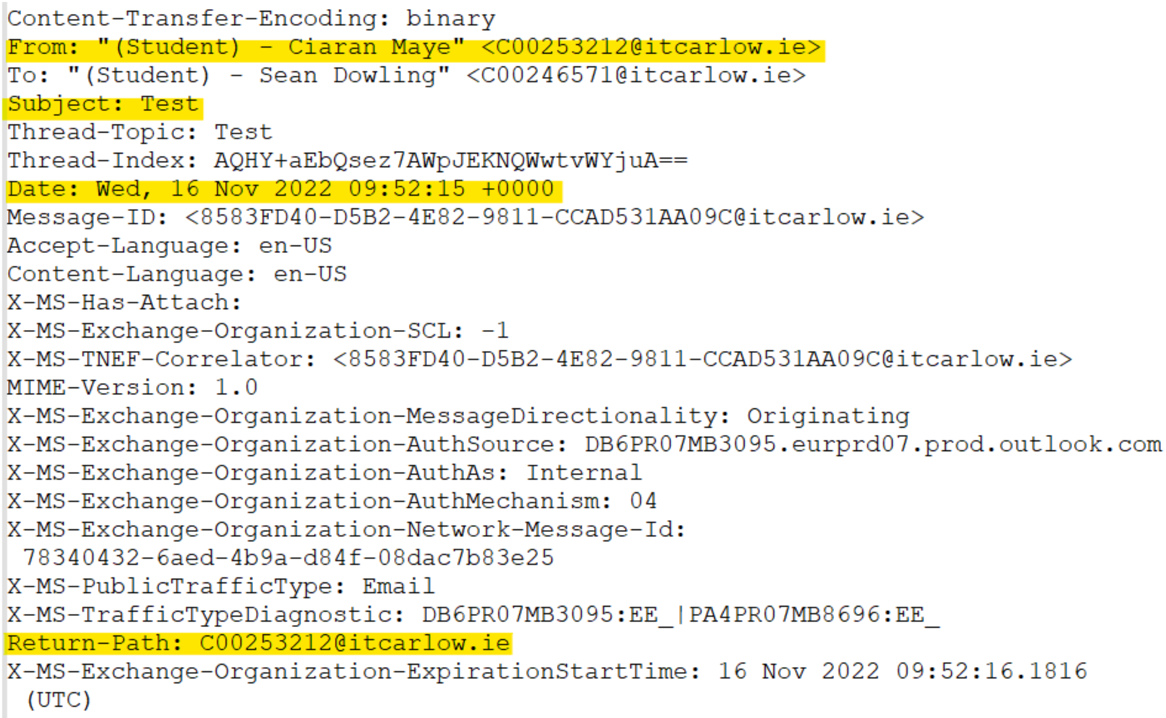
This may make the victim feel like they are in the wrong and sent the payment without batting an eyelid. Preventing emails like these are difficult as they may be legitimate emails, so ensuring I create the right program to ensure these scams are not fallen for, is an absolute must.

f) Conclusion

The ways described above are just some of the ways of detecting a phishing email. Although these will not be the primary focus of this project, prevent some of these will be. Getting a wider overview of all ways is always a good idea, as it will allow me to hopefully integrate other features into my project, if additional time will be available at the end.

7. Email Header Analysis

During my research, email headers contain a lot of information that goes unnoticed to many individuals. Vital information that is needed to determine if an email is a phish or not can be viewed here. The screenshot below shows information that can be used to see the time an email was sent at, the sender, subject, and the most important part, the return path. Attackers can manipulate this and send required information to a different email address. From this, I would be able to determine if an email is fraudulent or not, before even viewing the contents of the email. Within my project, I could incorporate a method of checking this before running any scans.



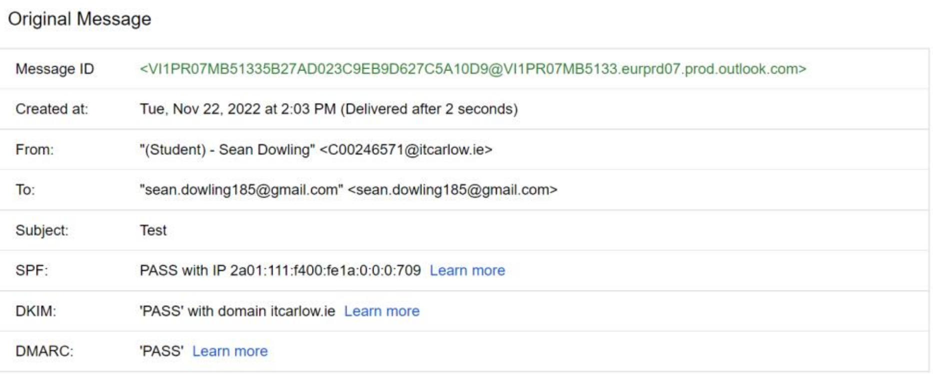
```
Content-Transfer-Encoding: binary
From: "(Student) - Ciaran Maye" <C00253212@itcarlow.ie>
To: "(Student) - Sean Dowling" <C00246571@itcarlow.ie>
Subject: Test
Thread-Topic: Test
Thread-Index: AQHY+aEbQsez7AWpJEKNQWwtvWYjuA==
Date: Wed, 16 Nov 2022 09:52:15 +0000
Message-ID: <8583FD40-D5B2-4E82-9811-CCAD531AA09C@itcarlow.ie>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <8583FD40-D5B2-4E82-9811-CCAD531AA09C@itcarlow.ie>
MIME-Version: 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource: DB6PR07MB3095.eurprd07.prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-MS-Exchange-Organization-Network-Message-Id:
 78340432-6aed-4b9a-d84f-08dac7b83e25
X-MS-PublicTrafficType: Email
X-MS-TrafficTypeDiagnostic: DB6PR07MB3095:EE_|PA4PR07MB8696:EE_
Return-Path: C00253212@itcarlow.ie
X-MS-Exchange-Organization-ExpirationStartTime: 16 Nov 2022 09:52:16.1816
 (UTC)
```

8. Email Authentication

There are three methods of email authentication:

- Sender Policy Framework (SPF)
- DomainKey Identified Mail (DKIM)
- Domain-Based Message Authentication Reporting and Conformance (DMARC)

In short, all three methods are ways Internet Service Providers (ISPs) authenticate email. Is the sender really who they say they are? (Paradigm, 2021). This will be a pivotal action in this project, verifying these will help greatly determine if an email is legitimate or not. Below is an example of each within Gmail.



Original Message

Message ID	<VI1PR07MB51335B27AD023C9EB9D627C5A10D9@VI1PR07MB5133.eurprd07.prod.outlook.com>
Created at:	Tue, Nov 22, 2022 at 2:03 PM (Delivered after 2 seconds)
From:	"(Student) - Sean Dowling" <C00246571@itcarlow.ie>
To:	"sean.dowling185@gmail.com" <sean.dowling185@gmail.com>
Subject:	Test
SPF:	PASS with IP 2a01:111:f400:fe1a:0:0:0:709 Learn more
DKIM:	'PASS' with domain itcarlow.ie Learn more
DMARC:	'PASS' Learn more

Figure 19: SPF, DKIM, DMARC

a) SPF

SPF, or Sender Policy Framework, is an email validation protocol designed to detect and block email spoofing. It allows mail exchangers to verify that incoming mail from a specific domain comes from an IP Address authorized by that domain's administrators (Paradigm, 2021). SPF will verify the sender to a publicly available list of senders that are approved to send emails from that domain. This will stop attackers using large corporations' domains like Amazon or YouTube for example.

b) DKIM

DKIM (Domain Keys Identified Mail) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature (DMARCAnalyzer, n.d.)

To create the signature, the sender uses the domain's private key to encrypt the message and create a hash. The recipient email server then uses the sender's public key to also encrypt the same components from the message. The recipient takes the encrypted result, a hash string, and compares it to the decrypted sender's hash. If both strings are the same, then DKIM validation passes (Proofpoint, n.d.)

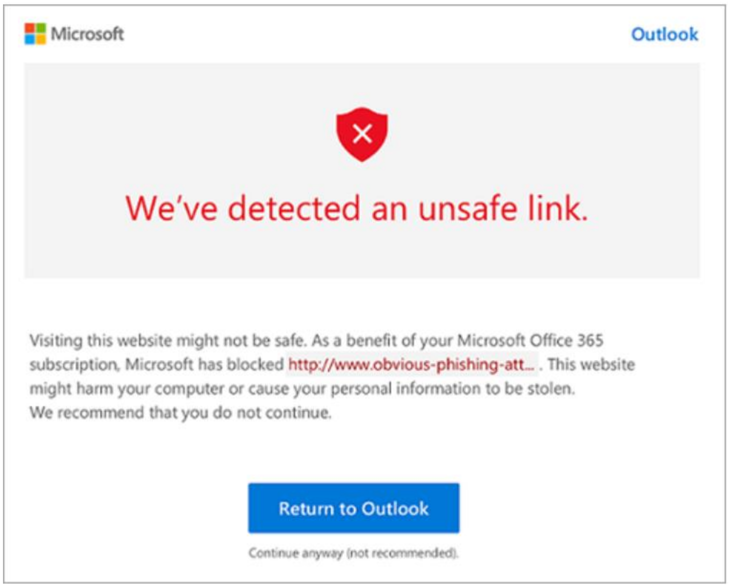
c) DMARC

It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email (DMARC, 2015).DMARC, like DKIM and SPF, can help prevent spoofing, it works hand in hand with the two. The DMARC will either pass or fail if the messages 'From:' header matches the sending domain.

9. Email Clients

I must decide which email client I will be using to host my tool. I have decided between Gmail and Outlook as I have the most experience using both. Gmail has many similar phishing detectors within its Workspace Marketplace, Outlook also offer similar tools. By default, Gmail displays warnings, and moves untrustworthy emails to the spam folder (Google, n.d.).

When you receive messages with links to web pages, Outlook.com checks whether the links are related to phishing scams or are likely to download viruses or malware onto your computer. If you click a link that is suspicious, you will be redirected to a warning page like the one below (Microsoft, 2021)



We've detected an unsafe link.

Visiting this website might not be safe. As a benefit of your Microsoft Office 365 subscription, Microsoft has blocked http://www.obvious-phishing-att... . This website might harm your computer or cause your personal information to be stolen. We recommend that you do not continue.

Figure 20. Outlook's Unsafe Link Detection (Microsoft, 2021)

From my research, I feel as if Outlook may be a strong contender to develop my tool as their detection system is of a good standard already.

10. Artificial Intelligence Vs. Programming Languages

I needed to decide whether I would use machine learning (Artificial Intelligence) to automatically do these checks or whether I would intend for the user to run a programme to detect if a link or attachment is malicious or not. From my initial thoughts, I feel as if using a programming language to determine the legitimacy of attachments would be easier for myself as I already have a good understanding of a few programming languages, compared to my knowledge of machine learning, in which I have a minimal understanding of. I think my knowledge of Java will yield me with the greatest results for this project. Upon further research I may reconsider using Python as most of the API's that I will discuss later work hand in hand with the language.

a) Java

The advantage of using Java is that I have had many years' experience using the language and its incorporated libraries. So, I feel being able to manipulate the code and make changes where necessary should be easier compared to using Python. There are also some libraries readily available for me to use to make my experience somewhat easier, like the Java Mail API, or if I want to output results in an Excel or PDF file, there are libraries like Apache PDFBox or JXLS.

b) Python

My knowledge of Python is much less than that of Java. But for the utilization of Application Programming Interface (API) keys I feel like Python will be a lot easier. There a wide range of API library tools that could be used, and seen as though APIs will be a large factor in this project, Python may be the better programming language to utilize.

c) Artificial Intelligence

Artificial Intelligence in itself is a very good method to detect phishing attacks. Basically, it uses data analysis and machine learning to examine metadata, content, context, and typical user behaviour (Gatefy, 2021). This allows the system to improve and learn from experience without having to manually programme and update code. Through my research, there have already been many approaches and applications made using machine learning. So, I feel the use of a programme using either Python or Java will be a better approach as I have not found any projects using these.

d) Conclusion

I feel there are still gaps when it comes to Artificial Intelligence, as it will never be 100% accurate, but by manually checking links and attachments, it will yield the best results for now. By manually running the programme, it also teaches the users to detect potential phish emails also without realizing.

11. API Utilization

API stands for Application Programming Interface. APIs let your product or service communicate with other products and services without having to know how they are implemented. This can simplify app development, saving time and money. When you are designing new tools and products—or managing existing ones—APIs give you flexibility; simplify design, administration, and use; and provide opportunities for innovation (RedHat, 2022). There are several phishing APIs available for use in real-time phishing email and website detection, giving you protection and a safe surfing experience. Below, I have researched APIs for malicious URLs and APIs for malicious attachments.

12. URL Checkers

To check if a URL is legitimate or not, I can utilize various APIs to determine the legitimacy of links. Below are some of these publicly available API's I may use.

- IsItPhish – This API evaluates 140 million URL syntax features.
- CheckPhish - Our AI and machine learning engine detects more than fourteen different types of scams across all top-level domains, including phishing, tech-support scams, counterfeiting, email phishing, and many more (CheckPhish, 2022).
- VirusTotal – Analyse suspicious files, domains, IPs, and URLs to detect malware and other breaches, automatically share them with the security community (VirusTotal, 2022)

13. Attachment Checkers

To check attachments, I will need to use other APIs to verify if they have been infected or not.

- VirusTotal allows users to analysis files also so I can utilize this tool.
- Kaspersky has a scan engine freely available also.
- MetaDefender Cloud – Is an advanced threat detection and prevention platform.

14. Existing Tools

There are already existing anti-phishing tools already on the market today. From my research of these tools, I may find innovative ideas that I may be able to incorporate into my project, while also learning and furthering my already thought of concepts. The tools below are mostly used by large organisations or businesses, thus making them unattainable to a single person. Through research I found some of the top anti-phishing tools and services on the market today, some that I have looked at in depth and taken ideas and concepts from are described below:

a) Avanan

By integrating via API, Avanan can analyse all historical emails to determine prior trust relations between sender and receiver, thereby increasing the likelihood of identifying user impersonation or fraudulent messages. With deep internal context, Avanan is the only solution that can truly stop Business Email Compromise (BEC) attacks (Avanan, 2022). This could be something I incorporate into my project. A warning could appear if it is the first time an email address is contacting you, raising suspicion for the user before reading the email. The main concern I have with Avanan though is their pricing, they offer three different monthly packages; Protect for €3.45 per month, Advanced Protect €4.41 per month, or Complete Protect for €5.76 per month. This is a good way to make money but for simple protection for a single user, this sort of money may not be in their budget.

b) Barracuda Sentinel

Unique API-based architecture gives Sentinel’s AI engine access to historical email data to learn each user’s unique communications patterns. The engine leverages multiple classifiers to map the social networks of every individual inside the company and identifies anomalous signals in message metadata and content (Barracuda, n.d.).Like Avanan, the use of AI to understand historical trends, like who are frequently communicating and who has never emailed you before, plays a large factor in phishing detection. Again, pricing is another large factor, Barracuda do not offer upfront prices, instead do it on a per user basis, which is immediately better than a flat rate per month like Avanan.

c) BrandShield

BrandShield provides a complete digital threat map, by monitoring the Internet including social media to detect phishing sites and pages, impersonation, and online fraud. Our takedown services are efficient and quick, transparent to you at any time from the system’s Threat Dashboard (BrandShield, 2022). This may be too advanced for this project as at the minute it will only be used for determining malicious links and attachments. BrandShield, compared to the previous two tools, does provide further tools like the dashboard mentioned, and includes innovative features like website duplication detector and takedown notices.

d) Cofense PDR

Upon detection, Cofense Protect immediately removes the phish from the user’s inbox and deactivates any malicious URLs found inline, found in an image or in any attachment. Cofense Protect immediately reduces the risk profile for your organization (Cofense, 2022). This is something I really want to implement into my tool. A way of moving potential phishes away from the user and deactivating the link, so no accidents occur. Cofense, unlike the others, provide a team you with a team of experts trained to identify, analyze, respond to, and remediate the phishing attacks that threaten your organization — on-demand, 24/7 (Cofense, 2022). This, in turn, makes their product one of the leading tool as often times, phishing emails may slip through the cracks and go unnoticed.

e) RSA FraudAction

The anti-phishing service is a managed service like what Cofense offers, and RSA brings capabilities like site shutdown, forensics, and optional countermeasures such as strategically responding to phishing attempts with planted credentials in order to track the attack chain and respond accordingly (Ferrill, 2022). This is something I would really like to involve in my project as well, but I can already tell this will be extremely hard and technical, so may be out of my range of knowledge. RSA provides similar services to the tools above, but also goes above and beyond and protects against social media threats and rogue mobile apps. In my research, none of the tools on this list have provided this service.

f) IRONSCALES

Through dynamic detection and analysis, IRONSCALES aims to augment your current email system by blocking, flagging, or even putting a banner on a potential phishing email. This seems like it could be along the lines my project will take, as it seems easier to implement. Like Cofense PDR, IRONSCALES offers a Human and Machine approach. This tool also integrates seamlessly with today’s modern email platforms.

g) Conclusion

The tools I have described above will definitely be an advantage when it comes to my project as I will be able to take bits and pieces from each and incorporate them all together. IRONSCALES approach of flagging or the use of banners will be the main approach I take for labelling malicious emails. Moving the malicious email into a separate folder feels like a great idea also by Cofense PDR, as it will deter users from accidentally opening the links or downloading attachments. Understanding the common communications users make can also be incorporated into the project, a warning may appear that this is the first time an user is contacting you.

15. Testing

To understand if my project is running the way I intend it to, I must test it. Through my research, I have found tools that allow you to send phishing emails to an email and gives feedback on results. The tools I will use to test will be:

a) GoPhish

With the use of this tool, I will be able to make my own phishing emails and send them to a testing email and understand where I may be able to improve my tool and where I have done successful checks. GoPhish updates results automatically. Using the UI, you can view a timeline for each recipient, tracking email opens, link clicks, submitted credentials, and more (GoPhish, 2022). This will be very good to enable me to understand what if the links were opened and even if the email was opened.

b) King-Phisher

King-Phisher is another tool I can utilize in my project. King Phisher features an easy to use, yet very flexible architecture allowing full control over both emails and server content. King Phisher can be used to run campaigns ranging from simple awareness training to more complicated scenarios in which user aware content is served for harvesting credentials (IMPACT, n.d.)

16. Conclusion

Through my research, the need for a simple tool like a phishing detection tool has never been higher. The ones on offer at the moment are good in aspects, but most cost a lot of money are designed for large corporation use instead of thinking of the needs of a single user. My tool will be designed for this purpose.

I will be using Python to write the script for this programme as through my research, it is designed in such a way that will benefit me and has a wide range of libraries ready to use. I also feel as if I will be out of my depth using machine learning to complete this project as my knowledge is limited in that field. I will avail of the wide range of APIs online also, using a mix of all of them if possible, this will allow me to make the best determination and compare results to other APIs. I will also check for common domain names are spelt correctly. To test if my tool is working correctly I will use both GoPhish and King Phisher, the benefits of using two tools is that I will be able get a wider range of results and be able to make better judgements.

Glossary

API	Application Programming Interface
AI	Artificial intelligence
BEC	Business Email Compromise
DNS	Domain Name System
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
Email	Electronic Mail
ISP	Internet Service Provider
PDR	Phishing Detection and Response
SPF	Sender Policy Framework
URL	Uniform Resource Locator

Bibliography

Ahola, M., 2021. *The 8 types of phishing attack that could target your business.* [Online]
Available at: https://blog.usecure.io/types-of-phishing-attack
[Accessed 18 November 2022].

Avanan, 2022. *Anti-Phishing Software.* [Online]
Available at: https://www.avanan.com/
[Accessed 22 November 2022].

Barracuda, n.d. *Barracuda Sentinel.* [Online]
Available at: https://www.barracuda.com/resources/Barracuda_Sentinel_DS_US
[Accessed 22 November 2022].

BrandShield, 2022. *We Find and Remove Online Phishing.* [Online]
Available at: https://www.brandshield.com/products/anti-phishing/
[Accessed 22 November 2022].

CheckPhish, 2022. *Automate Your Phishing Detection & Response with Real-Time Detection.* [Online]
Available at: https://checkphish.ai/checkphish-api/
[Accessed 22 November 2022].

Chipeta, C., 2022. *What is Business Email Compromise (BEC)? And How To Prevent It.* [Online]
Available at: https://www.upguard.com/blog/business-email-compromise
[Accessed 17 November 2022].

Cofense, 2022. *Managed Phishing Detection and Response Services.* [Online]
Available at: https://cofense.com/product-services/phishing-defense-services/
[Accessed 20 November 2022].

Cofense, 2022. *Real-Time Anti-Phishing Solution.* [Online]
Available at: https://cofense.com/product-services/cofense-protect/
[Accessed 22 November 2022].

Crane, C., 2020. *Re-Hashed: Phishing Email Examples — The Best & Worst.* [Online]
Available at: https://www.thesslstore.com/blog/phishing-email-examples-the-best-worst/
[Accessed 23 November 2022].

Cyren, 2021. *Anatomy of a Malware Attack: Emails with Password-Protected Files.* [Online]
Available at: https://www.cyren.com/blog/articles/anatomy-of-an-attack-password-

protected-files-attached-to-emails
[Accessed 23 November 2022].

DMARC, 2015. *What is DMARC?.* [Online]
Available at: https://dmarc.org/
[Accessed 21 November 2022].

DMARCAnalyzer, n.d. *What is DKIM?.* [Online]
Available at: https://www.dmarcanalyzer.com/dkim/
[Accessed 21 November 2022].

EMSI, 2018. *Beware: New wave of malware spreads via ISO file email attachments.* [Online]
Available at: https://www.emsisoft.com/en/blog/32373/beware-new-wave-of-malware-spreads-via-iso-file-email-attachments/
[Accessed 24 November 2022].

Ergos, n.d. *5 Types of email attachments you should look out for.* [Online]
Available at: https://ergos.com/business/5-types-of-email-attachments-you-should-look-out-for/
[Accessed 21 November 2022].

Ferrill, T., 2022. *10 top anti-phishing tools and services.* [Online]
Available at: https://www.csoonline.com/article/3575080/9-top-anti-phishing-tools-and-services.html
[Accessed 22 November 2022].

Fightcybercrime, n.d. *The Basics of Business Email Compromise.* [Online]
Available at: https://fightcybercrime.org/scams/business/email-compromise-bec/
[Accessed 17 November 2022].

Fortinet, 2021. *What Is a Worm Virus?.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/worm-virus
[Accessed 20 November 2022].

FRSecure, 2020. *Phishing Attack Examples and How to Protect Against Them.* [Online]
Available at: https://frsecure.com/blog/phishing-attack-examples/
[Accessed 16 November 2022].

Fruhlinger, J., 2020. *Ransomware explained: How it works and how to remove it.* [Online]
Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
[Accessed 20 November 2022].

Gatefy, 2021. *How artificial intelligence and machine learning fight phishing.* [Online]
Available at: https://gatefy.com/blog/how-ai-and-ml-fight-phishing/
[Accessed 22 November 2022].

Google, n.d. *Advanced phishing and malware protection.* [Online]
Available at: https://support.google.com/a/answer/9157861?hl=en
[Accessed 21 November 2022].

GoPhish, 2022. *Open-Source Phishing Framework.* [Online]
Available at: https://getgophish.com/
[Accessed 23 November 2022].

IMPACT, n.d. *DATASET DETAILS.* [Online]
Available at: https://www.impactcybertrust.org/dataset_view?idDataset=1319
[Accessed 20 November 2022].

Irwin, L., 2022. *5 ways to detect a phishing email – with examples.* [Online]
Available at: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
[Accessed 21 November 2022].

Johansen, A. G., 2020. *What is a Trojan? Is it a virus or is it malware?.* [Online]
Available at: https://us.norton.com/blog/malware/what-is-a-trojan
[Accessed 18 November 2022].

Kaspersky, n.d. *What is Adware? – Definition and Explanation.* [Online]
Available at: https://www.kaspersky.com/resource-center/threats/adware
[Accessed 19 November 2022].

Malwarebytes, 2021. *Keylogger.* [Online]
Available at: https://www.malwarebytes.com/keylogger
[Accessed 20 November 2022].

Malwarebytes, 2021. *Spyware.* [Online]
Available at: https://www.malwarebytes.com/spyware
[Accessed 18 November 2022].

Meskauskas, T., 2021. *Fantom Ransomware.* [Online]
Available at: https://www.pcrisk.com/removal-guides/10418-fantom-ransomware
[Accessed 23 November 2022].

Meskauskas, T., 2022. *Do not enter credentials on websites opened via the ShareFile Attachment email.* [Online]
Available at: https://www.pcrisk.com/removal-guides/17884-sharefile-attachment-email-scam
[Accessed 23 November 2022].

Microsoft, 2021. *Advanced Outlook.com security for Microsoft 365 subscribers.* [Online]
Available at: https://support.microsoft.com/en-us/office/advanced-outlook-com-security-for-microsoft-365-subscribers-882d2243-eab9-4545-a58a-b36fee4a46e2
[Accessed 21 November 2022].

Microsoft, n.d. *Protect yourself from phishing.* [Online]
Available at: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44
[Accessed 15 November 2022].

Micro, T., 2022. *What Are the Different Types of Phishing?.* [Online]
Available at: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
[Accessed 16 November 2022].

Montagnese, A., 2016. *WHALING, CEO FRAUD, BUSINESS EMAIL COMPROMISE… TARGETED SPEAR PHISHING ATTACKS CONTINUE TO TROUBLE BUSINESS.* [Online]
Available at: https://www.mailguard.com.au/blog/whaling-ceo-fraud-business-email-compromise-targeted-spear-phishing-attacks-continue-to-trouble-businesses
[Accessed 21 November 2022].

Northwestern, n.d. *Diving into Scam Emails at Northwestern.* [Online]
Available at: https://www.it.northwestern.edu/security/phishing/index.html
[Accessed 17 November 2022].

Paradigm, S., 2021. *What Are DMARC, DKIM, and SPF?.* [Online]
Available at: https://www.shiftparadigm.com/insights/what-are-dmarc-dkim-and-spf/
[Accessed 21 November 2022].

Proofpoint, n.d. *What Is DKIM?.* [Online]
Available at: https://www.proofpoint.com/us/threat-reference/dkim
[Accessed 21 November 2022].

RedHat, 2022. *What is an API?.* [Online]
Available at: https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces
[Accessed 22 November 2022].

Rosenthal, M., 2022. *Must-Know Phishing Statistics: Updated 2022.* [Online]
Available at: https://www.tessian.com/blog/phishing-statistics-2020/

Rosenthal, M., 2022. *Must-Know Phishing Statistics: Updated 2022.* [Online]
Available at: https://www.tessian.com/blog/phishing-statistics-2020/

Rosenthal, M., 2022. *Must-Know Phishing Statistics: Updated 2022.* [Online]
Available at: https://www.tessian.com/blog/phishing-statistics-2020/
[Accessed 15 November 2022].

Rosenthal, M., n.d. *Must-Know Phishing Statistics: Updated 2022.* [Online].

SecureList, 2022. *HTML attachments in phishing e-mails.* [Online]
Available at: https://securelist.com/html-attachments-in-phishing-e-mails/106481/
[Accessed 23 November 2022].

securityscorecard, 2021. *14 Types of Phishing Attacks and How to Identify Them.* [Online]
Available at: https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them
[Accessed 15 November 2022].

Spanning, 2022. *Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year.* [Online]
Available at: https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/#:~:text=Phishing%20attacks%20are%20responsible%20for,breaches%20occur%20due%20to%20phishing.

Spanning, 2022. *Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year.* [Online]
Available at: https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/#:~:text=Phishing%20attacks%20are%20responsible%20for,breaches%20occur%20due%20to%20phishing.
[Accessed 15 November 2022].

Spiceworks, 2018. *New spam targeting O365 accounts (credential harvesting).* [Online]
Available at: https://community.spiceworks.com/topic/2172100-new-spam-targeting-o365-accounts-credential-harvesting
[Accessed 15 November 2022].

Taibo, G., 2020. *Weaponized Disk Image Files: Analysis, Trends and Remediation.* [Online]
Available at: https://www.crowdstrike.com/blog/weaponizing-disk-image-files-analysis/
[Accessed 21 November 2022].

TerraNovaSecurity, 2022. *WHAT IS VISHING?.* [Online]
Available at: https://terranovasecurity.com/what-is-vishing/
[Accessed 17 November 2022].

Tripwire, 2020. *New Smishing Campaign Using USPS as Its Disguise.* [Online]
Available at: https://www.tripwire.com/state-of-security/new-smishing-campaign-using-usps-as-its-disguise
[Accessed 21 November 2022].

Vadesecure, 2020. *Pretexting: 5 Examples of Social Engineering Tactics.* [Online]
Available at: https://www.vadesecure.com/en/blog/pretexting-5-examples-of-social-engineering-tactics
[Accessed 18 November 2022].

Veracode, 2021. *Rootkit: What is a Rootkit?.* [Online]
Available at: https://www.veracode.com/security/rootkit
[Accessed 19 November 2022].

VirusTotal, 2022. *VirusTotal API v3 Overview.* [Online]
Available at: https://developers.virustotal.com/reference/overview
[Accessed 22 November 2022].