Swinburne University of Technology

Faculty of Science, Engineering and Technology

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code : COS30015 Unit Title : IT Security

Assignment number and title : Practical Project Due date : **31 October 2021 23:59**

Lab group : Class 9 Tutor : Daniel Hood Lecturer : (Sky) Yuantian Miao

Family name : Hudson Identity no : 102533320

Other names : Cobie

To be completed if this is an INDIVIDUAL ASSIGNMENT
I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature : C.Hudson

To be completed if this is a GROUP ASSIGNMENT
We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number	Name	Signature

Marker's comments:

Total Mark:_________________

Extension certification:

This assignment has been given an extension and is now due on ___________________________

Signature of Convener:___________________________________ Date: / 2021

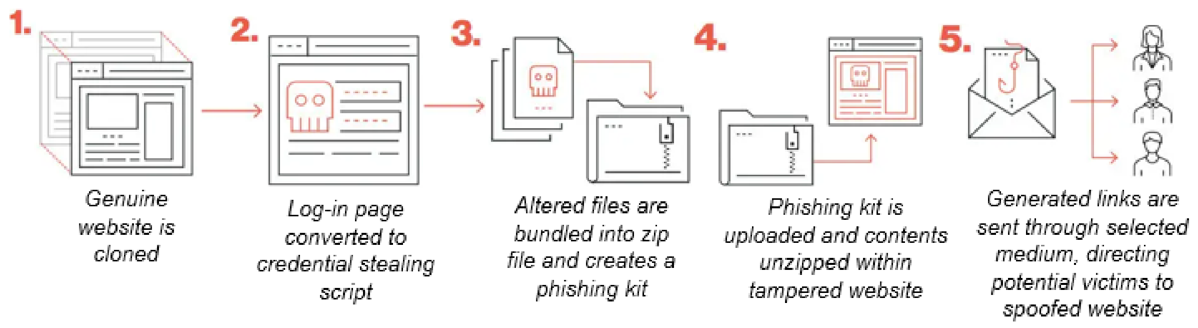
Practical Project : Topic 01 (Phishing)

Criteria 1 : Planning and Justification

A type of social engineering attack, phishing involves sending fraudulent mediums to deceive inattentive recipients. Resembling a malicious link or download attachment contained within a selected medium, phishing attacks entices victims into believing its legitimate. Often leading to devastating outcomes such as unauthorized purchases, identity theft, embezzlement, or installation of malware. Consequently, phishing is often directed towards corporate or governmental networks when conducting larger scale attacks. Through directing victims to a fabricated clone of a genuine website, any logged credentials are collected through a script and forwarded back to the assailant. This is then used to access any corresponding accounts or secured data, leading to the exposure of sensitive information. Organizations succumbing to such an attack often undergo severe financial loss in addition to a decline in market share, reputation, and consumer trust. Ultimately, phishing scams are a serious adherence to susceptible victims and companies, as reflected through the many successful attacks in the past :

- Occurring in 2016, this momentous phishing attack ensured the assailants gained access to Hillary Clintons campaign managers Gmail password
- Known as the “fappening” attack, the distribution of crude celebrity photos was leaked into the public due to a series of lucrative phishing attempts
- Resulting in financial loss, employees at the University of Kansas unknowingly provided a phishing scam with sensitive information of their paycheck deposits

Consequently, more than a third of all breaches within the past year have involved phishing, according to the 2021 Verizon Data Breach Investigations Report. Also stating an 11% increase compared to last year, phishing scams have become more prevalent each passing day. Through expanding availability of accessible tools and templates, phishing scams can be accomplished with ease. Also known as phishing kits, this allows cyber criminals to launch phishing operations with nominal technical expertise. Through bundling phishing website resources that are installed over a server, a malicious link is generated and sent to potential victims through email, text, or voice communication. Available on the dark web and crowd-sourced lists located on Phishtank and OpenPhish, contact lists and phishing kits can be effortlessly obtained. Similar in design, phishing kits have been analyzed assiduously by Duo Labs, concluding the common anatomy of these malicious tools as referenced below.


1.
Genuine website is cloned
2.
Log-in page converted to credential stealing script
3.
Altered files are bundled into zip file and creates a phishing kit
4.
Phishing kit is uploaded and contents unzipped within tampered website
5.
Generated links are sent through selected medium, directing potential victims to spoofed website

Moreover, phishing scams may introduce routine techniques to disguise their malicious intent. Through email address impersonation and masking egregious links with trustworthy URLs by shortening or converting to foreign character sets, assailents can broaden the chance to swindle potential victims. Consequently, there are certain approaches phishing scammers can implement. Depending on their motive, phishing attempts can vary in contents and purpose when seeking to bamboozle recipients. Typically two key approches are considered when conducting phishing campaigns :

- *Retrieving sensitive information.* Aimed at misleading individuals into exposing meaningful data – generally a username and password to ensure assailants can breach secured accounts. Commonly associated with dispatching emails adapted to mimic a message from a credible bank are spammed to millions of people. This ensures attackers advance their odds of contacting a recipient associated the corresponding bank. In this circumstance, victims would click the provided link and be directed to a malicious replication of the banks webpage. Ultimately, if convinced the correlating victims would provide their user credentials and allow attackers access to their bank account.
- *Installation of malware.* Aimed at deceiving individuals into infecting their device with malware. Typically known to be "soft-targeted" – they may be directed towards the HR sector of an organization, providing an attachment that implies to be career applicants resume. Often resembling a .zip file or Microsoft Office document, these attachments contain embedded malicious code.

Although not always targeted, phishing scams are commonly mass mailed to millions of potential victims in order to convince them into providing their credentials to spurious replications of familiar websites. As indicated by Ironscales, through monitoring over 50,000 fabricated login pages, they concluded the leading brands attackers utilized was PayPal (22%), Microsoft (19%), Facebook (15%), eBay (6%) and Amazon (3%). However, some phishing attempts may intend to steal login credentials or infect the devices of explicit high value targets. Consequently, attackers will devote more resources and effort to circumvent these recipients to reap the potential rewards. Dependent on preferred mediums and overall objective, cyber criminals have an extensive selection of approaches to attempt phishing scams, for instance :

- Mass Market Emails – The most familiar type of phishing scam, this involves attackers sending an abundance of emails to potential victims. Often relying on basic email spoofing techniques to appear as a trusted source
- Spear phishing – Fixated on governmental or high authority organizations, this phishing scam is directed towards distinct targets. Requiring extra resources and exertion to craft convincible ploys.
- Whaling – Requiring the most effort, this phishing approach involves the explicit targeting of high value recipients. Comprising of executive or CEO officials of an organization, deceiving these targets ensures attackers are rewarded with a range of worthwhile compensations.

- Business Email Compromise (BEC) – Through the impersonation of a CEO, this exploitive email fraud aims at deceiving other employees of the company.
- Clone Phishing – Involves the formulation of identical replications of credible emails with the only discrepancy being a malicious link or attachment. Through imitation the attacker may also clone corresponding webpages with a spoofed domain.
- Vishing – Short for "Voice Phishing", this technique relies on victims possessing a device with communication services. Typically, recipients would receive a voice message pretending to be a convincible institution.
- Smishing – Short for "SMS Phishing", this approach also relies on the possession of a device with texting services. Generally, victims would obtain a text message disguised as an authentic source.
- Snowshoeing – Involves forwarding numerous spam messages via a range of domains and IP addresses. Through limiting each IP address to a few messages, this ensures reputation or volume-based spam filtering automation cannot identify and thwart these malicious phishing scams.

Evidently, phishing is an immensely broad topic with many tools and resources at an attackers disposal. Referred to as Blackeye, this accessible attacking tool allows users to effortlessly accomplish phishing scams. Through the combination of ngrok and serveo technology, a replicated instance of a credible website can be constructed. Providing an array of popular brands, the user can select from a collection of 40+ distinct and credential stealing login pages. Additionally, through combining the Social Engineering Toolkit, malicious generated links can be sent to designated recipients to hopefully embezzle their personal data. Although other more advanced and robust options exist, a majority of these are only available through the dark web or illegally obtained. Similar to other publicly available tools, Blackeye is the most feature full, visually pleasing, and reliable offering. Providing more than 10+ options and relevant brands, Blackeye ensures attackers can launch an ample collection of phishing campaigns. Overall, other comparable tools are negligible when measured against the practical opportunities that Blackeye presents. As a result, this prolific tool will be thoroughly documented within the PayPal phishing scenario discussed below and further examined in Criteria 2.

- PayPal Phishing Scam – Typically a phishing scammers purpose when launching an attack commonly emanates from a desire of money. Consequently, this scenario will fixate on replicating a convincing PayPal email using both plain text and HTML schemes. Additionally, both mass mailing and spear phishing techniques will be conveyed, along with any other optional preferences that may exist. Ultimately, Blackeye in conjunction with the Social Engineering Toolkit will ensure a convincing PayPal webpage is constructed and successfully provided to designated victims through a malicious link over email. As a result, the victim will be directed to this fictitious website, enter their login credentials, and provide us their username / password to access any relevant PayPal accounts.

Consequently, there exists very few means of defending against these lucrative phishing scams. However, applications such as Mimecast or Office 365 offer automated techniques that mark unknown / spamming domains as a threatening sender. This will ensure any relevant emails are relocated to a recipients spam with a sizeable red exclamation mark, while also disabling any links and images provided. Although this solution seems plausible, attackers can effortlessly avoid this adherence by creating fresh email accounts and altering their network context. Subsequently, security awareness training can overcome a majority of these challenges. Although this training suite is commonly applied in the workplace, any individual can employ these practices. As a result, through the education of phishing attacks, potential victims could effectively avoid succumbing to these scams, for instance :

- Training – Phishing alertness begins with enlightening employees about its adverse nature, empowering them to identify and expel any phishing attempts. Depending on the mode of delivery, initial training may be distributed via documentation, video, meetings, classroom environment or a combination of these elements.
- Simulation – Simulated renditions of phishing campaigns can further reinforce an employee's understanding of the risks, indirectly bettering workforce resilience. Existing in many forms such as mass phishing, spear phishing and whaling, these simulations create a harmless environment for learning.
- Reinforcement – Experience is key to training, such that if an employee where to click on a link or attachment within a simulated phishing email, possible risks should be communicated to them. The implementation of a "training page" could also emphasize the threats of phishing and how to handle suspected emails.
- Improvement – Through an analysis of results, a multitude of conclusions can be made. Ranging from effective attack types or vulnerable teams, this data can be documented and interpreted to improve the overall training process.

Evidently, implementing these workplace practices can ensure individuals don't fall for phishing attempts. However, a variety of indications can also be considered when uncovering a suspected phishing scam as attackers commonly :

- Creating a sense of urgency
- Use spoofed emails addresses and credible resources
- Appear to be threatening or enticing
- Include suspicious links or attachments
- Make grammatical errors

Evidently, security awareness training is remarkably impactful when disputing against phishing attempts. Overall, due to its interactive and informative approach, security awareness training is the leading defense tool against phishing campaigns. Also given that very few tools exist, this is the most effective alternative. As a result, through implementing the various techniques and indications above, the defending scenario will comprise of dissecting any ensuing elements within our attacking tool outcomes. This will be discussed further in Criteria 2.

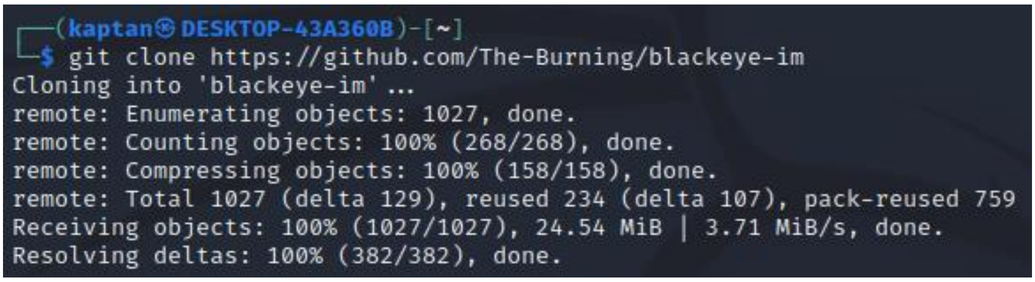
Criteria 2 : Documentation and Application

Attacking Tool Documentation –

Blackeye GitHub : https://bit.ly/3pPioz4

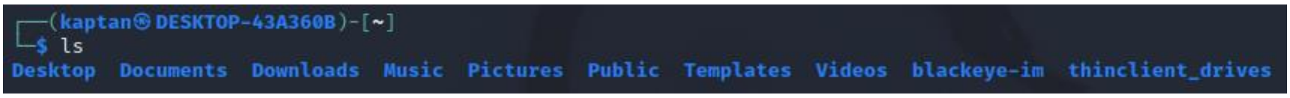
Blackeye Installation

- ➢ Entering “git clone” into the terminal, followed by the Blackeye GitHub link, this will automatically clone and package the tool in your current location



```
┌──(kaptan㉿DESKTOP-43A360B)-[~]
└─$ git clone https://github.com/The-Burning/blackeye-im
Cloning into 'blackeye-im' ...
remote: Enumerating objects: 1027, done.
remote: Counting objects: 100% (268/268), done.
remote: Compressing objects: 100% (158/158), done.
remote: Total 1027 (delta 129), reused 234 (delta 107), pack-reused 759
Receiving objects: 100% (1027/1027), 24.54 MiB | 3.71 MiB/s, done.
Resolving deltas: 100% (382/382), done.
```

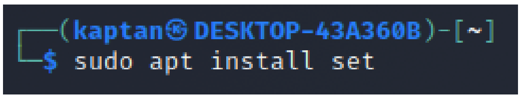
- ➢ This can be confirmed using the “ls” command



```
┌──(kaptan㉿DESKTOP-43A360B)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  blackeye-im  thinclient_drives
```

SET Installation

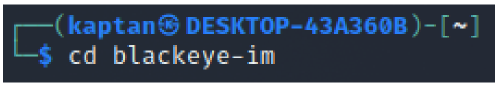
- ➢ Entering “sudo apt install set” will download any required assets and automatically install the tool within your virtual environment
- ➢ Be sure to agree with any appealed questions



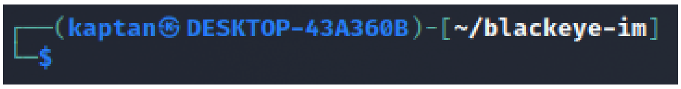
```
┌──(kaptan㉿DESKTOP-43A360B)-[~]
└─$ sudo apt install set
```

Blackeye Tool

- ➢ Launching the tool will require users to access the folder withholding its contents
- ➢ Entering “cd” followed by the folder you want to access will change your current directory

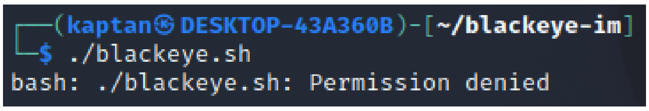


```
┌──(kaptan㉿DESKTOP-43A360B)-[~]
└─$ cd blackeye-im
```

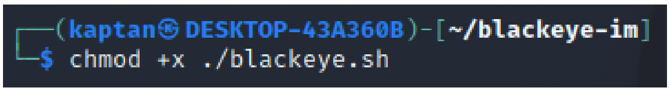


```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$
```

- ➢ Entering “./blackeye.sh” will execute the shell script
- ➢ However, if user permission is denied, this can be easily fixed using the following command “chmod +x ./blackeye.sh”

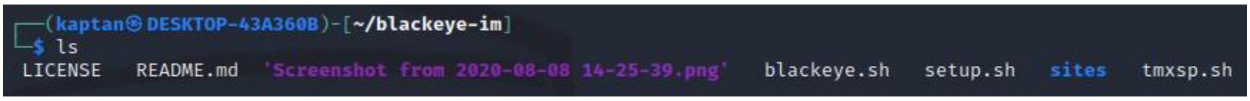


```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$ ./blackeye.sh
bash: ./blackeye.sh: Permission denied
```

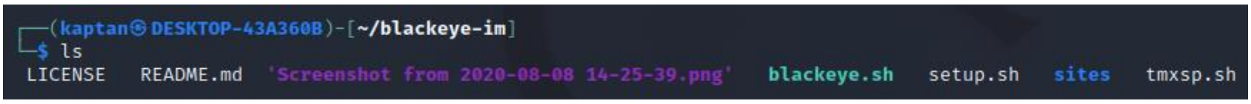


```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$ chmod +x ./blackeye.sh
```

- After any permission changes “blackeye.sh” text should now be turquoise
- Before and after permission modifications are reflected below

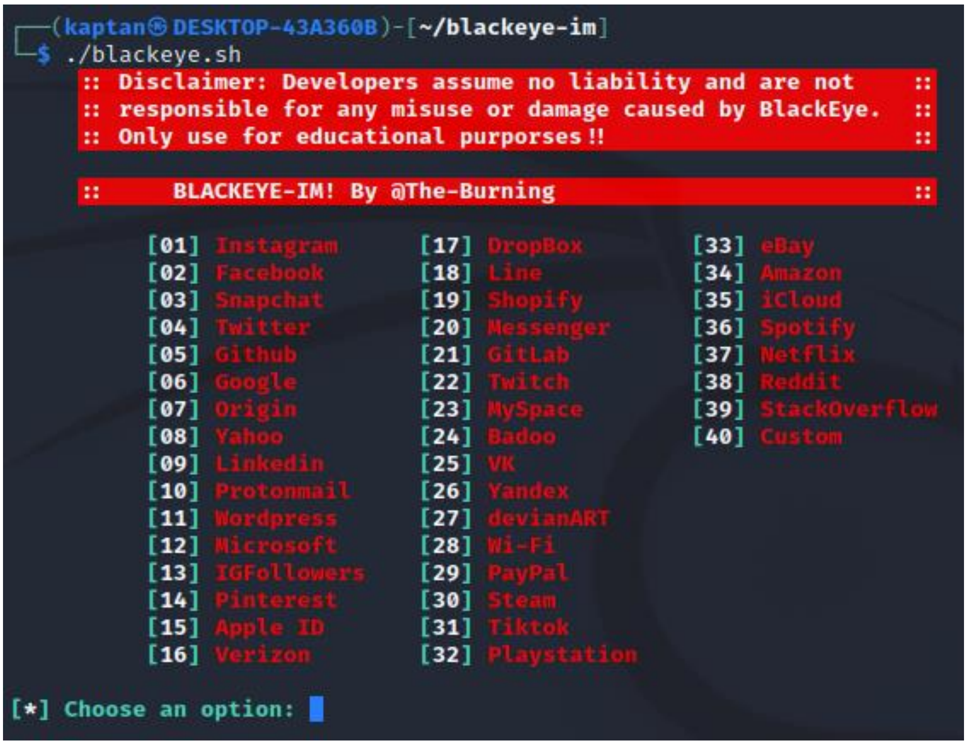


```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$ ls
LICENSE   README.md  'Screenshot from 2020-08-08 14-25-39.png'   blackeye.sh   setup.sh   sites   tmxsp.sh
```



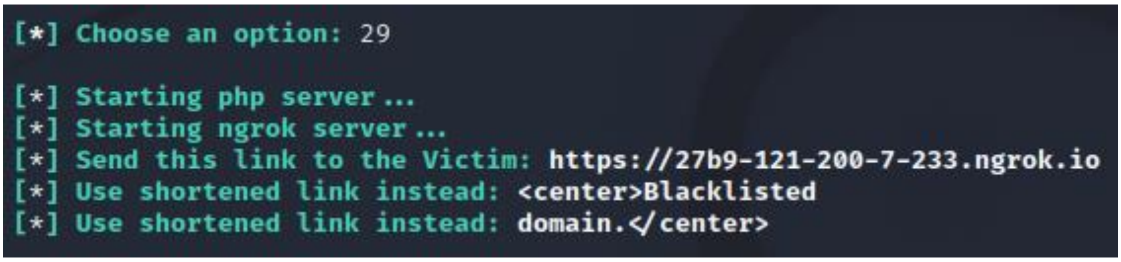
```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$ ls
LICENSE   README.md  'Screenshot from 2020-08-08 14-25-39.png'   blackeye.sh   setup.sh   sites   tmxsp.sh
```

- Consequently, entering the “./blackeye.sh” command should successfully execute
- This will display a collection of options the user can select from



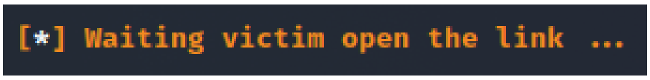
```
┌──(kaptan㉿DESKTOP-43A360B)-[~/blackeye-im]
└─$ ./blackeye.sh
      :: Disclaimer: Developers assume no liability and are not   ::
      :: responsible for any misuse or damage caused by BlackEye. ::
      :: Only use for educational purposes!!                      ::

      ::      BLACKEYE-IM! By @The-Burning                        ::

           [01] Instagram        [17] DropBox         [33] eBay
           [02] Facebook         [18] Line            [34] Amazon
           [03] Snapchat         [19] Shopify         [35] iCloud
           [04] Twitter          [20] Messenger       [36] Spotify
           [05] Github           [21] GitLab          [37] Netflix
           [06] Google           [22] Twitch          [38] Reddit
           [07] Origin           [23] MySpace         [39] StackOverflow
           [08] Yahoo            [24] Badoo           [40] Custom
           [09] Linkedin         [25] VK
           [10] Protonmail       [26] Yandex
           [11] Wordpress        [27] devianART
           [12] Microsoft        [28] Wi-Fi
           [13] IGFollowers      [29] PayPal
           [14] Pinterest        [30] Steam
           [15] Apple ID         [31] Tiktok
           [16] Verizon          [32] Playstation

[*] Choose an option:
```

- Since our goal is to access a victims PayPal account, by entering “29” this will ensure a replicated rendition of the official PayPal login screen is constructed
- Consequently, this will generate a link that directed to this fabricated webpage
- However, users may choose any of these options, depending on their goals



```
[*] Choose an option: 29

[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim: https://27b9-121-200-7-233.ngrok.io
[*] Use shortened link instead: <center>Blacklisted
[*] Use shortened link instead: domain.</center>
```

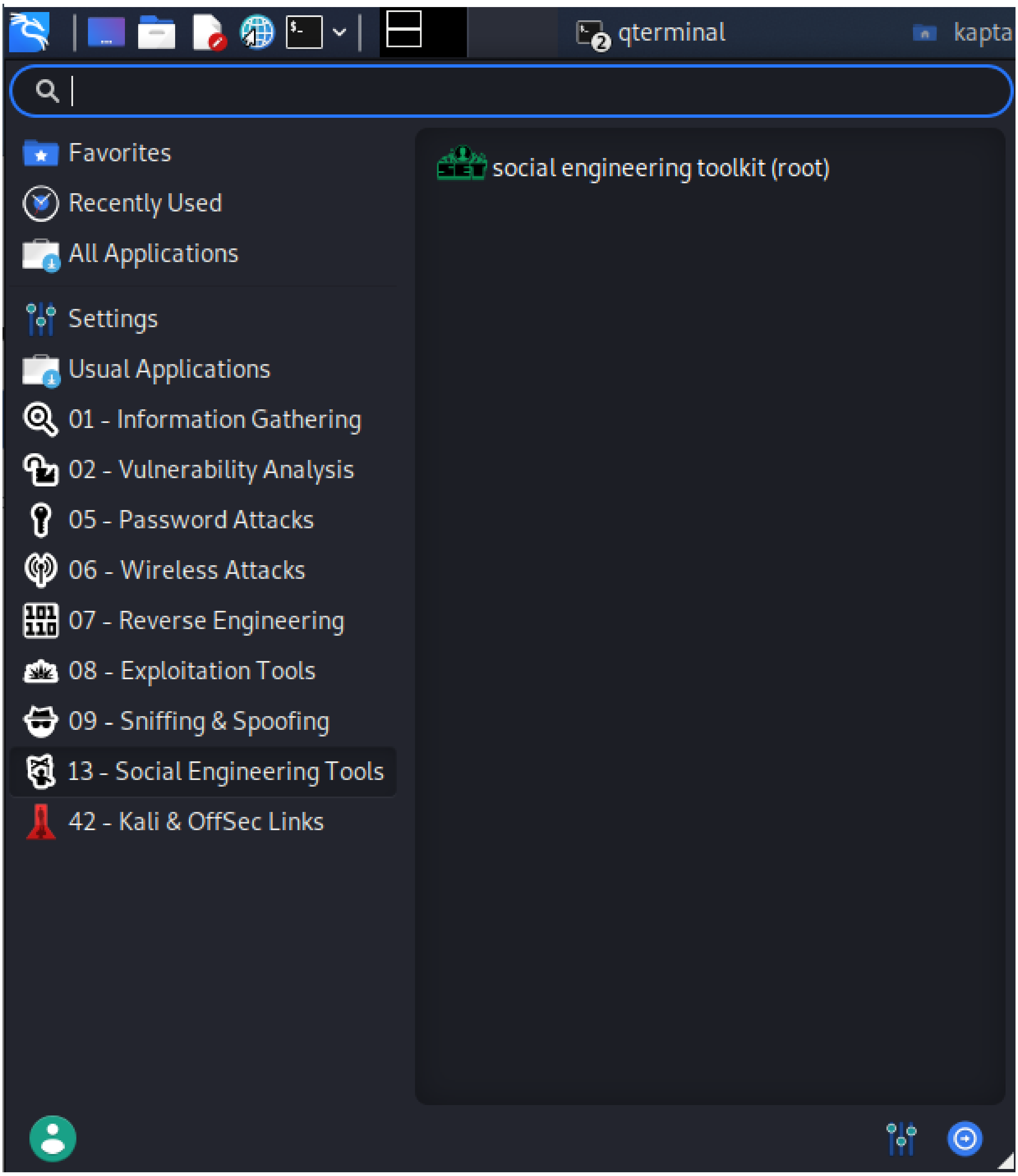
- As a result, the application will wait for any oblivious recipients that click the link



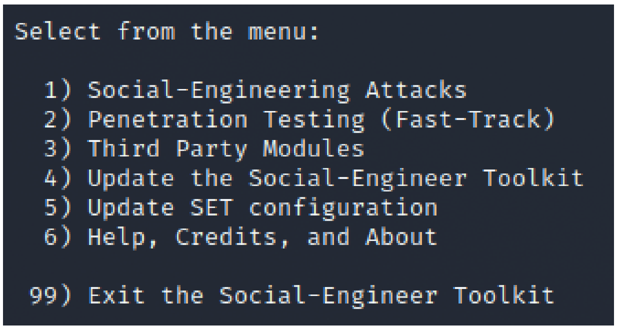
```
[*] Waiting victim open the link ...
```

SET Tool

- Subsequently, after the malicious link is prepared to be sent out, the SET tool has to be used email potential victims
- Accessed by navigating to the top left icon in the corner, this should resemble the Kali Linux logo
- The supposed tool should be located somewhere within this window
- If unable to locate this tool, use the search bar to distinguish its existence

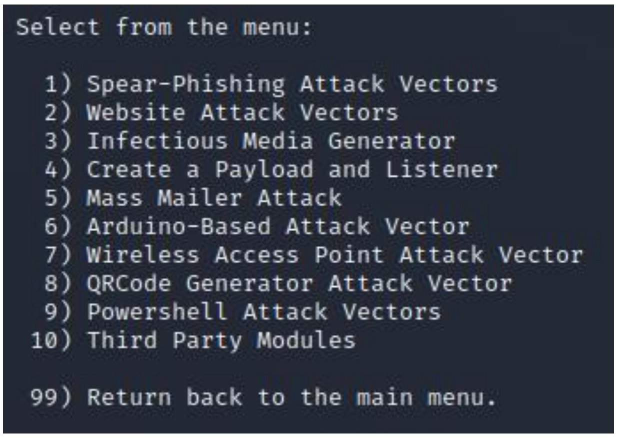


- Once the application is launched, a terminal will appear displaying some options
- Since we plan to send an email, we will select option “1”



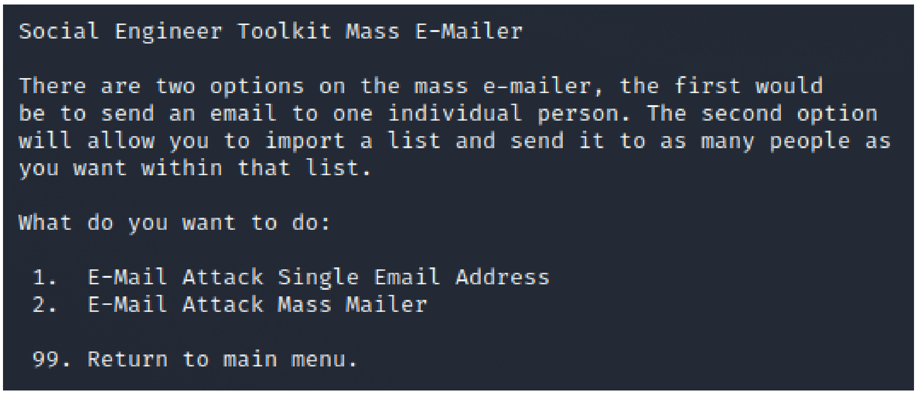
```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

- This will present a series of social engineering attacks that we can conduct
- Consequently, option “5” will be selected as this involves sending emails



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```

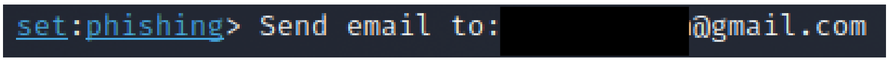
- Subsequently, two options will be shown
- In this case we can choose between a spear-phish attack or mass mail
- Option “1” will request a single email to be input while option “2” will require the user to specify a path to a text file containing a list of emails, both resulting in sending emails to the appointed recipients



```
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

 1.  E-Mail Attack Single Email Address
 2.  E-Mail Attack Mass Mailer

 99. Return to main menu.
```

Option 1 :

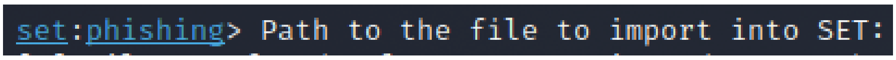
- Enter designated target email



```
set:phishing> Send email to:[redacted]@gmail.com
```

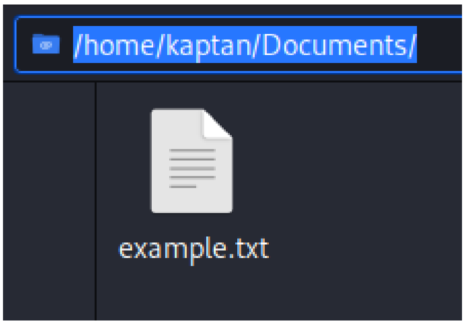
Option 2 :

- Indicate path leading to text file containing list of emails

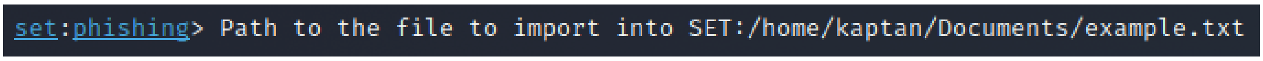


```
set:phishing> Path to the file to import into SET:
```

- Path can be found by accessing the location of the corresponding file and copying the path appending it with the file name

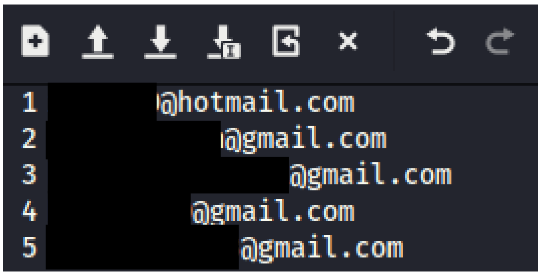


/home/kaptan/Documents/



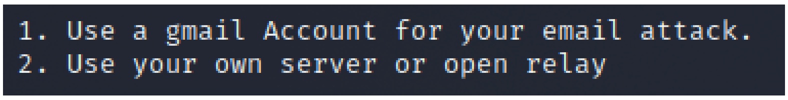
```
set:phishing> Path to the file to import into SET:/home/kaptan/Documents/example.txt
```

- This list must be formatted so each line is dedicated to a single email



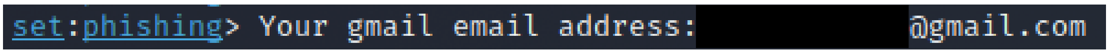
```
[redacted]@hotmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
[redacted]@gmail.com
```

- Once either of the two options are fulfilled, two options will be displayed
- Since we don’t require an email sever in this scenario, option “1” will be selected



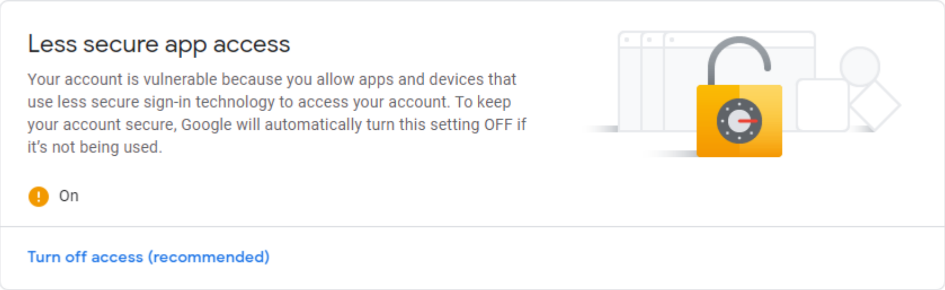
```
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
```

- As a result, a sender Gmail address must be input
- This email usually involves using a fresh email account to avoid identification



```
set:phishing> Your gmail email address:[redacted]@gmail.com
```

- Additionally, ensure that this account has “less secure app access” turned on
- This ensures the SET tool has full access to your account



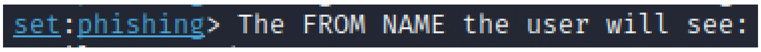
Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account. To keep your account secure, Google will automatically turn this setting OFF if it’s not being used.

On

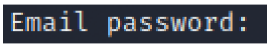
Turn off access (recommended)

- After inputting the provided Gmail, the “FROM NAME” will need to be specified



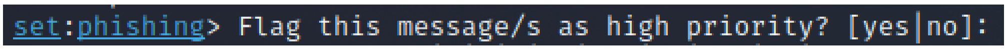
```
set:phishing> The FROM NAME the user will see:
```

- Subsequently, the provided email will also require the corresponding password



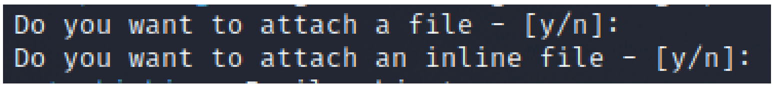
```
Email password:
```

- Concluding previous steps, a series of questions will be presented
- First of which will request if the message is high priority (sent to inbox or spam)

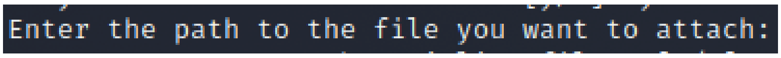


```
set:phishing> Flag this message/s as high priority? [yes|no]:
```

- Secondly, users can attach a file and / or inline file
- Path must be provided

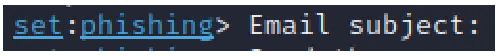


```
Do you want to attach a file - [y/n]:
Do you want to attach an inline file - [y/n]:
```



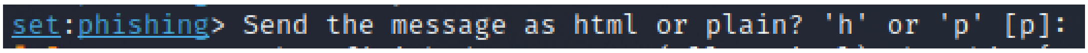
```
Enter the path to the file you want to attach:
```

- After which the remaining content within the email is specified
- With the email subject being specified first

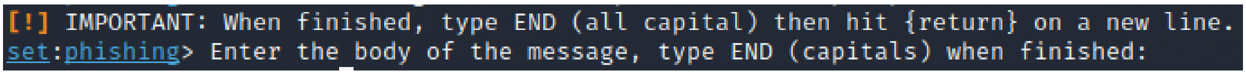


```
set:phishing> Email subject:
```

- Additionally, the body text type must be specified
- Either using a plain text or html scheme, this can drastically alter the way an email is presented to potential victims
- Moreover, closing out the body of text with “END” will indicate the end of the emails content and no more text lines are needed
- The generated link from the Blackeye tool should be included in this body text



```
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:
```



```
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
```

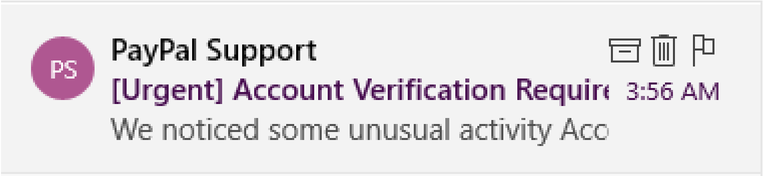
- As a result, previously determined recipients are sent an email of provided content, satisfying any decisions made throughout this process

Attacking Tool Application

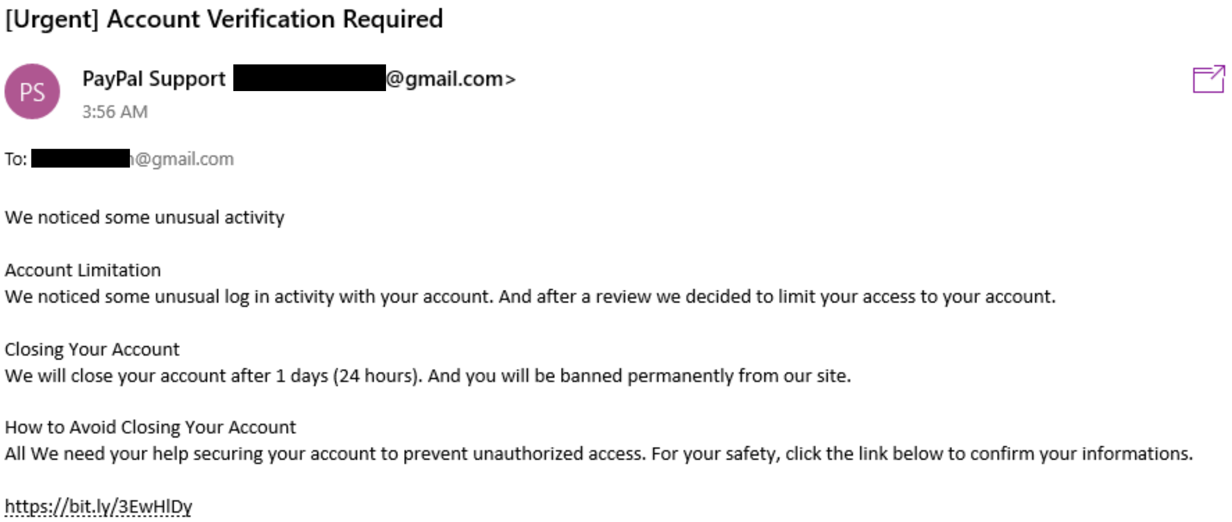
Upon completing each documentation step, two distinct schemes can be potentially constructed. Ranging in authenticity, plain text or HTML structured emails are noticeably diverse in appearance and credibility. Although plain text requires much less effort than its HTML counterpart, crafting the more convincing option should always be prioritized. Consequently, both approaches will implement common practices involved with PayPal scams and incorporate content previously applied in these phishing attempts.

<u>Plain Text Approach</u>

- ➢ Involves simply providing the necessary preferences and content throughout the many processes of each tool
- ➢ Through link shortening using Bitly the link will be further disguised



PayPal Support
[Urgent] Account Verification Require 3:56 AM
We noticed some unusual activity Acc



[Urgent] Account Verification Required

PayPal Support [redacted]@gmail.com>
3:56 AM

To: [redacted]@gmail.com

We noticed some unusual activity

Account Limitation
We noticed some unusual log in activity with your account. And after a review we decided to limit your access to your account.

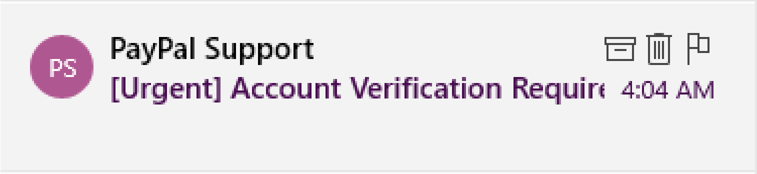
Closing Your Account
We will close your account after 1 days (24 hours). And you will be banned permanently from our site.

How to Avoid Closing Your Account
All We need your help securing your account to prevent unauthorized access. For your safety, click the link below to confirm your informations.

https://bit.ly/3EwHlDy

HTML Approach

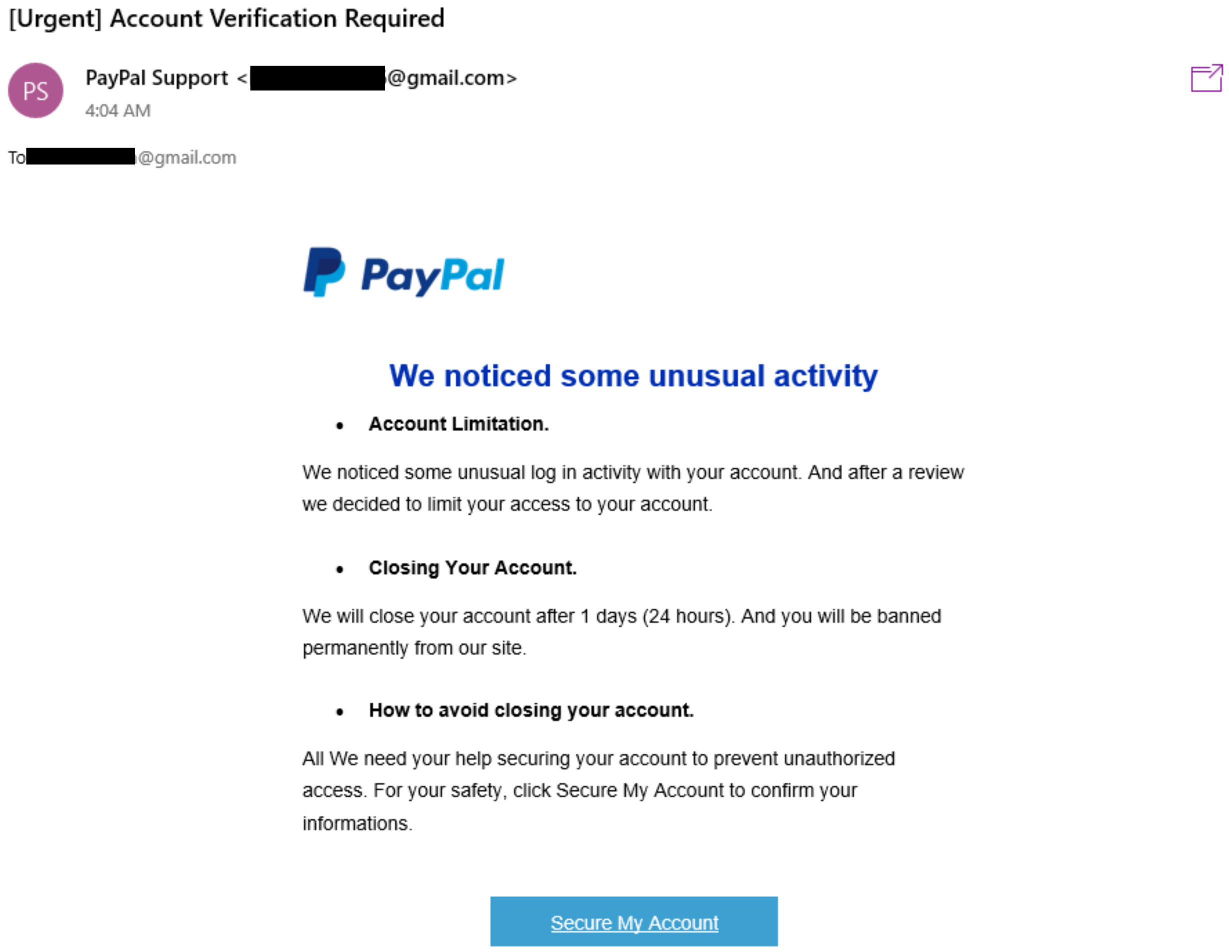
- Through using online templates, a convincing email can be constructed
- The only altercation will be the link connected to the “Secure My Account” button



PS

PayPal Support

[Urgent] Account Verification Requir 4:04 AM



[Urgent] Account Verification Required

PS

PayPal Support <[redacted]@gmail.com>

4:04 AM

To [redacted]@gmail.com

We noticed some unusual activity

- **Account Limitation.**

We noticed some unusual log in activity with your account. And after a review we decided to limit your access to your account.

- **Closing Your Account.**

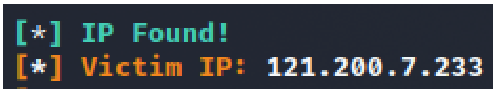
We will close your account after 1 days (24 hours). And you will be banned permanently from our site.

- **How to avoid closing your account.**

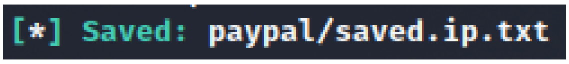
All We need your help securing your account to prevent unauthorized access. For your safety, click Secure My Account to confirm your informations.

Results

- ➢ As a result, if the recipient is successfully deceived and opens the link, we will obtain the victims IP address
- ➢ This will be saved in a text file



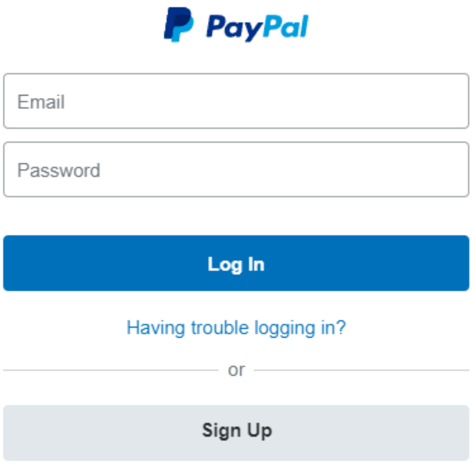
```
[*] IP Found!
[*] Victim IP: 121.200.7.233
```



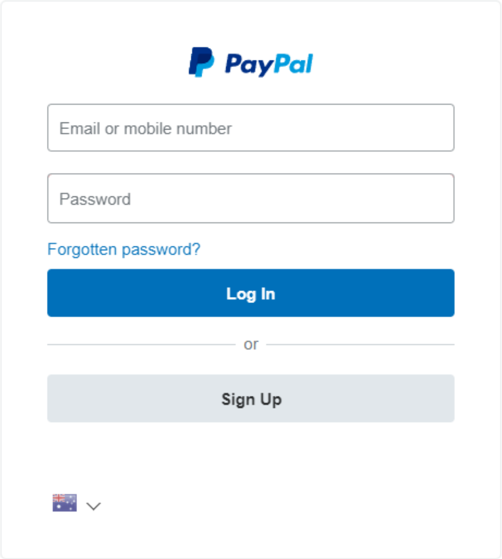
```
[*] Saved: paypal/saved.ip.txt
```

- ➢ Subsequently, the victim will be presented with a replication of the official website

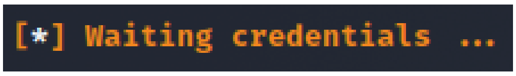
Fake :



Real :

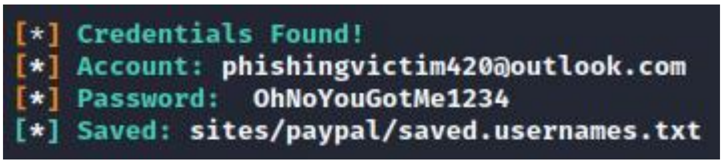


- ➢ If the victim is still convinced and enters their login credentials, the tool will wait for this action and collect any sensitive data



```
[*] Waiting credentials ...
```

- ➢ This will be in the form of a username and password
- ➢ This will also be saved in a text file

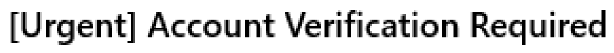


```
[*] Credentials Found!
[*] Account: phishingvictim420@outlook.com
[*] Password:  OhNoYouGotMe1234
[*] Saved: sites/paypal/saved.usernames.txt
```

Defending Tool –

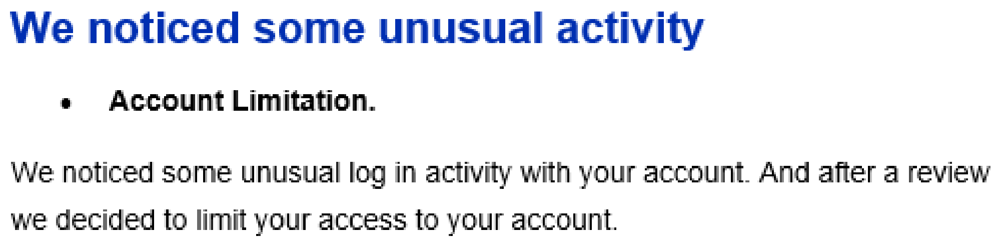
As discussed in Criteria 1, there are many indications when attempting to uncover a phishing attempt. By analyzing the resulting webpage from Blackeye and the constructed HTML email from the Social Engineering Toolkit, we can successfully distinguish any evidence to confirm it’s a phishing scam

Sense of Urgency



[Urgent] Account Verification Required

Commonly implemented, attackers will create a sense of urgency. In this case, the words “Urgent” is surrounded by square brackets to emphasize its importance, followed by a critical process to be carried out “Account Verification Required”. Additionally, other approaches may be considered such as capitalizing or bolding the content within the email. Attackers will ensure the entirety of a phishing scam creates imperative scenarios that may be relevant to recipients. Moreover, attackers may indicate that there has been unusual activity, further reinforcing that the recipient should be concerned.

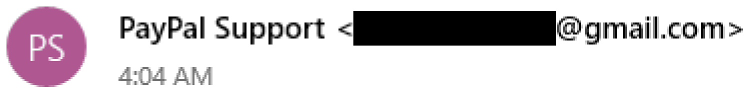


We noticed some unusual activity

- **Account Limitation.**

We noticed some unusual log in activity with your account. And after a review we decided to limit your access to your account.

Spoofed Contact

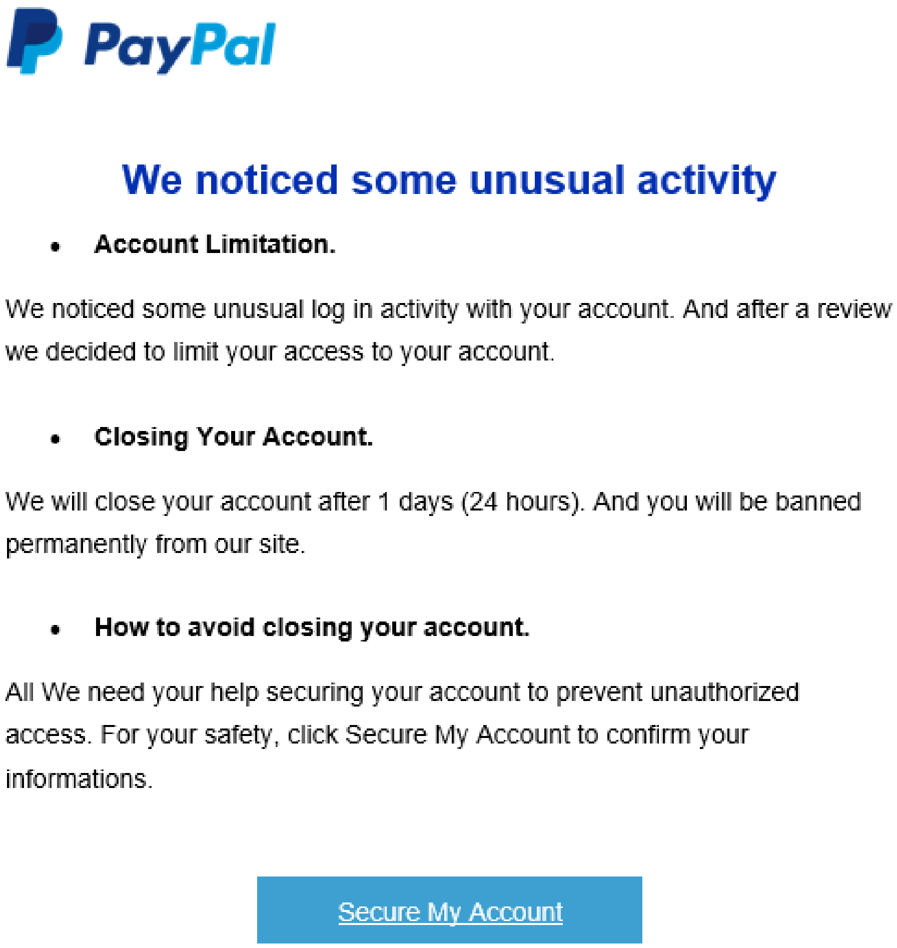


PayPal Support <[redacted]@gmail.com>
4:04 AM

Generally, attackers will often impersonate a credible source. By changing the FROM NAME and masking sender details to a plausible origin, this can further solidify a victims trust. Evidently, this example is impersonating to be “PayPal Support”.

Spoofed Resources

Additionally, attackers may employ corresponding resources to mimic a legitimate contact. Ranging from brand logos, font, color, and structure, this can increase believability. Subsequently, this example uses the PayPal logo and commonly used fonts, colors, and structure relevant in a PayPal email.



We noticed some unusual activity

- **Account Limitation.**

We noticed some unusual log in activity with your account. And after a review we decided to limit your access to your account.

- **Closing Your Account.**

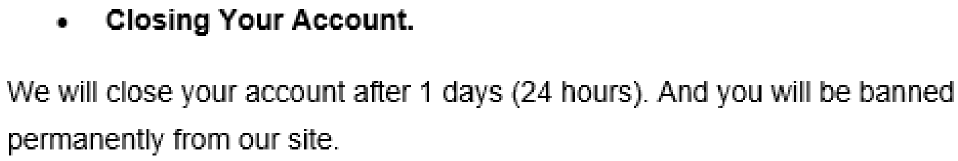
We will close your account after 1 days (24 hours). And you will be banned permanently from our site.

- **How to avoid closing your account.**

All We need your help securing your account to prevent unauthorized access. For your safety, click Secure My Account to confirm your informations.

Threats

Attackers may also try to seem threatening or enticing when attempting a phishing scam. This is achieved by affirming the recipient may lose something valuable. Additionally, some phishing scams may blackmail their victims to entice them to do what they require. Consequently, this email states an account closure will occur with 24 hours.

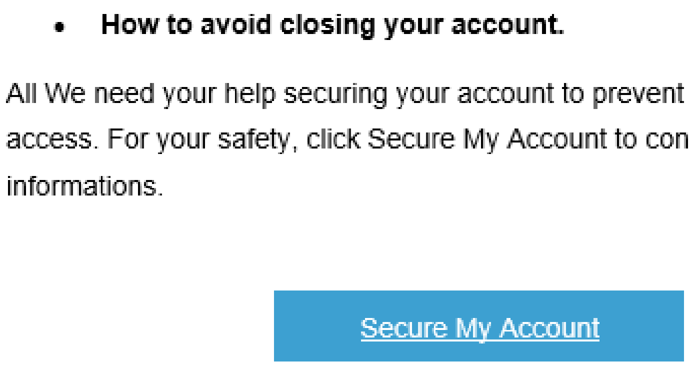


- **Closing Your Account.**

We will close your account after 1 days (24 hours). And you will be banned permanently from our site.

Suspicious Links or Attachments

Phishing scammers will almost always include a link or attachment in an attempt to steal their data or install malware. This could include a hyperlink or button that directs victims to a credential stealing webpage, additionally attachments can act as a link to this webpage too. As a result, attackers will convince the victim to click the link in order to resolve any threats or fulfillments that have been presented.

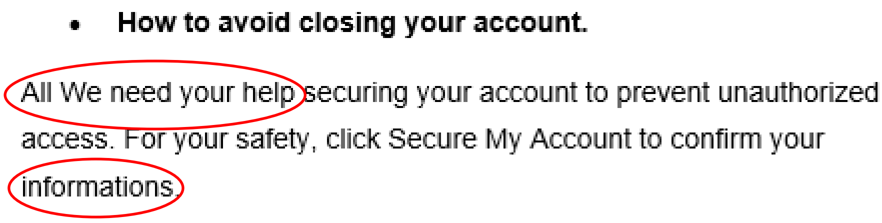


- **How to avoid closing your account.**

All We need your help securing your account to prevent unauthorized access. For your safety, click Secure My Account to confirm your informations.

Grammatical Errors

Typically, inexperienced phishing assailants may make grammatical errors within the context of the email. Ranging from spelling to punctuation, this is a common indication the email could be fabricated. For instance, some grammatical errors were made in the last block of text, this is circled in red below.



- **How to avoid closing your account.**

All We need your help securing your account to prevent unauthorized access. For your safety, click Secure My Account to confirm your informations.

Results

Overall, through a combination of the above indications within a training environment, this would ensure potential victims can effectively avoid succumbing to a phishing attempt.

Criteria 3 : Analysis

Evidently, conducting a phishing scam is overly effortless to carry out, requiring minimal technical skill to be successful. Through accessible tools, templates and resources, phishing campaigns can be constructed swiftly. As shown in Criteria 2, an accurate rendition of a PayPal email and webpage can be simply crafted using publicly available tools, allowing anyone to operate a convincing phishing scam. As indicated in Criteria 1, phishing scams are the most common cybercrime due to the accessible nature of phishing assets.

Consequently, combining tools such as Blackeye, Social Engineering Toolkit and Unlayer, attackers can mimic popular brands in order to deceive victims into providing sensitive information, for instance :

- Blackeye – Constructs accurate renditions of over 40 credible webpages, generating a link that can be sent to potential victims.
- Social Engineering Toolkit – Formulates and organizes an email that can be manipulated to resemble a credible source relevant to the recipient.
- Unlayer – Drag and drop email template website.

Subsequently, through merging the skills of these tools, attackers can conveniently create convincing phishing attempts. Unfortunately, phishing scams will become more authentic and advanced as attackers continue to improve upon similar tools. Emanating future challenges, defending against the many adherences of phishing will sustain, becoming more progressive and relevant each day. Referred in Criteria 1, victims will continue to yield against the efforts that phishing scammers present. However, as attacking tools become more meticulous, defending tools such as security awareness training and automated tools ensures potential victims don’t succumb to the devastating outcomes of phishing. Organizations and typical recipients can employ these defensive strategies. Ranging from automated tools to security awareness training, future and present challenges can be somewhat diminished. As show in Criteria 2, an assortment of indications can be accounted when uncovering if an email is a phishing scam. Commonly stumbling into these discernible signals, attackers are unable to avoid a majority of them. Although, phishing assailants can formulate convincible depictions of credible sources, with the appropriate training, whether individual or conducted within a company, phishing scams can be effectively distinguished. As discussed in Criteria 1 and 2, both attacking / defending tools are associated with a wide range of challenges, impacts and considerations when measured against each other.

Criteria 4 : Evaluation

In conclusion, phishing scams will continue to be a reality, developing into more precise extortions as attackers gradually escalate in skill and amount, as tools like Blackeye and Social Engineering Toolkit will allow anyone to commit a potential phishing scam. While defending tools such as Office 365 and Mimecast continue to struggle, security awareness training can effectively prevent possible victims succumbing to these manipulative scams. Although there are many challenges and threats that victims will continue to endure, the implementation of defending approaches will at the very least alleviate any concerns. Evidently, the resulting culmination of both attacking and defending tools in Criteria 2 effectively confirms that opposing tools can nullify any arising challenges or threats they present.

References

Rapid7. (2019). *Phishing Awareness Training: Simulating Phishing Attacks*. [online] Available at: https://bit.ly/2Y3VzfK.

Duo Security. (n.d.). *Phish in a Barrel: Hunting and Analyzing Phishing Kits at Scale*. [online] Available at: https://duo.sc/3pPkXRS.

www.cbsnews.com. (n.d.). *The phishing email that hacked the account of John Podesta*. [online] Available at: https://cbsn.ws/3Cz7DEF.

TechCrunch. (n.d.). *Prosecutors find that "Fappening" celebrity nudes leak was not Apple's fault*. [online] Available at: https://tcrn.ch/3CvG52V.

Wichita and Bryan (2020). *KU employees fall victim to phishing scam, lose paychecks*. [online] Available at: https://bit.ly/3GFGJgL.

Verizon Business. (n.d.). *2021 Data Breach Investigations Report*. [online] Available at: https://vz.to/2ZFQnik.

Rashid, F.Y. (2020). *8 types of phishing attacks and how to identify them*. [online] Available at: https://bit.ly/3GEL587.

Trend Micro. (n.d.). *What are the different types of phishing?* [online] Available at: https://bit.ly/3BwykbZ.

Fruhlinger, J. (2020). *What is phishing? How this cyber attack works and how to prevent it*. [online] Available at: https://bit.ly/3q7HXvJ.

Imperva (2019). *What is phishing | Attack techniques & scam examples | Imperva*. [online] Available at: https://bit.ly/3pTmQwY.

blog.usecure.io. (n.d.). *The Three Stages Of a Phishing Attack - Bait, Hook And Catch*. [online] Available at: https://bit.ly/3pRkjTS.

IRONSCALES. (2020). *Fake Login Pages Spoof Over 200 Brands*. [online] Available at: https://bit.ly/3jUFmkD.

Gendre, A. (n.d.). *Phishing Awareness Training: 8 Things Your Employees Should Understand*. [online] Available at: https://bit.ly/3BvcC80.

chrisda (n.d.). *Anti-phishing protection - Office 365*. [online] Available at: https://bit.ly/3kcqiPJ.

McShanag, D. (n.d.). *Don't fall for this new PayPal scam in the holiday rush*. [online] Available at: https://bit.ly/3pTQLVS.