International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Email Phishing Attack Vector Examination and Experimentation

Micah Roble[1], Munther Abualkibash[2]
[1]School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, United States-48197
[2]School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, United States-48197

Abstract– *The Internet has evolved from its humble beginnings to be a place full of different kinds of communication services. Email paved the way for instant messaging which revolutionized the concept of communication around the world. Due to the ever-evolving nature of the internet, it has led to offensive capabilities of the cyber landscape rapidly developing over the course of the last 30 years. This change has led to cyber security professionals developing new ways to combat old and emerging cyber threats. Common attempts at mitigating cyber threats have included the implementation of encryption, the use of strong password policies, and the implementation of strong access controls. However, cyber threats continue to cause issues for security professionals resulting in the need for new ways for security professionals to defend their organizations and themselves. One form of cyber threat that is largely determined by human error however, is phishing. Phishing scams can target specific individuals or an entire organization resulting in sensitive information being revealed if a user is not careful. Malicious actors can attempt to infiltrate a user's computer, steal information, or install malicious software all through a simple and dangerous phishing email or text. This has led to security professionals taking action and bringing attention to the dangers of phishing. For the improvement of the security of online communications, experiments were conducted to reveal how an attacker might conduct a phishing scam. The phishing scams tested included the use of a keylogger over email, and a credential stealing email. Research was also done on how a user might attempt to mitigate possible phishing scams and actions that can be taken to detect phishing scam. This research hopes to inform security professionals on the seriousness of phishing scams and how to combat them.*

Keywords– *Cyber security, Email, Phishing scam, Encryption, Access control.*

I. INTRODUCTION

Advancements in the internet have led to the further advancement of online threats such as hackers, NGOs, cybercriminals, and other security vulnerabilities. In the past, hacking was considered a very intelligent field that only a select few knew how to do. Hackers were seen as figures that could take over a computer with just a few keystrokes. Time however has changed due to the revolutionary capabilities of the internet. Many today can learn about hacking by watching tutorials, buying books specifically for hacking, taking courses directed at ethical hacking, or even just learning about hacking from acquaintances. The art of offensive security/hacking has grown into an active war into who can discover a vulnerability first and either patch it or exploit it. Many hackers today are amateurs and hobbyists who can use tools found online to assist the facilitation of hacking. Due to the expansion of technology, security professionals are constantly assessing the safety of organizations. One form of offensive security that hackers utilize often is phishing. By utilizing this method, malicious actors and hackers can sometimes obtain critical information that can cripple an organization. This paper contains 6 sections including the Introduction. Section II will describe the brief history and concept of email. Section III describes information related to phishing, in IV I will go over phishing experiments. Section V will discuss phishing and email security concepts that can be used by security professionals to help mitigate potential phishing threats to an organization. Lastly, section VI will be the conclusion.

II. EMAIL

There are numerous different ways for one to communicate online. Apps like Whatsapp allow millions to connect. Facebook, Instagram, and many other forms of communication also exist that allow for people across the world to message each other. One of the oldest forms of online communications is email. There are many email providers in the modern age. Whether it be yahoo, google, comcast, hotmail, or others, email has truly revolutionized the ability to communicate with one another. Currently it is estimated that over 2.6 billion active users and over 4.6 billion email accounts are in operation. Email arguably is the most important and widely used communications medium on the internet [1].

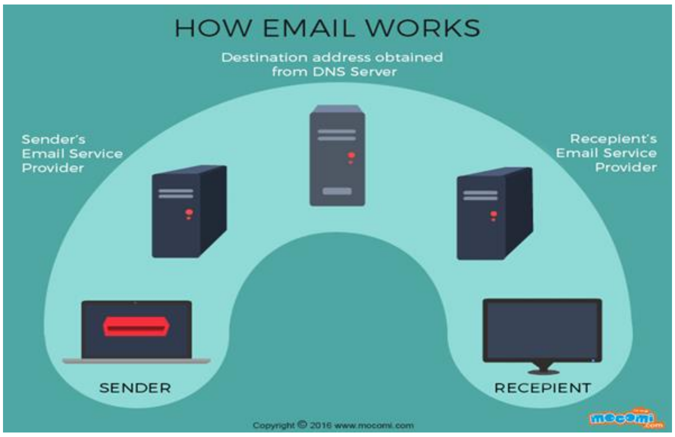

HOW EMAIL WORKS
Destination address obtained from DNS Server
Sender's Email Service Provider
Recepient's Email Service Provider
SENDER
RECEPIENT
Copyright © 2016 www.mocomi.com
mocomi.com

Fig. 1. Email Fundamentals

Email has become an indispensable part of global communication and commerce. The first form of electronic mail messaging began in 1971, invented by Ray Tomlinson by creating ARPANET's networked email system. As email evolved, email hosting sites began to form as a way for users to store and better manage emails that were sent to them. This eventually led to organizations like AOL, yahoo, and others. Email capabilities have expanded past the simple form of text messaging [2]. One can send videos, pictures, Excel files, documents, and in malicious cases viruses.

III. PHISHING

Phishing is usually described as an attempt by a hacker or cyber criminal to lure a user into divulging personal, financial, or business information through a maliciously crafted email or virus. Sensitive information that is sought after includes birthdays, credit card numbers, social security numbers, passwords, and other personal identifiable information. According to some estimates, over 156 million phishing emails are sent everyday, usually resulting in more than 80,000 victims opening the emails [3].

Historically phishing can be traced back to the beginning of instant messaging on the internet. Malicious users on AOL began using spoof email accounts to create the impression that they were AOL employees. By impersonating AOL employees these malicious actors would message AOL users asking for personal information. The messages sent by the hackers would be specifically crafted to look like an official AOL email to make users more likely to fall for the trick.

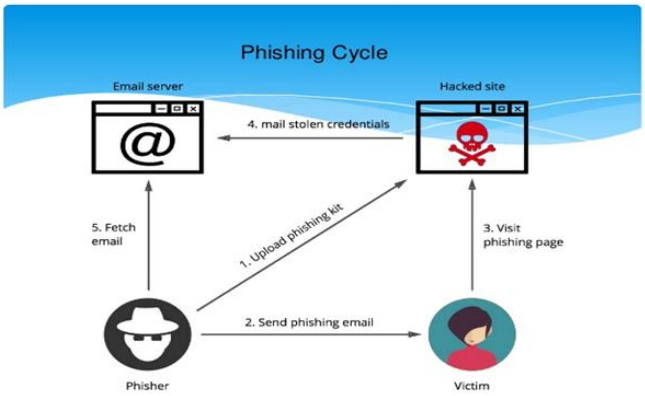
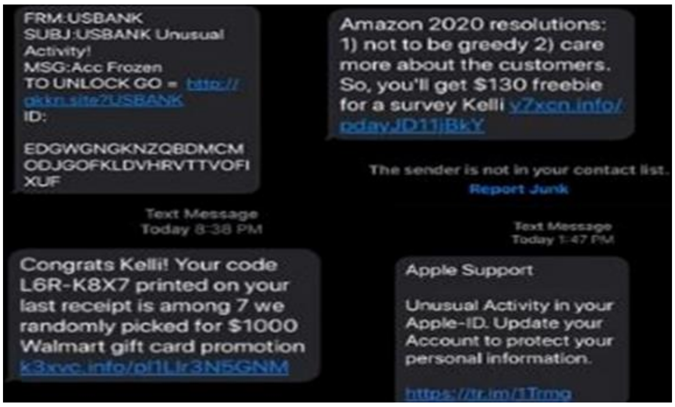


Fig. 2. Phishing Fundamentals

Since the early days of the internet however phishing has evolved to be an incredibly serious and dangerous threat. Multiple different forms of phishing have developed. Spear phishing is a form of phishing that targets a specific individual or group. This form of phishing can be more personalized and appear very legitimate to an unsuspecting user. Attackers will usually send an email with a phishing link claiming that there has been a compromise to a victim's account, claiming they need to re-sign in in order to verify security. However by performing this action it will allow the attacker to obtain the credentials from the individual. Historically, this is the most common form of phishing and is very similar to the phishing scams from AOL. A newer form of phishing is vishing. Vishing is when an attacker calls or texts a user rather than emailing a user, in an attempt to obtain sensitive information. A common vishing attack is when an attacker calls a user claiming to be a representative from a large organization, saying that the victim's computer has been compromised. The attacker will then ask the user for credit card or banking information and assist in installing a new anti virus that usually contains malware [4].

Although there are many negative connotations with phishing, it has slowly become a commonality among businesses to use phishing as a form of security testing. Phishing tests are run by numerous security professionals and businesses. Phishing tests are where IT professionals in a business will send a fake phishing scam to fellow employees to gauge employee security readiness. If a victim clicks on the phishing test link, instead of facing serious security repercussions, this safe form of phishing will usually take the user to information on how to not fall for phishing scams or may even lead a user to phishing security training to ensure that the user does not fall for similar scams in the future.



FRM:USBANK
SUBJ:USBANK Unusual Activity!
MSG:Acc Frozen
TO UNLOCK GO = http://qkkn.site?USBANK
ID:
EDGWGNGKNZQBDMCMODJGOFKLDVHRVTTVOFIXUF

Text Message
Today 8:38 PM

Congrats Kelli! Your code L6R-K8X7 printed on your last receipt is among 7 we randomly picked for $1000 Walmart gift card promotion k3xvc.info/pl1Llr3N5GNM

Amazon 2020 resolutions: 1) not to be greedy 2) care more about the customers. So, you'll get $130 freebie for a survey Kelli y7xcn.info/pdayJD11jBkY

The sender is not in your contact list.
Report Junk

Text Message
Today 1:47 PM

Apple Support

Unusual Activity in your Apple-ID. Update your Account to protect your personal information.

https://tr.im/1Trmg

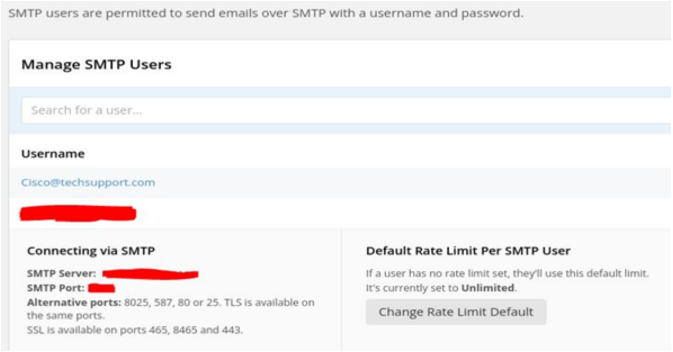
Fig. 3. Vishing Example

IV. PHISHING EXPERIMENTS

A. Email phishing with a keylogger

One of the most important steps when performing a phishing attempt is maintaining anonymity. An application that allows for a user to send emails from a reliable relay server, and from different accounts is smtp2go.com. After creating an account with this service, one can send emails from custom made users and use the smtp2go relay server to forward emails. After creating a smtp2go account, if one goes to the settings dashboard and then selects “SMTP Users”, it will allow for the account manager to create a new smtp user. By hitting “add SMTP User”. One can add a user with any username. This allows for an individual to create a user with an @google, @Microsfot, @facebook, or any possible domain. Furthermore a password is provided for the newly created user, allowing the new account to be utilized by the smtp2go SMTP server [5]. In figure 4 it can be seen that the username “Cisco@techsupport.com” is listed.

This user can send emails if needed, and can easily be deleted if required.



SMTP users are permitted to send emails over SMTP with a username and password.

Manage SMTP Users

Search for a user...

Username

Cisco@techsupport.com

[redacted]

Connecting via SMTP

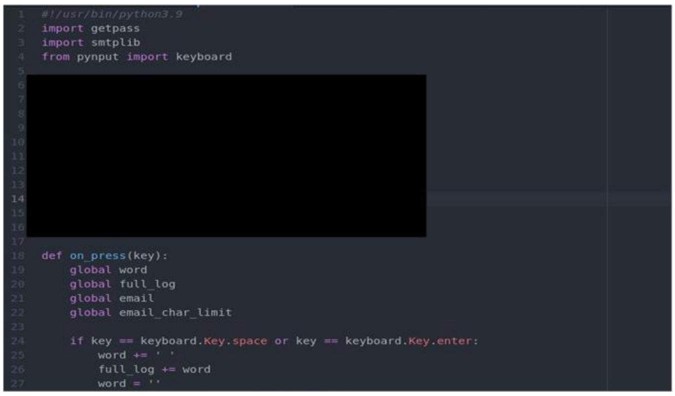
SMTP Server: [redacted]
SMTP Port: [redacted]
Alternative ports: 8025, 587, 80 or 25. TLS is available on the same ports.
SSL is available on ports 465, 8465 and 443.

Default Rate Limit Per SMTP User

If a user has no rate limit set, they'll use this default limit. It's currently set to **Unlimited**.

Fig. 4. Smtp2go User

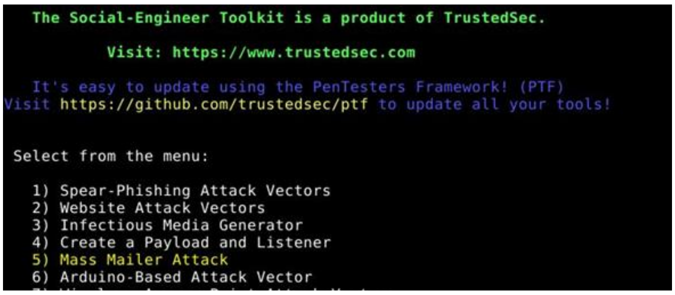
With a user created an attacker can begin crafting their phishing email and creating their payload. In this experiment, I created a keylogger to be the payload. Once the keylogger is run on a victim's computer, it will send keystrokes to an anonymous email that can easily be discarded if compromised. Creating a keylogger can be done by installing the pynput module in python and sending the recorded keystrokes to a log [6].



```
#!/usr/bin/python3.9
import getpass
import smtplib
from pynput import keyboard

[redacted]

def on_press(key):
    global word
    global full_log
    global email
    global email_char_limit

    if key == keyboard.Key.space or key == keyboard.Key.enter:
        word += ' '
        full_log += word
        word = ''
```

Fig. 5. Keylogger Code

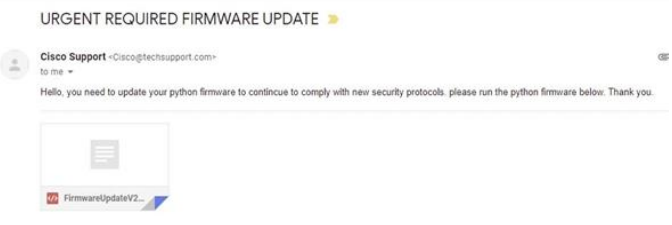
After the payload is crafted, the delivery method for the email can be devised. By using the tool Social Engineering Toolkit (SET), one can create an email and attach the keylogger payload to an unsuspecting target. Using the Social Engineering Toolkit in tandem with smtp2go will allow for the delivery of the payload to appear much more authentic due to the utilization of the smpt2go smtp server. When running SET one can select the 5th option which allows for one to select an individual email to send a phishing email to. While using SET, one can have the application run through an SMTP open-relay if a proper username and password are provided. In this experiment I used the Cisco@techsupport.com user that was created earlier. Next the address for the smtp server needs to be input, as well as the port required by the service. When using smtp2go, the SMTP email server address will be mail.smtp2go.com“ and the port can be set to “2525”. After entering the last information required in SET, the smtp2go server will send the phishing email to the target.



```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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
```

Fig. 6. SET Dashboard

Once the email has been sent, it will appear in the victim’s mailbox as shown in figure 7. Once the user runs the python script that is described to be a firmware update, it'll appear to do nothing, allowing the victim to continue their work without gaining suspicion of the python script that was just run. However, due to the keylogger, while the script is running, every 50 characters that are typed will be sent to the anonymous email that was mentioned previously. As seen in figure 8, the keylogger was able to capture what appears to be the user going to facebook.com, and then logging in with their username and password.

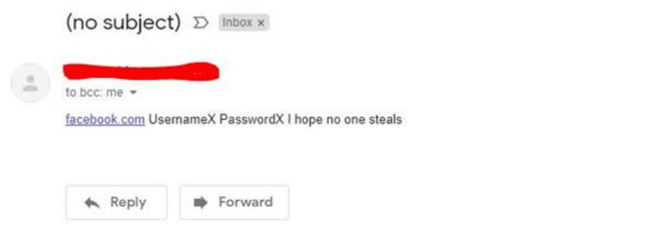


URGENT REQUIRED FIRMWARE UPDATE

Cisco Support <Cisco@techsupport.com>
to me

Hello, you need to update your python firmware to contincue to comply with new security protocols. please run the python firmware below. Thank you.

Fig. 7. Phishing Email



(no subject)

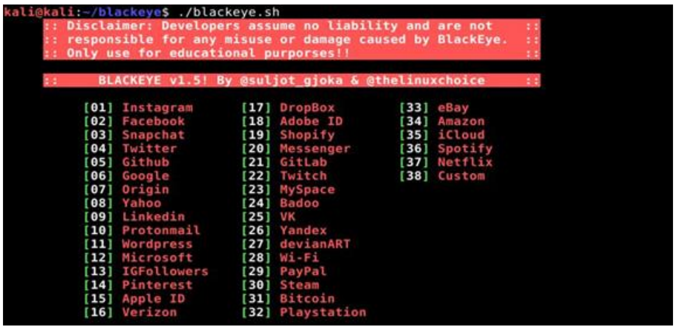
[redacted]
to bcc: me

facebook.com UsernameX PasswordX I hope no one steals

Fig. 8. Phishing Email Results

B. Email phishing with BlackEye

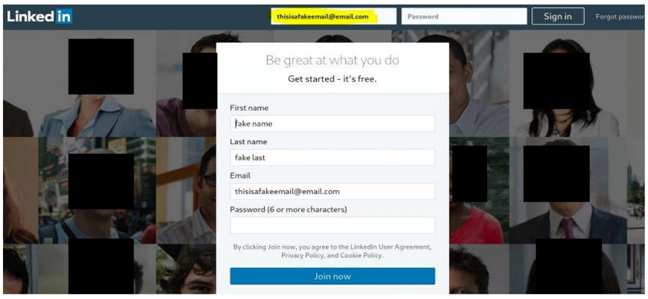
There are also numerous open source tools that can assist attackers in phishing attacks. One such tool is BlackEye. BlackEye works in conjunction with Ngrok. Ngrok is a cross-platform application that enables developers locally-hosted web servers to appear to be hosted on a subdomain of ngrok.com, meaning that no public IP or domain name on the local machine is needed to host [7]. When launching BlackEye, numerous pages are presented allowing the attacker to attempt phishing attacks at multiple different sites. As can be seen in figure 9, some of the websites include Instagram, Facebook, Linkedin, and others.



```
kali@kali:~/blackeye$ ./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 v1.5! By @suljot_gjoka & @thelinuxchoice    ::

          [01] Instagram      [17] DropBox        [33] eBay
          [02] Facebook       [18] Adobe ID       [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] Custom
          [07] Origin         [23] MySpace
          [08] Yahoo          [24] Badoo
          [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] Bitcoin
          [16] Verizon        [32] Playstation
```

Fig. 9. BlackEye Launch

After launching BlackEye, if a user selects option 9, Blackeye will create a phishing Linkedin page that will capture any credentials if they are input into the login area [8]. BlackEye generates a link that attackers can then send to unsuspecting users to lead them to the malicious Linkedin page. Using similar methods as in the previous experiment, an email designed to look like that of a Linkedin alert was generated and sent to a target user. When the user clicked on the link it opened the page seen in figure 10 with blank fields.



thisisafakeemail@email.com
Password

Be great at what you do

Get started - it's free.

First name
fake name

Last name
fake last

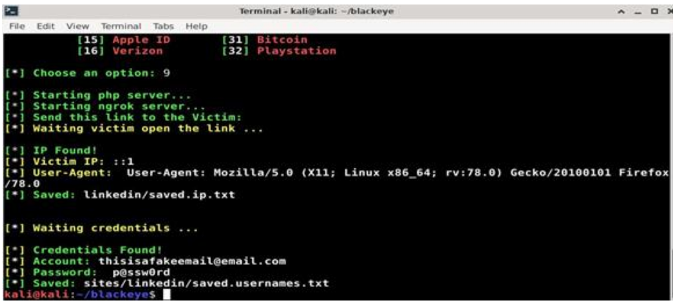
Email
thisisafakeemail@email.com

Password (6 or more characters)

By clicking Join now, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Fig. 10. Linkedin Phishing Page With Input

After inputting credentials into the login field, BlackEye would then redirect the user to a real Linkedin login page. This would make the user think that something had gone wrong and the user would most likely log into their Linkedin account not realizing that their credentials were just stolen. In figure 11, the results of the input in the malicious Linkedin page can be seen. As shown, the username and password that were input are captured by BlackEye and saved to a file on the system.



```
          [15] Apple ID       [31] Bitcoin
          [16] Verizon        [32] Playstation

[*] Choose an option: 9

[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim:
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: ::1
[*] User-Agent:  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox
/78.0
[*] Saved: linkedin/saved.ip.txt


[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: thisisafakeemail@email.com
[*] Password:  p@ssw0rd
[*] Saved: sites/linkedin/saved.usernames.txt
kali@kali:~/blackeye$ 
```

Fig. 11. BlackEye Results

V. Phishing Mitigation And Email Security

As can be seen in the experiments above, phishing can be extremely effective and dangerous if a user falls victim to it. There are however multiple methods to reduce the likelihood of a phishing scam succeeding. First, one experiment that I ran regarding phishing security was simply DNS filtering [9]. Using a free service like clearbrowsing.com can greatly inhibit phishing. When Cleanbrowsing was enabled, numerous malicious phishing websites I attempted to go to on a virtual environment were blocked. Second, antivirus can be used to further decrease the chances of a phishing attack succeeding [10]. Next, similar to the last two mitigations, a spam filter can further reduce phishing scams. Ensuring that emails from only trusted providers and do not contain abnormalities can also be effective. Common URL phishing abnormalities that should trigger an alert or filter include if the URL is misspelled, points to the wrong top-level domain, a combination of a valid and a fraudulent URL, is incredibly long, is just an IP address, has a low pagerank, orhas a young domain age [11].

VI. Conclusion

In this paper attack vectors related to phishing were experimented on and investigated. As a result of the investigation, it was shown that phishing attacks can be crafted in numerous different ways, phishing payloads can vary, and open source tools related to phishing are available online. The ability for a standard browser or email service to detect potential phishing attacks were shown to be miniscule and default security measures failed to stop both experiments from executing. Experimentation however with DNS filtering was capable of blocking malicious websites and user examination of suspicious emails and urls were effective methods at limiting the success of phishing attempts. Due to the ever expanding audience the internet is capable of reaching, better security practices in relation to detecting and blocking phishing attempts must be met.

References

[1] “A brief history of email: Dedicated to Ray Tomlinson,” Phrasee, 28-Sep-2021. [Online]. Available: https://phrasee.co/blog/a-brief-history-of-email/.

[2] Z. Bloom, “The history of email,” The Cloudflare Blog, 29-Aug-2018. [Online]. Available: https://blog.cloudflare.com/the-history-of-email/.

[3] “History of phishing: How phishing attacks evolved from poorly constructed attempts to highly sophisticated attacks,” PhishProtection.com, 25-Oct-2021. [Online]. Available: https://www.phishprotection.com/resources/history-of-phishing/#:~:text=The%20term%20phishing%20and%20its,personal%20information%20from%20AOL%20users.

[4] “What are the different types of phishing?,” Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html.

[5] “Reliable &amp; Scalable Email Delivery Service,” SMTP2GO, 26-Apr-2018. [Online]. Available: https://www.smtp2go.com/.

[6] “Pynput,” PyPI. [Online]. Available: https://pypi.org/project/pynput/.

[7] “Ngrok and cross-platform development,” PubNub, 16-Mar-2021. [Online]. Available: https://www.pubnub.com/learn/glossary/what-is-ngrok/.

P. by K. Rajalingham, K. Rajalingham, Kalyani Rajalingham I'm from Sri Lanka (live in Canada), and I'm from Sri Lanka (live in Canada),

[8] “BlackEye – creating a phishing page,” zSecurity. [Online]. Available: https://zsecurity.org/blackeye/.

[9] N. Z, “Phishing protection - comparing DNS security filters,” Medium, 31-May-2018. [Online]. Available: https://medium.com/@nykolas.z/phishing-protection-comparing-dns-security-filters-9d5a09849b91.

[10] "Phishing attack prevention: How to identify &amp; avoid phishing scams in 2021," Digital Guardian, 09-Sep-2021. [Online]. Available: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams.

[11] Swaathi KakarlaGuest blogger: Swaathi Kakarla is the co-founder and CTO at Skcript. She enjoys talking and writing about code efficiency, "How to detect a phishing URL using python and machine learning," ActiveState, 11-Feb-2021. [Online]. Available: https://www.activestate.com/blog/phishing-url-detection-with-python-and-ml/.