

## CERT Lab 2 – Social Engineering

---

### Educational Objectives

1. Learn how social engineering techniques are performed by adversaries
2. Prevent yourself from the most popular social engineering attack: phishing

### Tools

1. Kali Linux VM

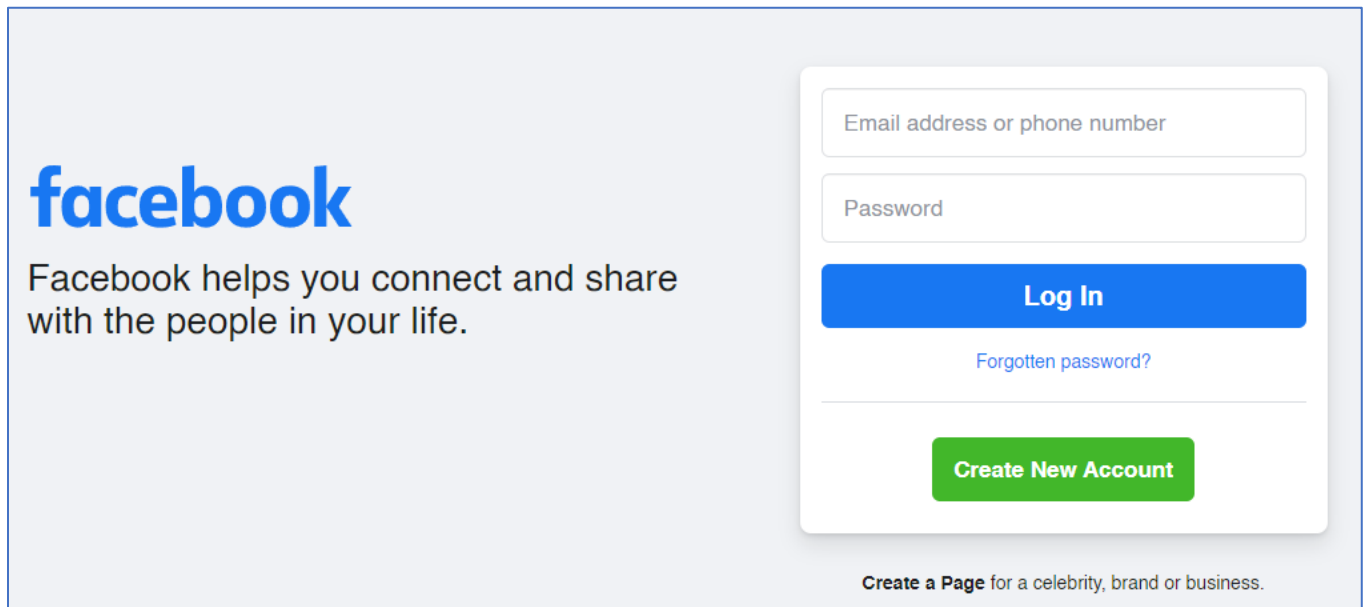
### Theory

One of the most critical security measures you can learn and teach to your family, colleagues, and peers is how to recognize and avoid fishing. Therefore, we will examine the entire process of a spear phishing email and determine why so many people click on spearfishing or even standard phishing emails. In the past, every email was poorly written and contained numerous spelling errors. Today's attacks are significantly more complex, so that is what we will create. We will build a spear phishing attack with Kali Linux.

The phishing attack typically follows these phases:


**Creating a fake website > Send phishing emails > Wait for victim to interact > Capture login credentials**

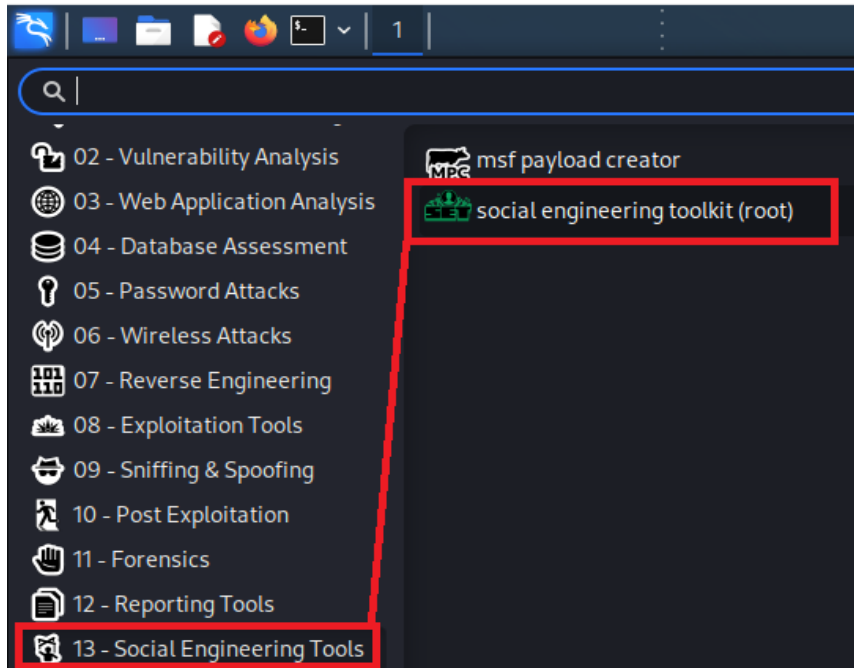
We will start with observing a real email from Facebook or Twitter or any social media sites. Any place that has the username and the password box on the same page as Facebook



You can see that both username and password boxes are located together in the same page, and this is important because most phishing attempts use the same technique to fool victims.

## Lab Tasks 2.0

1. In the Kali Linux machine, click on the Applications button  > 13 Social Engineering Tools > social engineering toolkit (root)



- i. Enter password when prompted (default password: **kali**).

```
The Social-Engineer Toolkit is designed purely for good
it is a tool for malicious purposes that are not authorized
If you use it for anything other than good, you are violating the terms of service and license
If you agree to the terms of service and that you will only use it for good, type 'y'
Do you agree to the terms of service [y/n]: y|
```

- ii. Type “Y” and press enter to agree to the service terms.

2. The main screen of social engineering toolkit will appear

```

Shell No. 1
File Actions Edit View Help

Trash .M"" "bgd `7MM"" "YMM MMP"" "MM"" "YMM
,MI      "Y  MM      `7 P'  MM      `7
`MMb.      MM      d      MM
`YMMNq.    MMmmMM      MM
.      `MM  MM      Y ,      MM
Mb      dM  MM      ,M      MM
P"Ybmmd" .JMMmmmmMMM .JMML.

File System

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
      Version: 8.0.3
      Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

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) 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> 1|
  
```

- i. Press 1 for **Social-Engineering Attacks** then press enter
- ii. Then select 2 for **Website Attack Vectors**
- iii. Select 3 for **Credential Harvester Attack Method**
- iv. Finally select 2 for **Site Cloner**

3. Set the IP address for the phishing site to the IP address of the Kali Linux VM, (in this example, the IP address is 10.0.9.4), then press enter.

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
[-] to harvest credentials or parameters from a website as well as place them in

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.


set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.9.4]:|
```

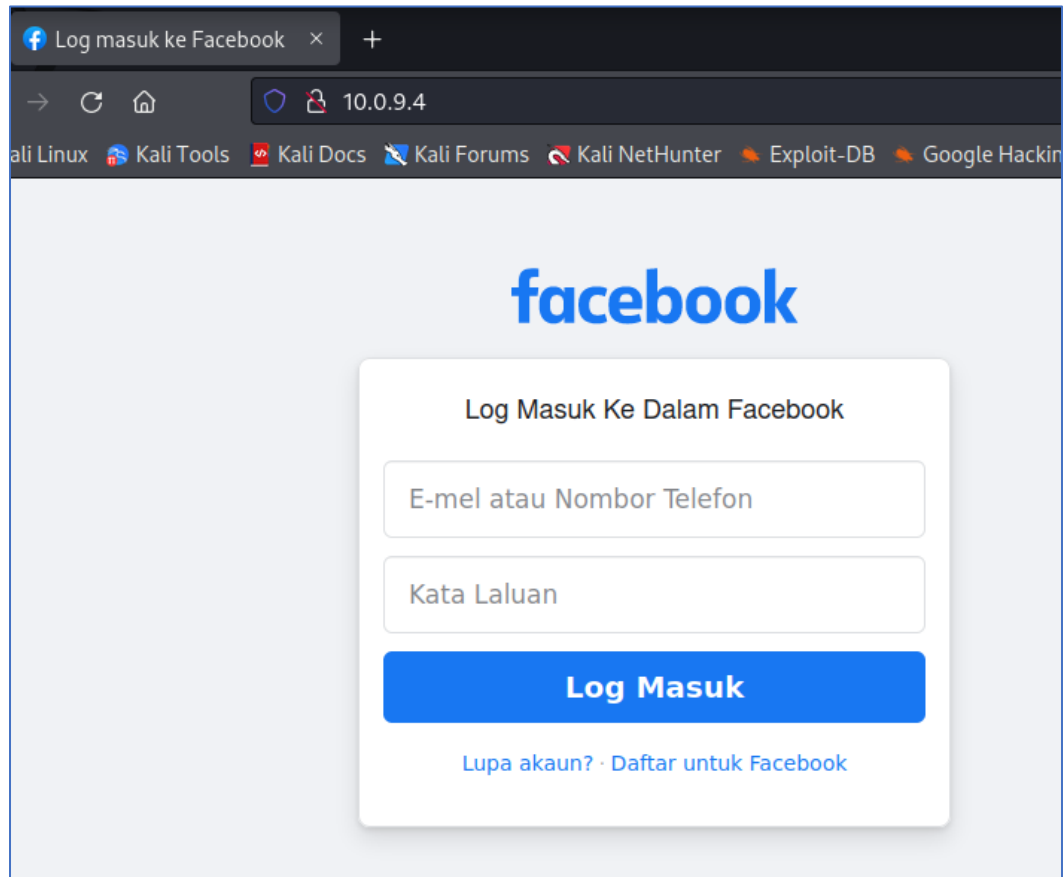
4. Enter the URL to clone to [www.facebook.com](http://www.facebook.com)

```
set:webattack> Enter the url to clone:www.facebook.com

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

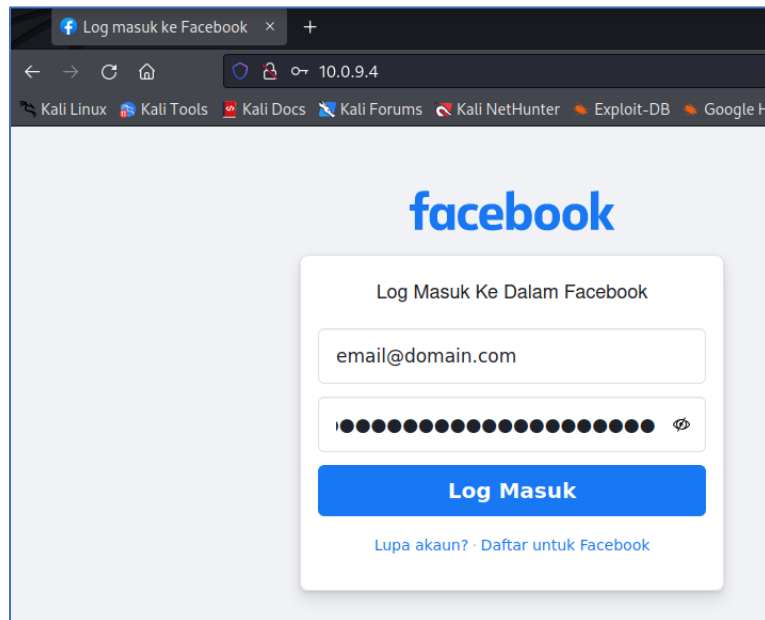
The best way to use this attack is if username and password form
captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

- Once it has finished cloning, we can now check if the phishing website is up and running, to do this, open browser (Firefox ESR ) , and type the IP address of the Kali Linux machine in the address bar.



The local IP address of Kali Linux machine shows a **copy** of Facebook login page

6. Enter any email and password into the fake login page. In this example, we will use [email@domain.com](mailto:email@domain.com) as the email and “ThisIsMyPassword12345” as the password



- i. Click on the login button

7. Return to the terminal and observe that we have captured the login credentials that was entered

```

Shell No. 1
File Actions Edit View Help

10.0.9.4 - - [22/May/2022 19:38:08] "POST /ajax/bz?_a=1&_ccg=EXCELLENT&_
6Fo4OQlPyUbFuClswgE98nwgU6C7UW3q327E2vwXx60kO4o3Bw5VCwjE3awbG782Cw8G1Qw5MKd
E3fw5rwSyE15822wrU&_hs=19134.BP%3ADEFAULT.2.0.0.0.&_hsi=71007083104974817
3&_s=rd2vk7%3Aiqmlvl%3Aqfxdf3&_spin_b=trunk&_spin_r=1005562353&_spin_t=
zoest=2978&lsd=AVqrCchl7Dc HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2978
PARAM: lsd=AVqrCchl7Dc
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxOTIwLCJoiJsImF3IjoxOTIwLCJhaCI6OTQwLCJjIjoyNH0=
PARAM: lgnrnd=163446_akDl
PARAM: login=1653262634
POSSIBLE USERNAME FIELD FOUND: email=email@domain.com
POSSIBLE PASSWORD FIELD FOUND: pass=ThisIsMyPassword12345
PARAM: prefill_contact_point
PARAM: prefill_source=
    
```

## Lab Tasks 2.1 – IP Address Masking: Hiding URL

Now that we've set up a fake login page to get the victim's login information, we need to hide the URL so that it doesn't look like we're running something from a Kali Linux virtual machine (VM).

Using "www.facebook.com@google.com" is something we could try. The '@' symbol is a holdover from the days when FTP and other user logins were done through a browser.

So, this will take everything that comes before the @ symbol (if there are no illegal characters like slashes), then will try to use everything before the @ as a username for the website that comes after the @.

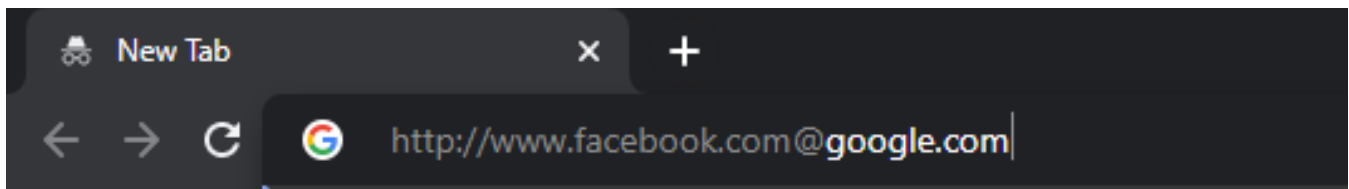


Figure 1: Typing `http://site1@site2.com` into the address bar will take the user to the site after the @ symbol

So, if you just looked at this quickly, you might think it would take you to Facebook. It starts with `www.facebook.com`, and if you don't notice the rest, you might think it would take you to Facebook. But if you type 'http://' before this address, you'll see that the first half is greyed out because it thinks that's a username. Mozilla Firefox illustrates this example in a clearer way:

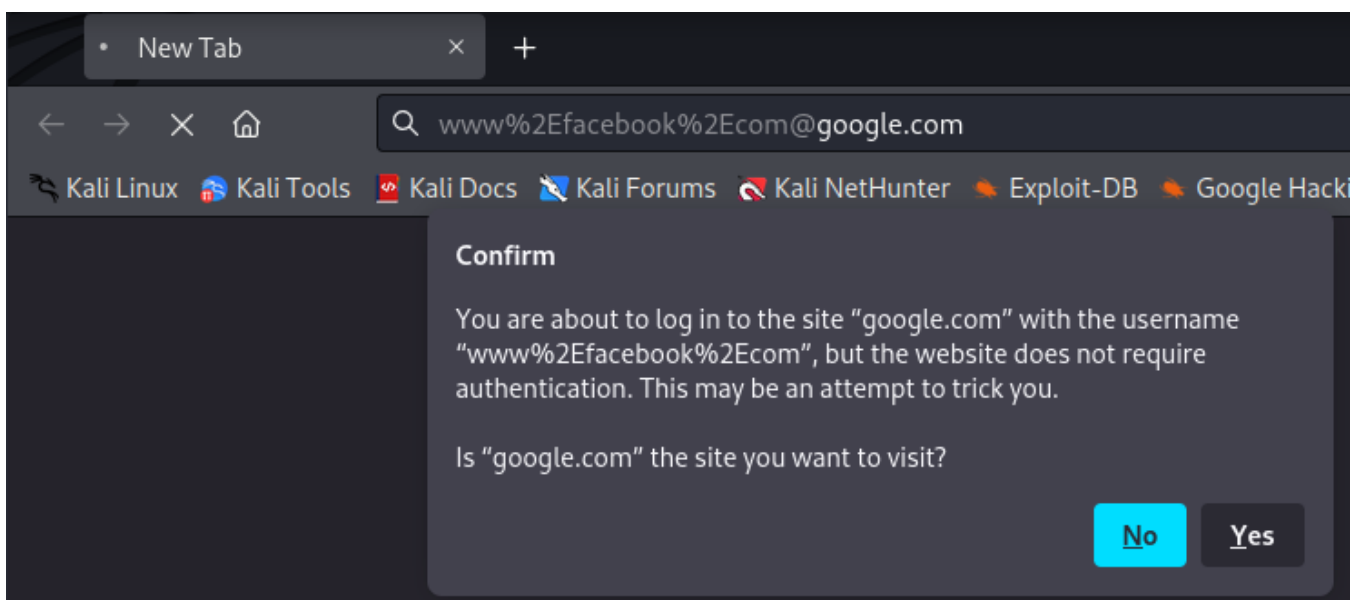


Figure 2: `http://www.facebook.com@google.com` using Firefox browser warning message



If the victim uses Google Chrome, there will not be any warning and thus when the link is entered, the victim will be redirected to google.com.

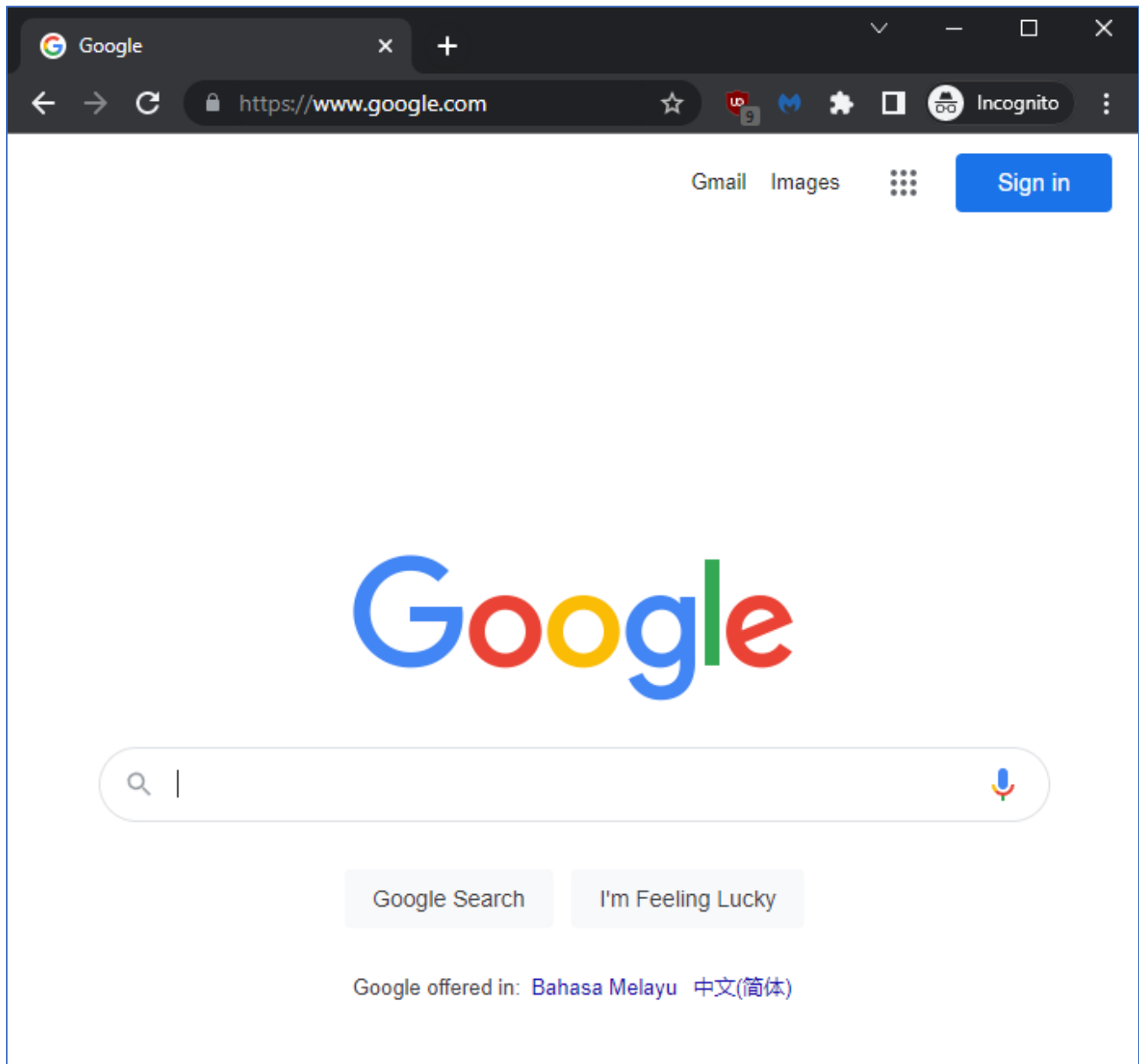


Figure 3: <http://www.facebook.com@google.com>, when entered, the user is simply redirected to Google start page

Now that we have a way to trick users into clicking a link simply by hiding the link within another link using the @ symbol method. With this method, the link that we crafted before can be made into:




http://www.facebook.com@10.0.9.4

Figure 4: Phishing link to redirect user to the fake login site

However, this link still looks suspicious, especially with the IP address at the end of the site. What we can do now is to translate the IP address part of the URL into numbers:

1. Go to a search engine and search for “IP Address to decimal converter”
2. Click on any of the online tool that you could find
3. Convert the IP of the fake website, in this example 10.0.9.4 into decimal



IP-To-Decimal

IP address 10.0.9.4 is equal to 167774468.

**IP Address / IP Number**

10.0.9.4

Convert

Figure 5: IP to decimal converter. Site: <https://www.ipaddressguide.com/ip>

4. To test this out, type <http://167774468> (or whatever the result of your IP to decimal is) and press enter

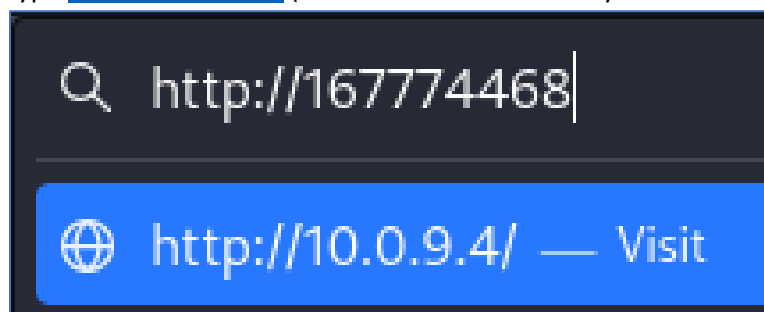



Figure 6: We could observe that the decimal 167774468 is equals to the IP 10.0.9.4

5. Therefore, the result of our phishing URL to send is:



Q <http://www.facebook.com@167774468>

*Figure 7: A slightly more convincing phishing URL to send*

6. The next step is to send this URL to the victim.

### (Extra) Lab Tasks 2.2– Crafting a Phishing email

After making the link, we need to put it into a convincing email. The first step in creating a phishing email is to start with a legitimate email from a company. So, in this case, Facebook has already sent a notification email (pictured below). We're going to use this as the basis for a new email we're going to send, so we can either forward it or copy and paste it into a new email.

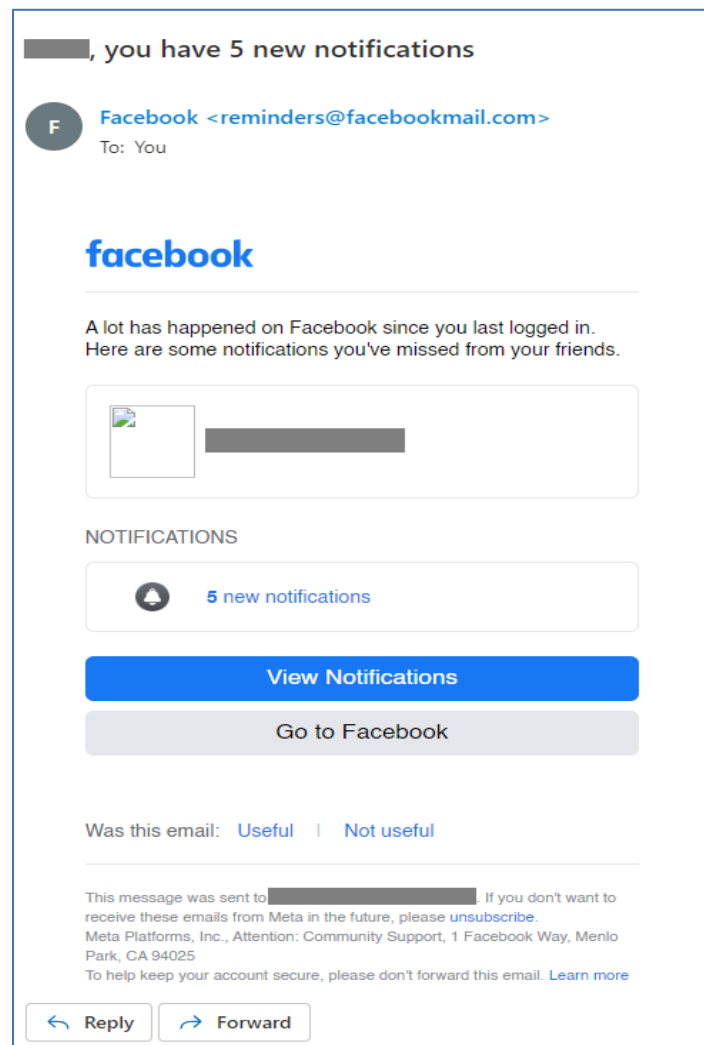
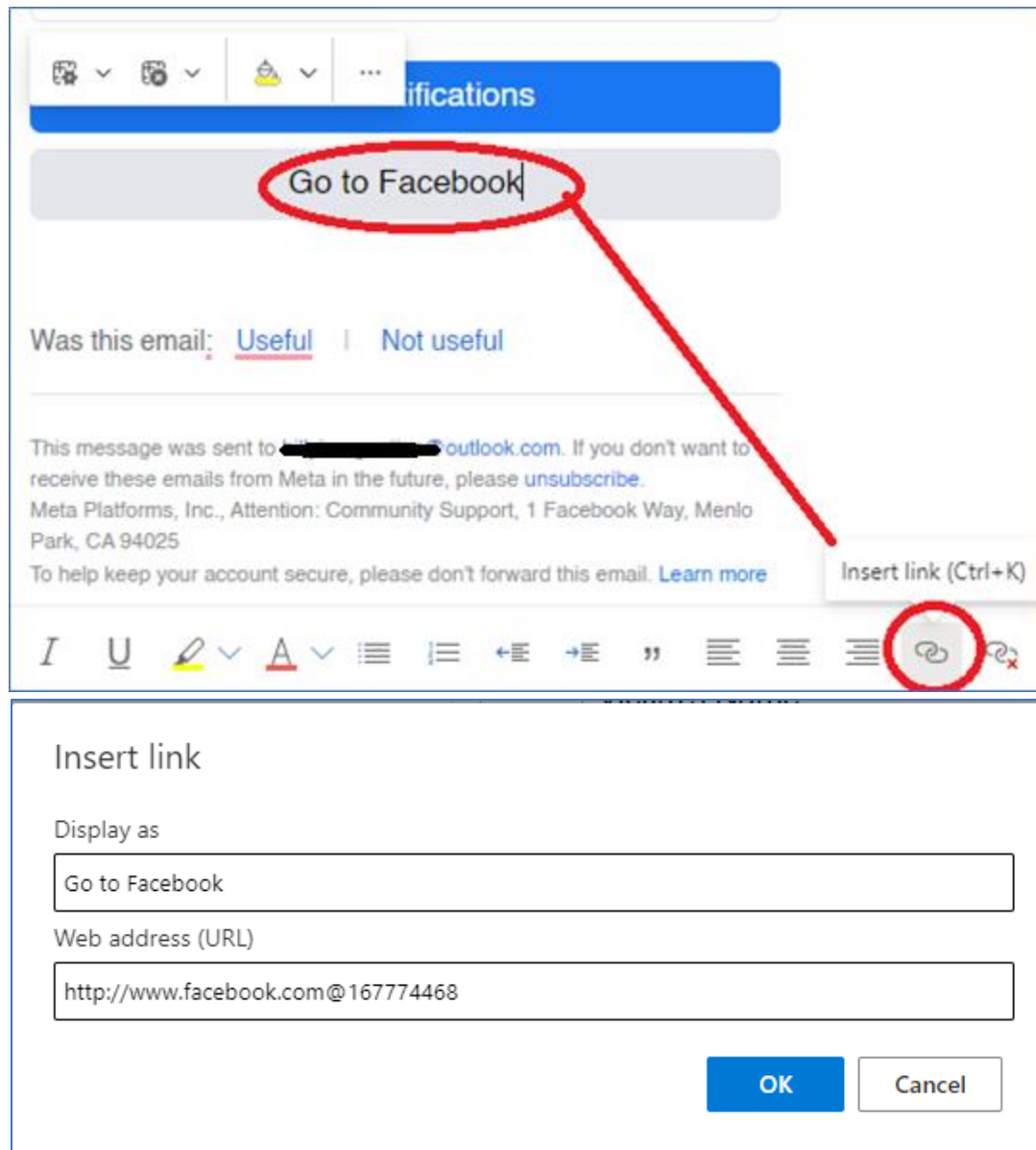


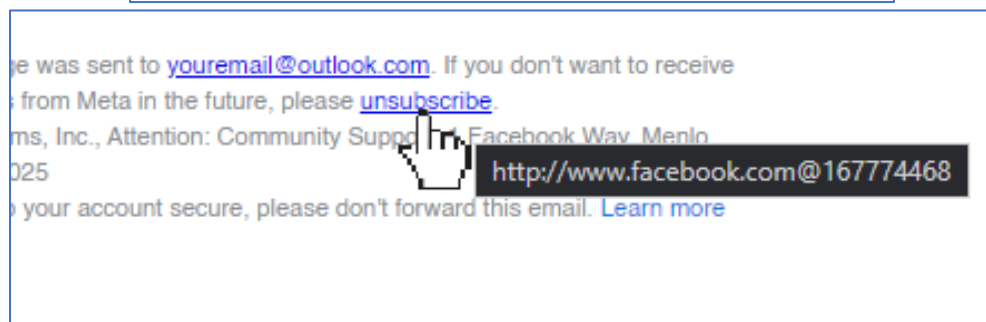
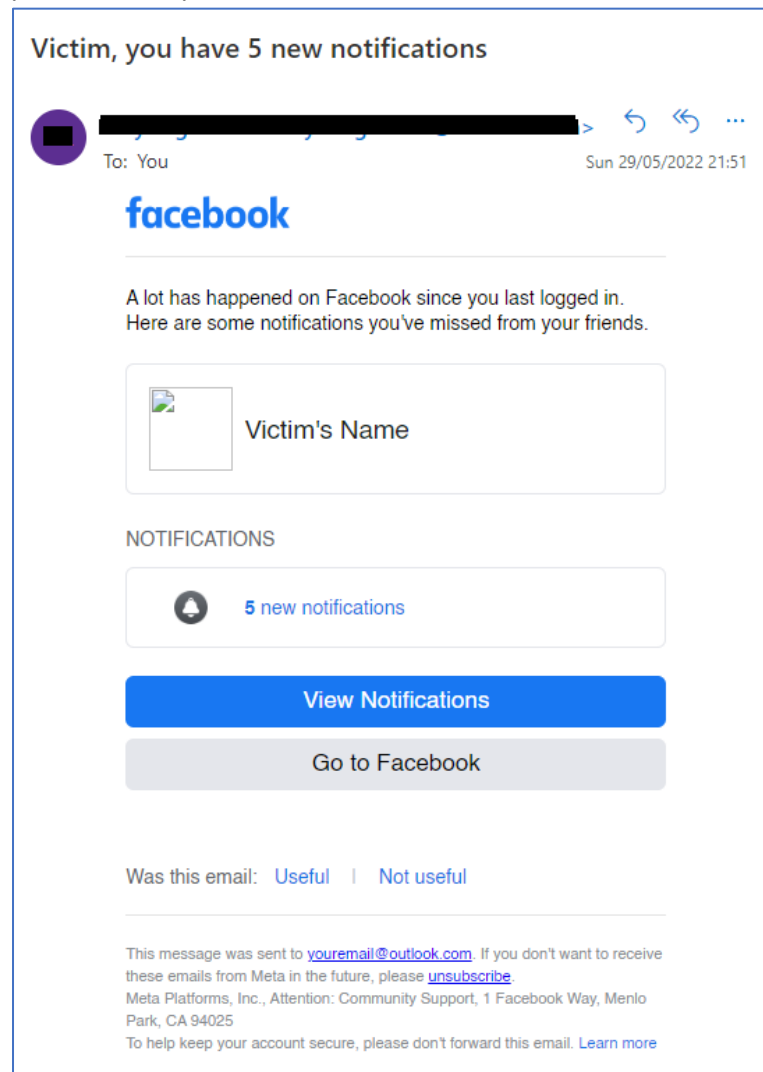
Figure 8: Real Email from Facebook

1. Open your email inbox and search for any notification/update emails from a legitimate site.
2. Forward or copy paste the email into a new mail
3. Change the subject into something convincing that a victim might click
4. Change the To field into the victim's email address
5. Change every clickable links in the email, especially the unsubscribe button, into the fake site that we have created in the previous lab:



6. Repeat step 5 until every single button in the email redirects the victim into the phishing site (<http://www.facebook.com@167774468/>)

7. Send the email to your secondary email address and observe the email contents:



(Q1) Describe another way to hide links

## Recommended Links (further learning)

---

<https://phishingquiz.withgoogle.com/>