Phishing Vs. Legit: Comparative Analysis of Client-Side Resources of Phishing and Target Brand Websites

Kyungchan Lim
University of Tennessee

Jaehwan Park
University of Tennessee

Doowon Kim
University of Tennessee

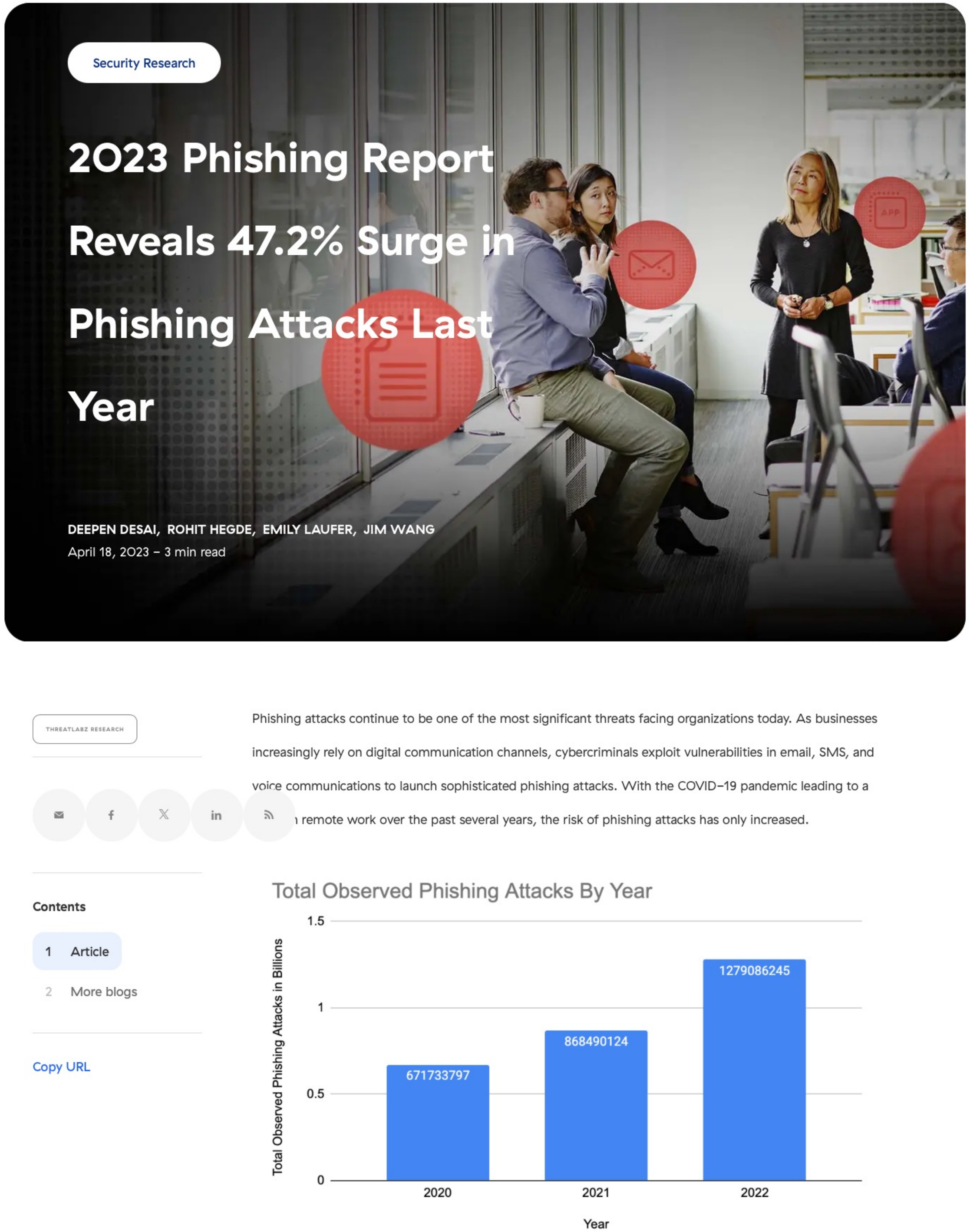
The Web Conference 2024

THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Severe Phishing Attacks!

THE UNIVERSITY OF TENNESSEE KNOXVILLE

ttacks!



Security Research

2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

DEEPEN DESAI, ROHIT HEGDE, EMILY LAUFER, JIM WANG

April 18, 2023 – 3 min read

THREATLABZ RESEARCH

Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a ı remote work over the past several years, the risk of phishing attacks has only increased.

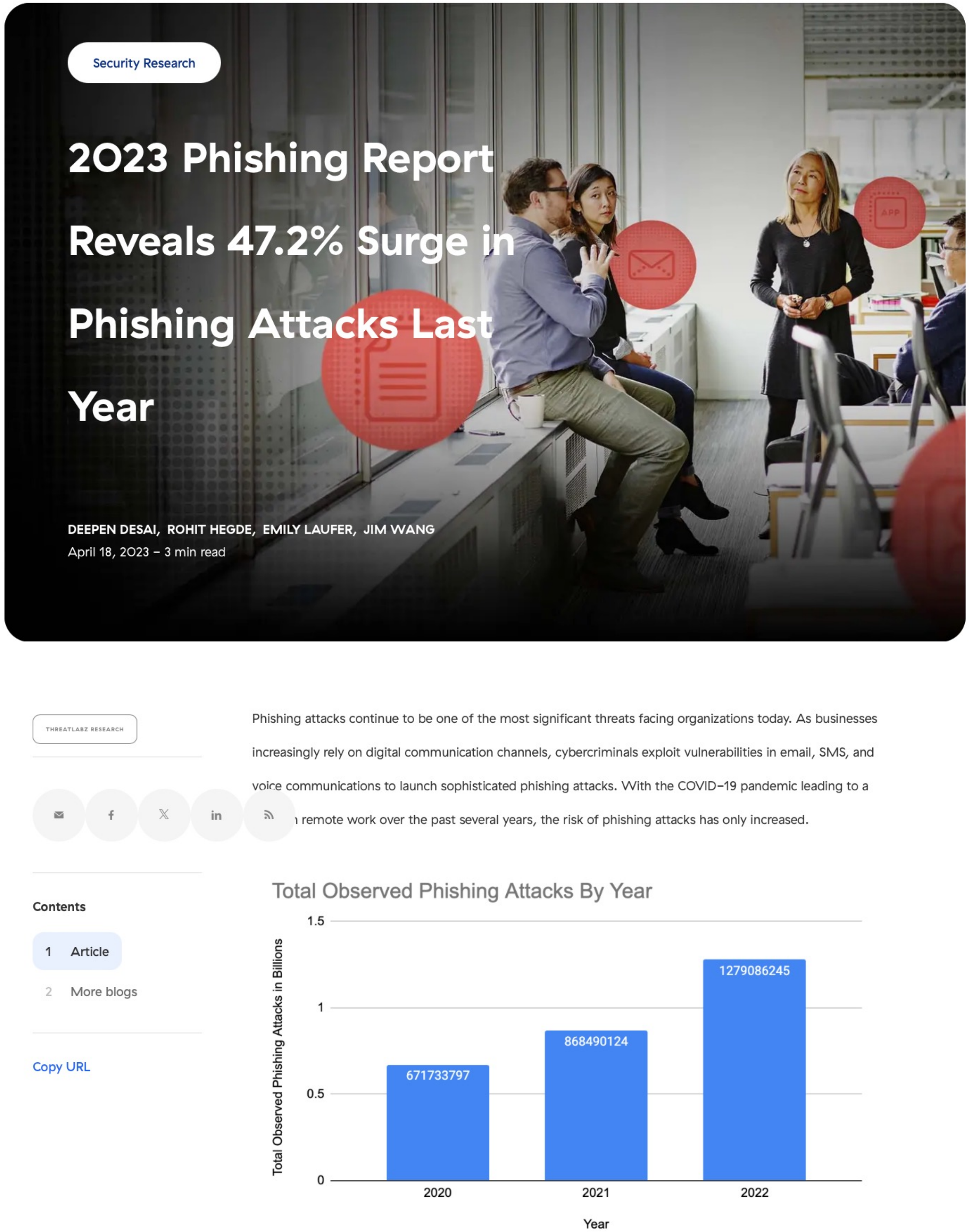
Contents

1 Article

2 More blogs

Copy URL

Total Observed Phishing Attacks By Year



Security Research

2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

DEEPEN DESAI, ROHIT HEGDE, EMILY LAUFER, JIM WANG
April 18, 2023 – 3 min read

THREATLABZ RESEARCH

Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a remote work over the past several years, the risk of phishing attacks has only increased.

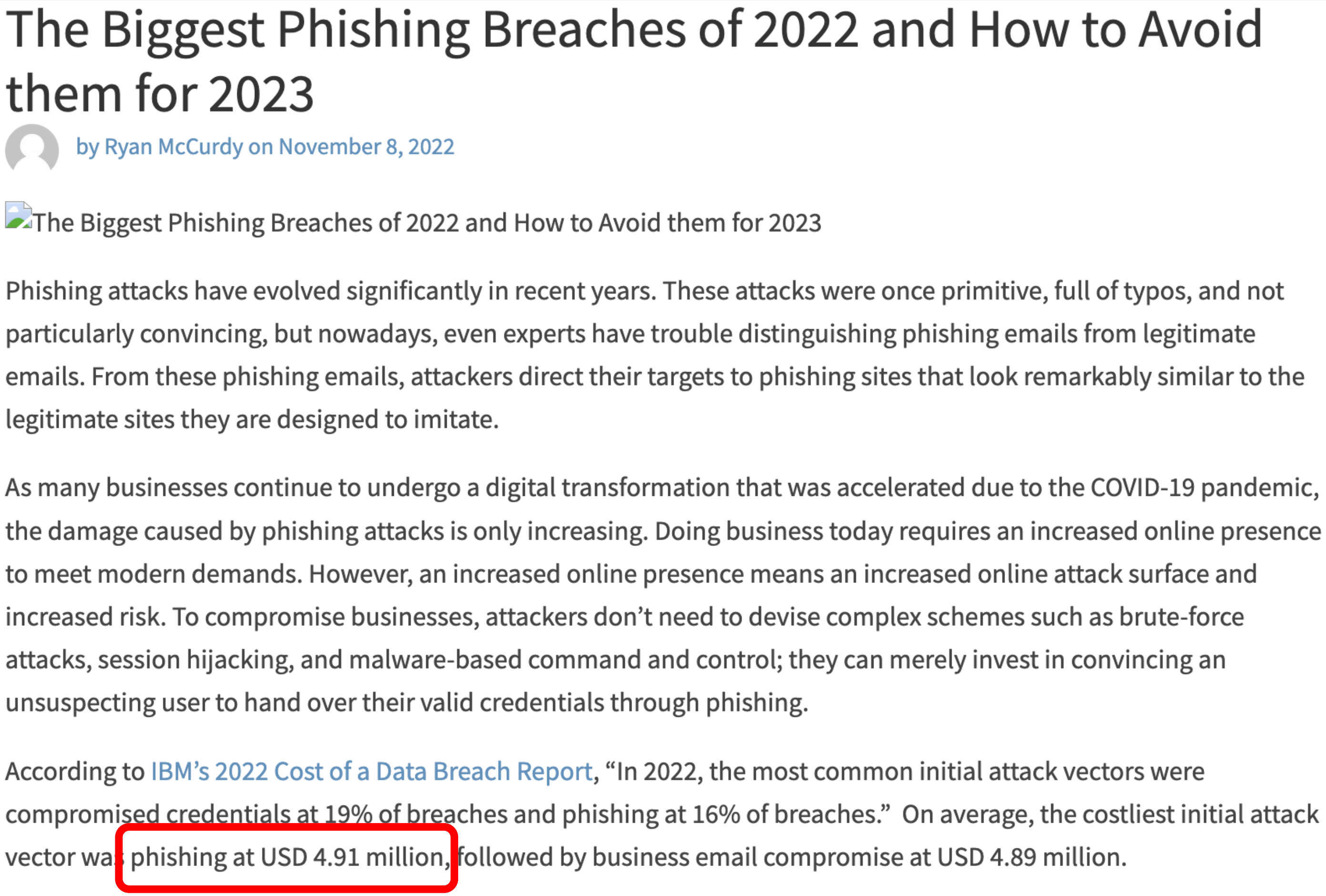
Contents

1 Article

2 More blogs

Copy URL

Total Observed Phishing Attacks By Year



The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023

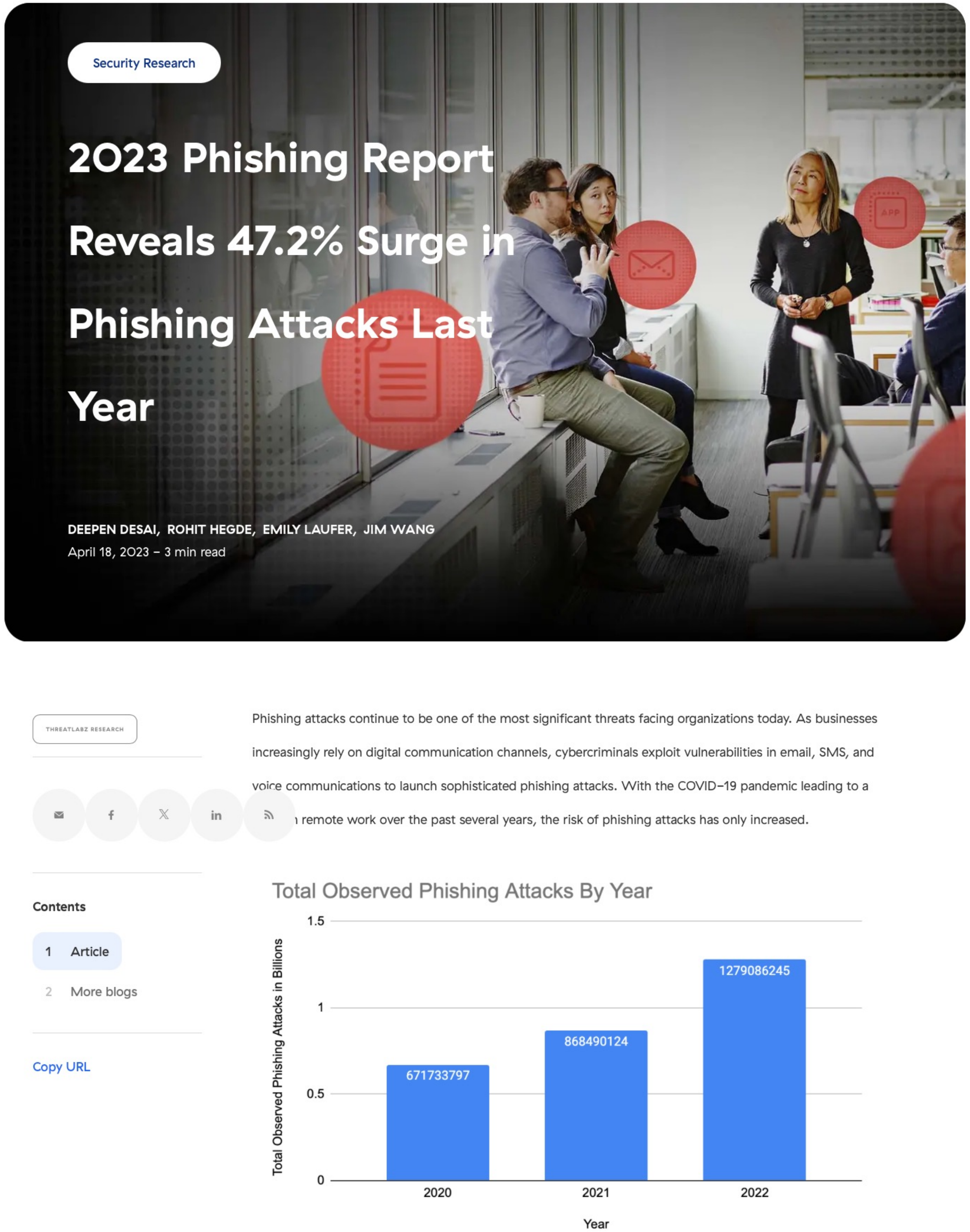
by Ryan McCurdy on November 8, 2022

The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023

Phishing attacks have evolved significantly in recent years. These attacks were once primitive, full of typos, and not particularly convincing, but nowadays, even experts have trouble distinguishing phishing emails from legitimate emails. From these phishing emails, attackers direct their targets to phishing sites that look remarkably similar to the legitimate sites they are designed to imitate.

As many businesses continue to undergo a digital transformation that was accelerated due to the COVID-19 pandemic, the damage caused by phishing attacks is only increasing. Doing business today requires an increased online presence to meet modern demands. However, an increased online presence means an increased online attack surface and increased risk. To compromise businesses, attackers don't need to devise complex schemes such as brute-force attacks, session hijacking, and malware-based command and control; they can merely invest in convincing an unsuspecting user to hand over their valid credentials through phishing.

According to IBM's 2022 Cost of a Data Breach Report, "In 2022, the most common initial attack vectors were compromised credentials at 19% of breaches and phishing at 16% of breaches." On average, the costliest initial attack vector was phishing at USD 4.91 million, followed by business email compromise at USD 4.89 million.



Security Research

2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

DEEPEN DESAI, ROHIT HEGDE, EMILY LAUFER, JIM WANG

April 18, 2023 – 3 min read

THREATLABZ RESEARCH

Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a ı remote work over the past several years, the risk of phishing attacks has only increased.

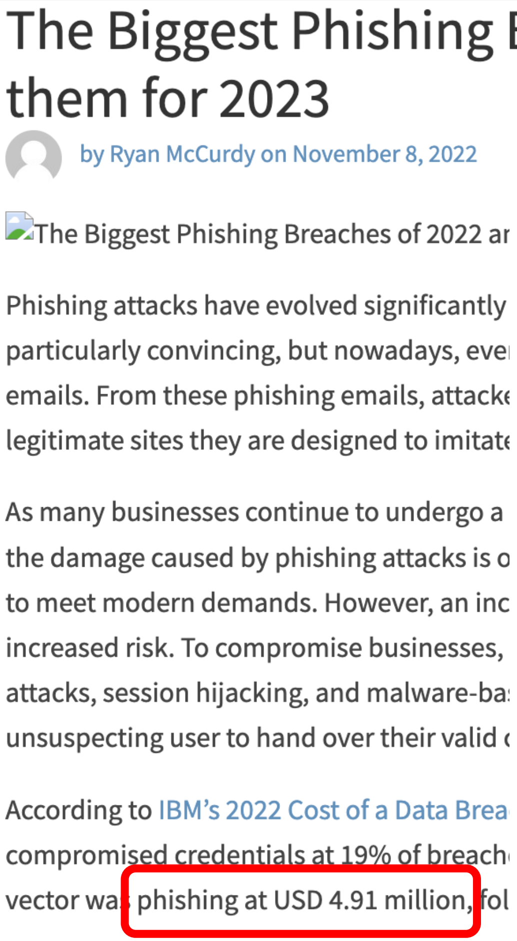
Contents

1 Article

2 More blogs

Copy URL

Total Observed Phishing Attacks By Year



The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023

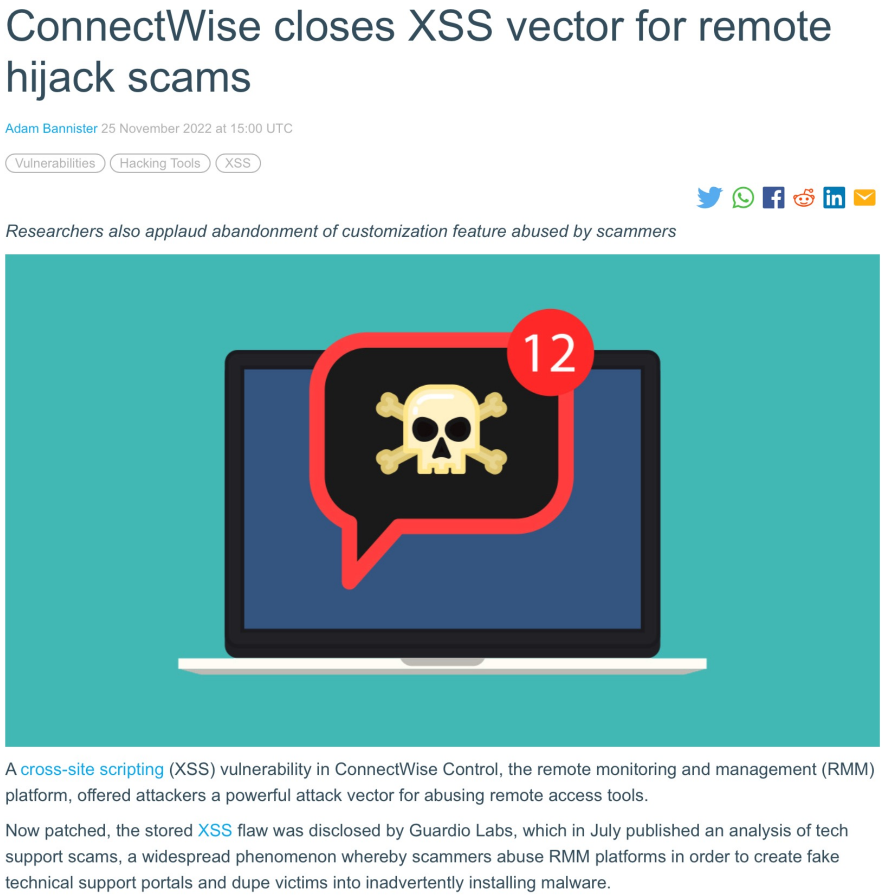
by Ryan McCurdy on November 8, 2022

The Biggest Phishing Breaches of 2022 ar

Phishing attacks have evolved significantly particularly convincing, but nowadays, eve emails. From these phishing emails, attacke legitimate sites they are designed to imitate

As many businesses continue to undergo a the damage caused by phishing attacks is o to meet modern demands. However, an inc increased risk. To compromise businesses, attacks, session hijacking, and malware-ba unsuspecting user to hand over their valid

According to IBM's 2022 Cost of a Data Brea compromised credentials at 19% of breach vector was phishing at USD 4.91 million, fol



ConnectWise closes XSS vector for remote hijack scams

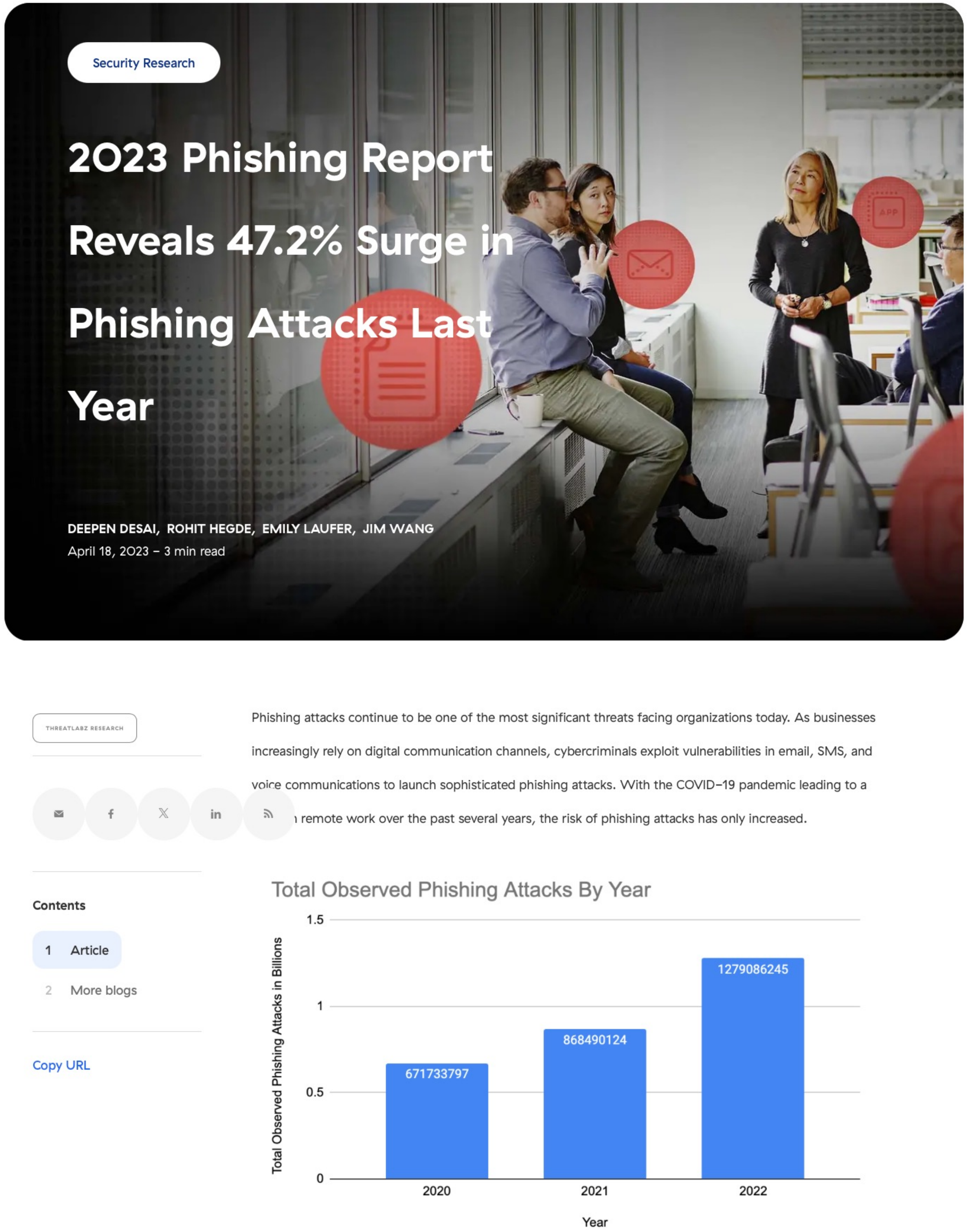
Adam Bannister 25 November 2022 at 15:00 UTC

Vulnerabilities Hacking Tools XSS

Researchers also applaud abandonment of customization feature abused by scammers

A cross-site scripting (XSS) vulnerability in ConnectWise Control, the remote monitoring and management (RMM) platform, offered attackers a powerful attack vector for abusing remote access tools.

Now patched, the stored XSS flaw was disclosed by Guardio Labs, which in July published an analysis of tech support scams, a widespread phenomenon whereby scammers abuse RMM platforms in order to create fake technical support portals and dupe victims into inadvertently installing malware.



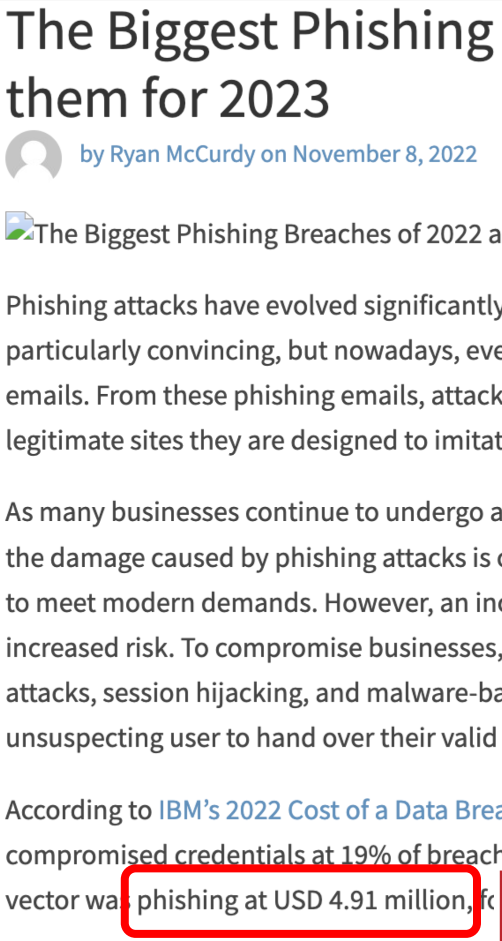
2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

DEEPEN DESAI, ROHIT HEGDE, EMILY LAUFER, JIM WANG

April 18, 2023 – 3 min read

Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a n remote work over the past several years, the risk of phishing attacks has only increased.

Total Observed Phishing Attacks By Year



The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023

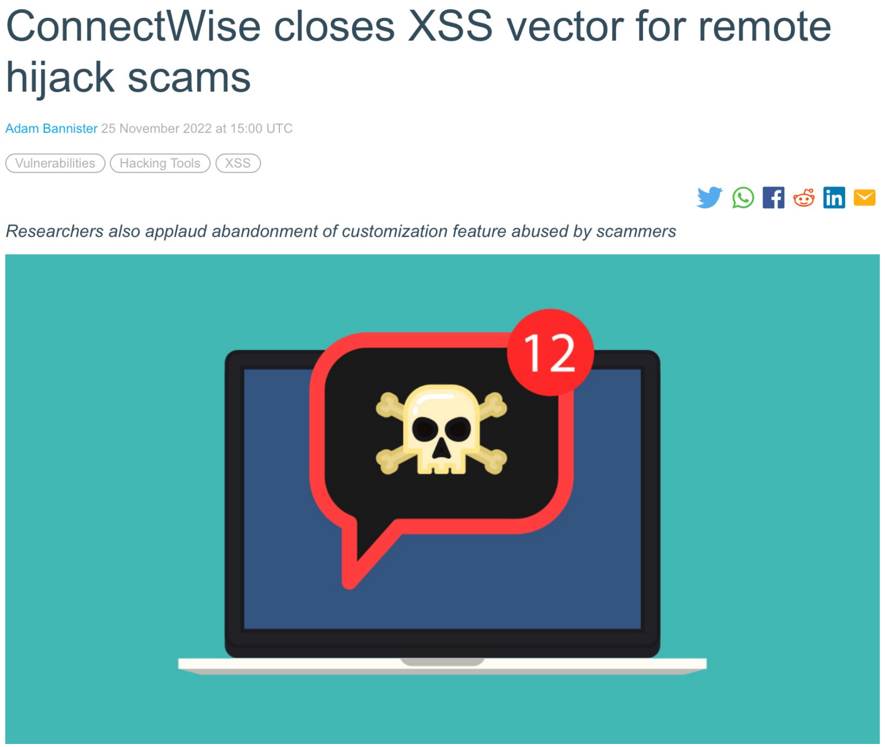
by Ryan McCurdy on November 8, 2022

The Biggest Phishing Breaches of 2022 ar

Phishing attacks have evolved significantly
particularly convincing, but nowadays, eve
emails. From these phishing emails, attacke
legitimate sites they are designed to imitate

As many businesses continue to undergo a
the damage caused by phishing attacks is o
to meet modern demands. However, an inc
increased risk. To compromise businesses,
attacks, session hijacking, and malware-ba
unsuspecting user to hand over their valid

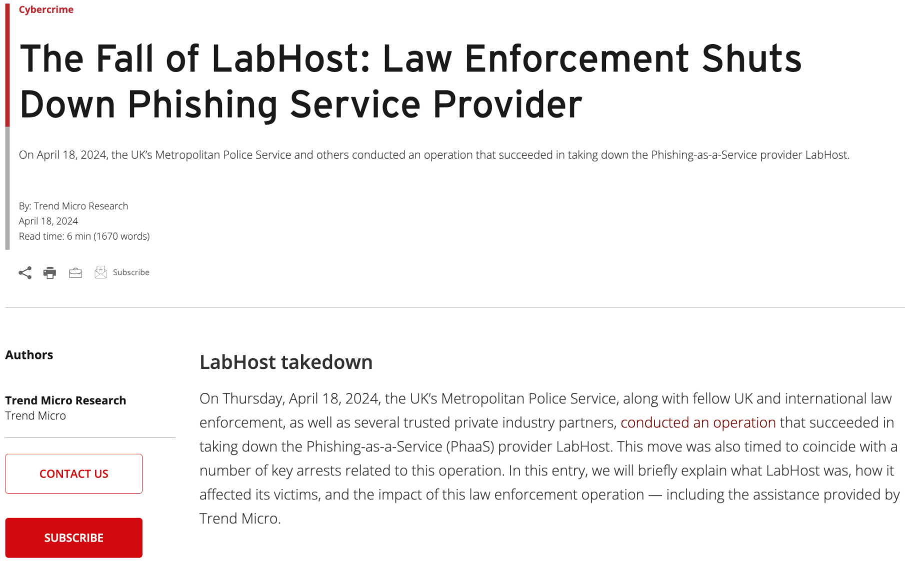
According to IBM's 2022 Cost of a Data Brea
compromised credentials at 19% of breach
vector was phishing at USD 4.91 million, fc



ConnectWise closes XSS vector for remote hijack scams

Adam Bannister 25 November 2022 at 15:00 UTC

Researchers also applaud abandonment of customization feature abused by scammers



Cybercrime

The Fall of LabHost: Law Enforcement Shuts Down Phishing Service Provider

On April 18, 2024, the UK's Metropolitan Police Service and others conducted an operation that succeeded in taking down the Phishing-as-a-Service provider LabHost.

By: Trend Micro Research
April 18, 2024
Read time: 6 min (1670 words)

Authors

Trend Micro Research
Trend Micro

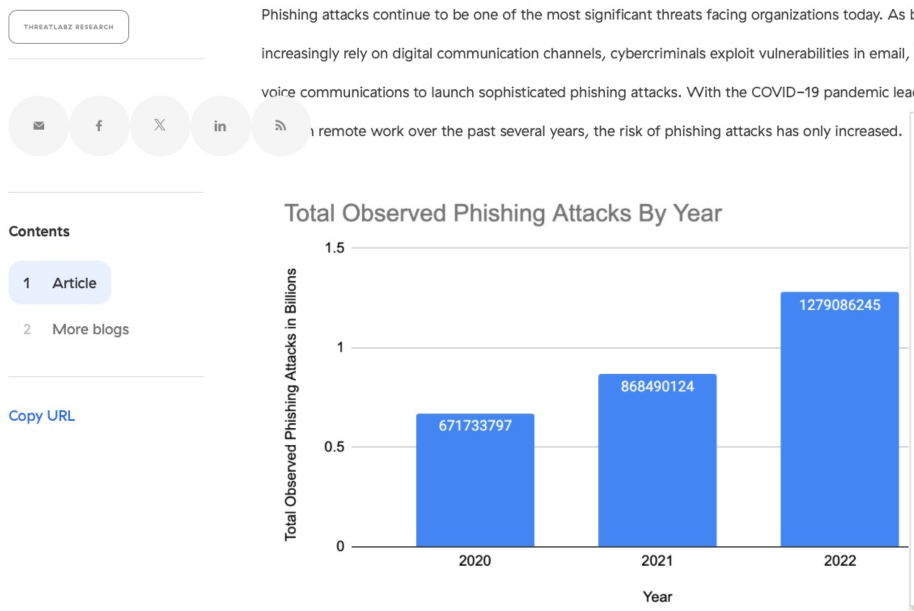
LabHost takedown

On Thursday, April 18, 2024, the UK's Metropolitan Police Service, along with fellow UK and international law enforcement, as well as several trusted private industry partners, conducted an operation that succeeded in taking down the Phishing-as-a-Service (PhaaS) provider LabHost. This move was also timed to coincide with a number of key arrests related to this operation. In this entry, we will briefly explain what LabHost was, how it affected its victims, and the impact of this law enforcement operation — including the assistance provided by Trend Micro.

Security Research

2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year

DEEPEN DESAI, ROHIT HEGDE, EMILY LAUFER, JIM WANG
April 18, 2023 – 3 min read



THREATLABZ RESEARCH

Contents

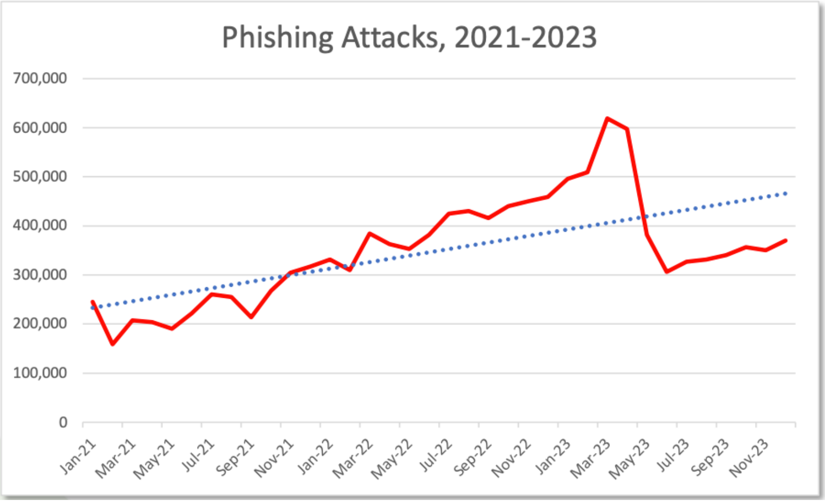
1 Article

2 More blogs

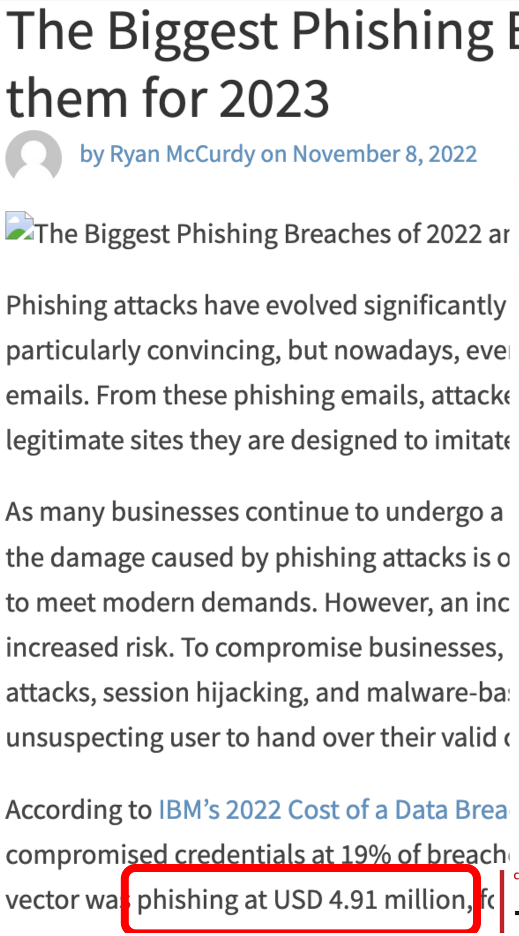
Copy URL

Phishing attacks continue to be one of the most significant threats facing organizations today. As businesses increasingly rely on digital communication channels, cybercriminals exploit vulnerabilities in email, SMS, and voice communications to launch sophisticated phishing attacks. With the COVID-19 pandemic leading to a 1 remote work over the past several years, the risk of phishing attacks has only increased.

Total Observed Phishing Attacks By Year



Phishing Attacks, 2021-2023



The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023

by Ryan McCurdy on November 8, 2022

The Biggest Phishing Breaches of 2022 ar

Phishing attacks have evolved significantly particularly convincing, but nowadays, eve emails. From these phishing emails, attacke legitimate sites they are designed to imitate

As many businesses continue to undergo a the damage caused by phishing attacks is o to meet modern demands. However, an inc increased risk. To compromise businesses, attacks, session hijacking, and malware-ba unsuspecting user to hand over their valid

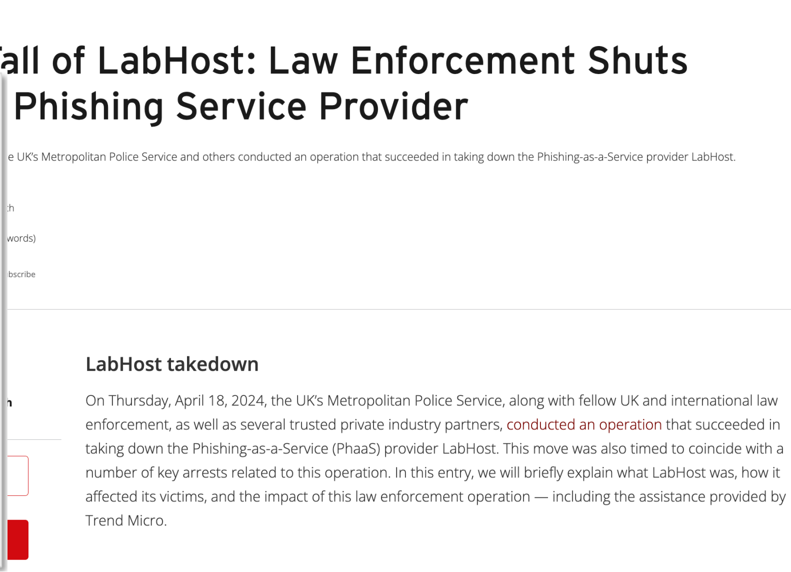
According to IBM's 2022 Cost of a Data Brea compromised credentials at 19% of breach vector was phishing at USD 4.91 million, fo

ConnectWise closes XSS vector for remote hijack scams

Adam Bannister 25 November 2022 at 15:00 UTC

Vulnerabilities Hacking Tools XSS

Researchers also applaud abandonment of customization feature abused by scammers



Cybercrime

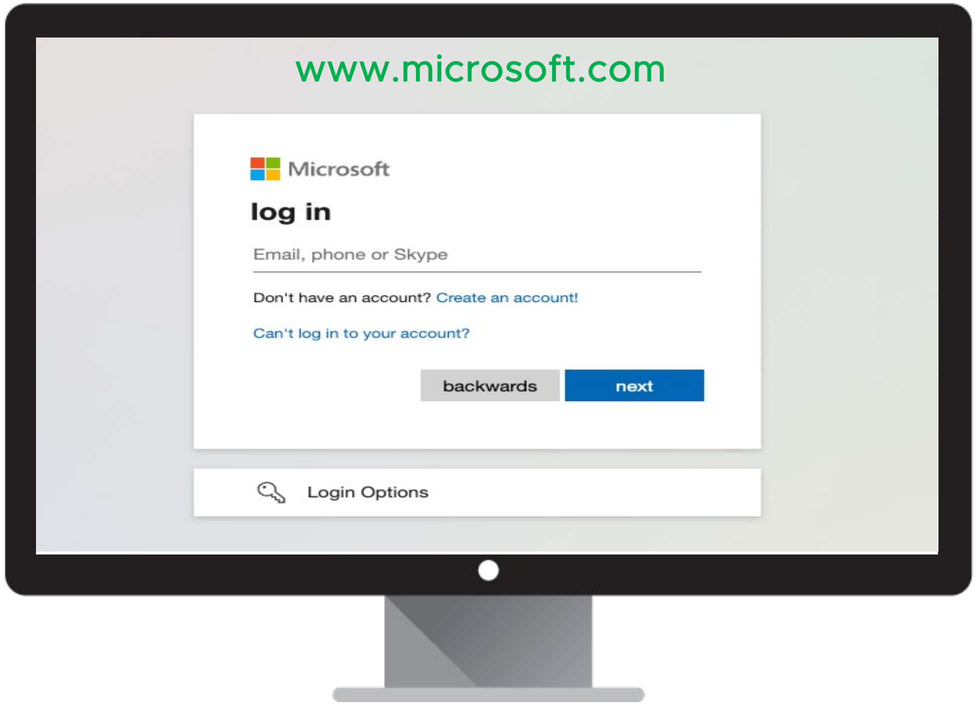
The Fall of LabHost: Law Enforcement Shuts Phishing Service Provider

e UK's Metropolitan Police Service and others conducted an operation that succeeded in taking down the Phishing-as-a-Service provider LabHost.

LabHost takedown

On Thursday, April 18, 2024, the UK's Metropolitan Police Service, along with fellow UK and international law enforcement, as well as several trusted private industry partners, conducted an operation that succeeded in taking down the Phishing-as-a-Service (PhaaS) provider LabHost. This move was also timed to coincide with a number of key arrests related to this operation. In this entry, we will briefly explain what LabHost was, how it affected its victims, and the impact of this law enforcement operation — including the assistance provided by Trend Micro.

Phishing Attacks



www.microsoft.com

Microsoft

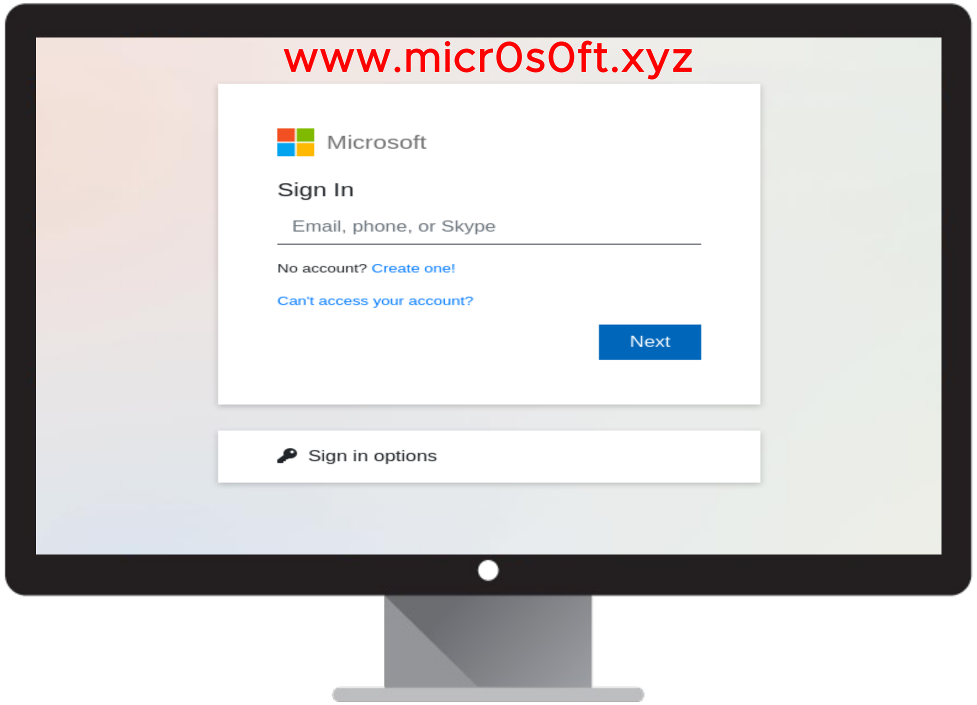
log in

Email, phone or Skype

Don't have an account? Create an account!

Can't log in to your account?

Benign



www.micr0s0ft.xyz

Microsoft

Sign In

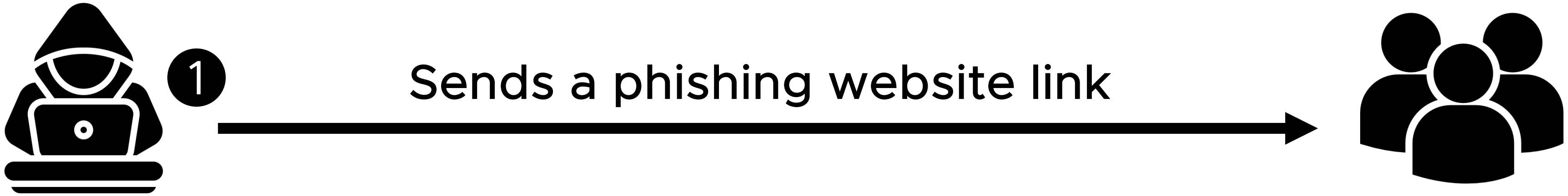
Email, phone, or Skype

No account? Create one!

Can't access your account?

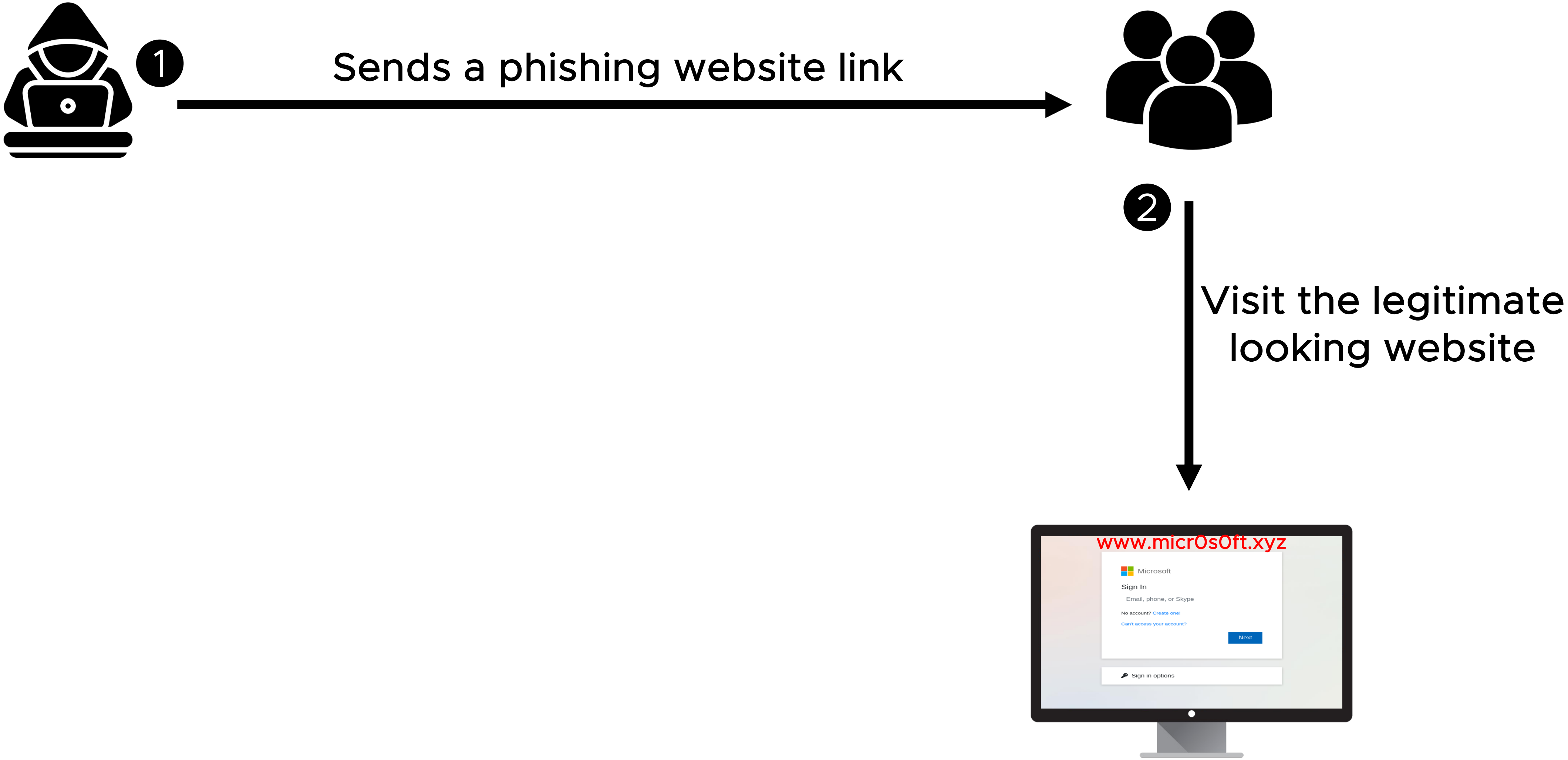
Phishing

Phishing! (How does phishing attack work?)



❶ Sends a phishing website link

Phishing! (How does phishing attack work?)



1 Sends a phishing website link

2 Visit the legitimate looking website

www.micr0s0ft.xyz

Microsoft

Sign In

Email, phone, or Skype

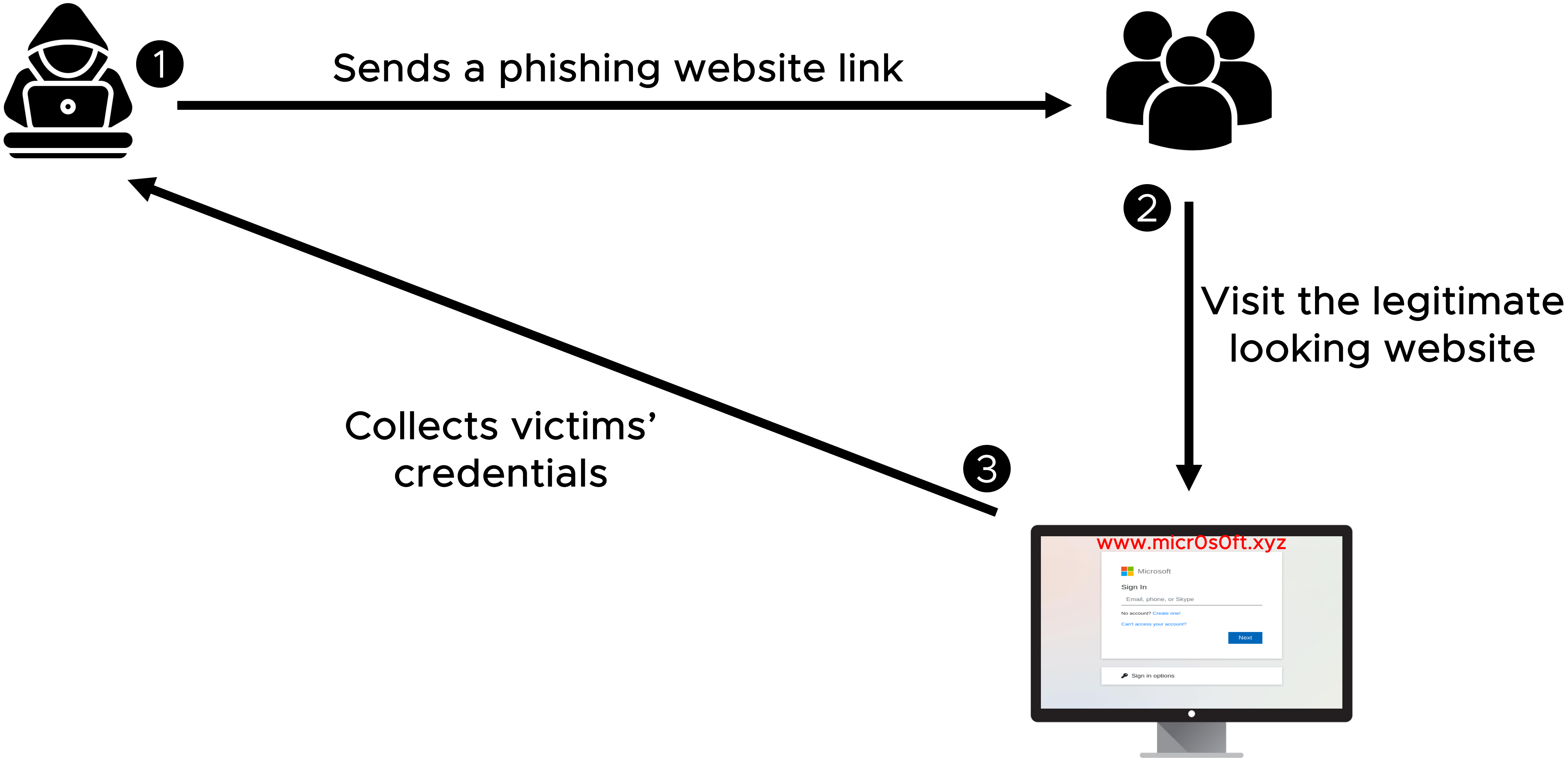
No account? Create one!

Can't access your account?

Next

Sign in options

Phishing! (How does phishing attack work?)

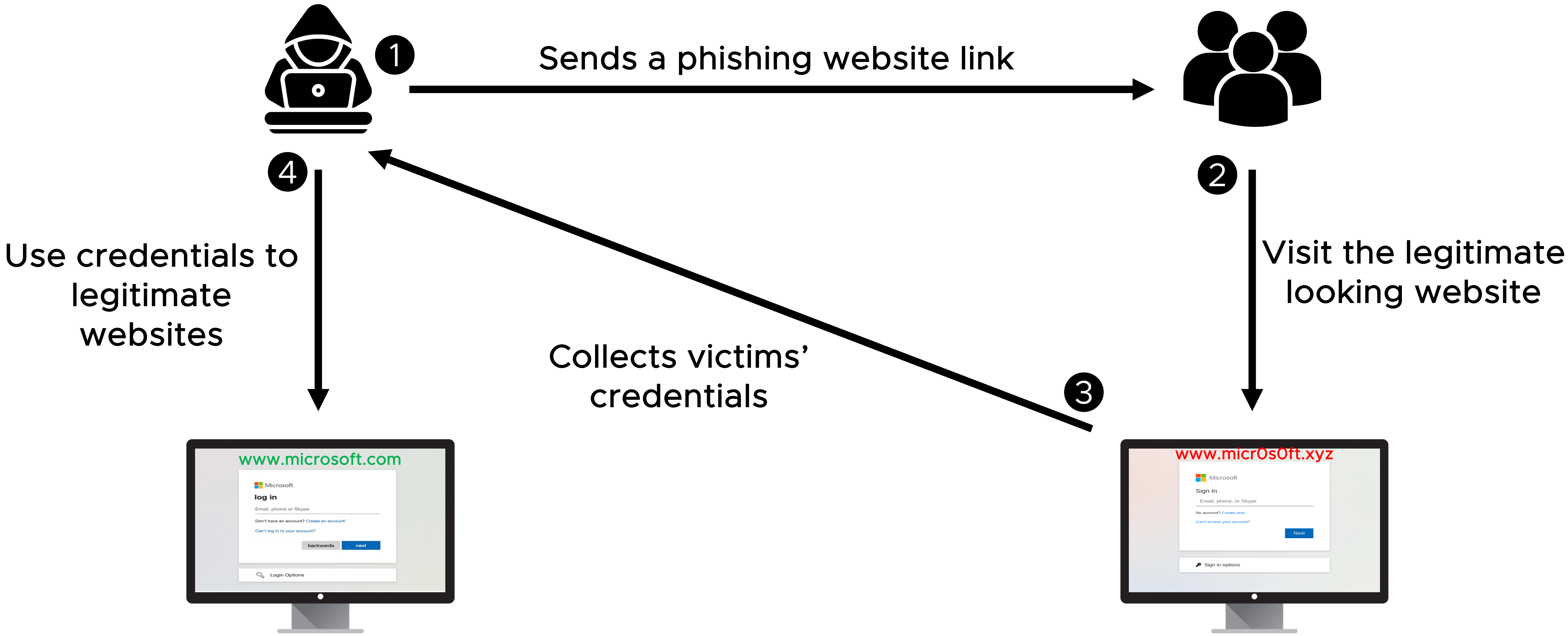


1 Sends a phishing website link

2 Visit the legitimate looking website

3 Collects victims' credentials

Phishing! (How does phishing attack work?)



1 Sends a phishing website link

2 Visit the legitimate looking website

3 Collects victims' credentials

4 Use credentials to legitimate websites

www.microsoft.com

Don't have an account? Create an account!

Can't log in to your account?

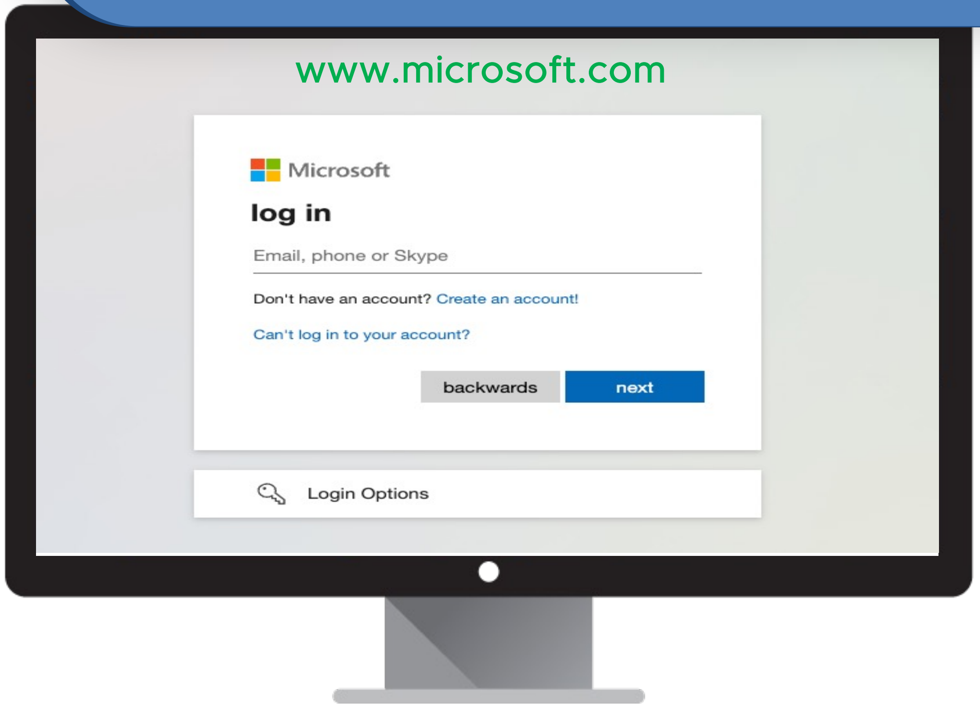
www.micr0s0ft.xyz

No account? Create one!

Can't access your account?

Goal of Phishing Attacks

Lure victim by providing similar looking websites



www.microsoft.com

Microsoft

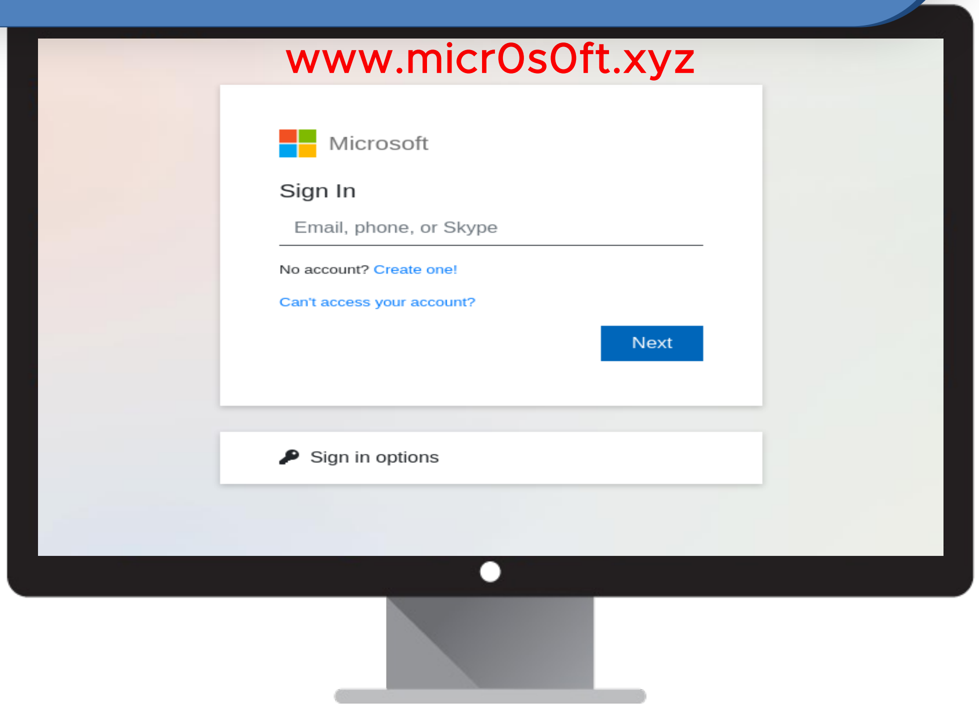
log in

Email, phone or Skype

Don't have an account? Create an account!

Can't log in to your account?

Benign



www.micr0s0ft.xyz

Microsoft

Sign In

Email, phone, or Skype

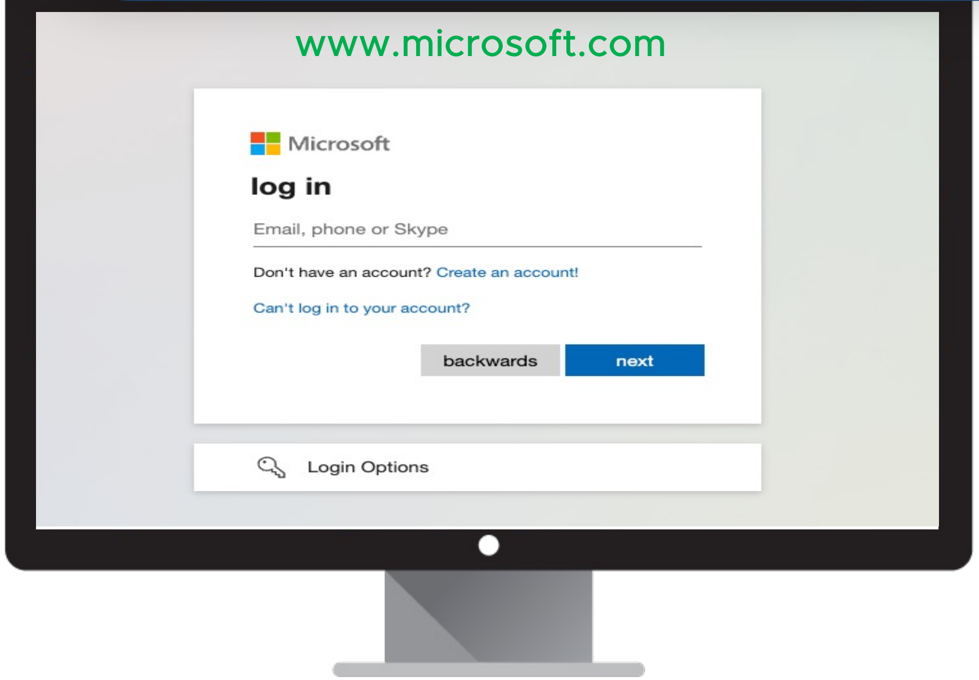
No account? Create one!

Can't access your account?

Phishing

Goal of Phishing Attacks

How do phishing attackers create legitimate looking website?



www.microsoft.com

Microsoft

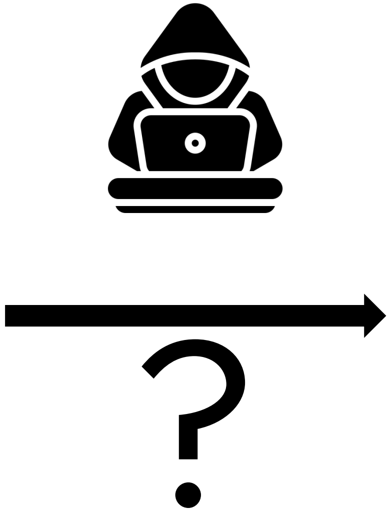
log in

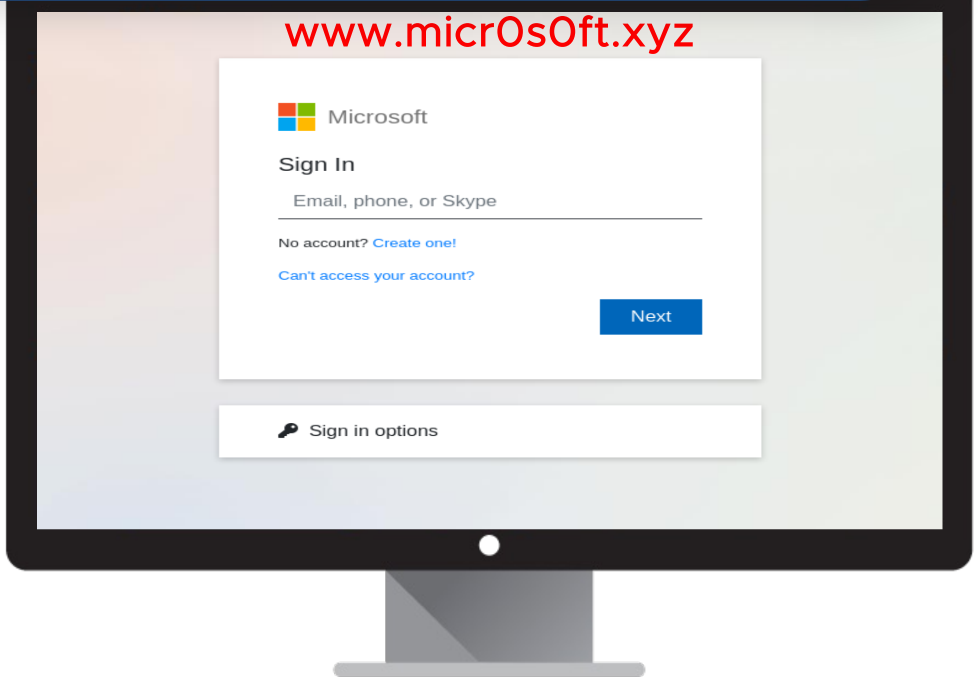
Email, phone or Skype

Don't have an account? Create an account!

Can't log in to your account?

Benign





www.micr0s0ft.xyz

Microsoft

Sign In

Email, phone, or Skype

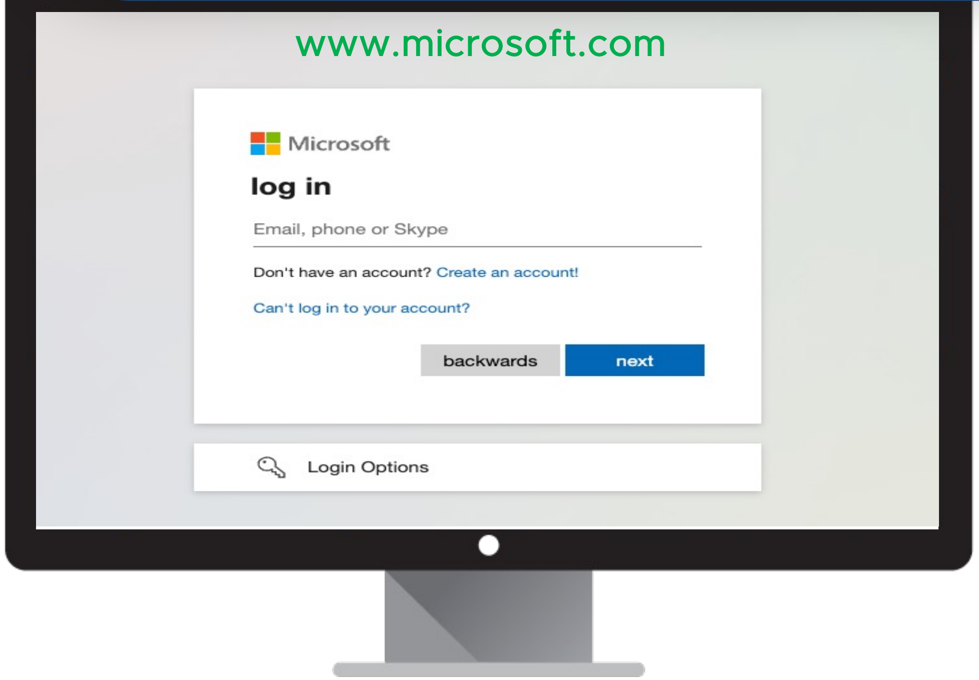
No account? Create one!

Can't access your account?

Phishing

Goal of Phishing Attacks

How do phishing attackers create legitimate looking website?


www.microsoft.com

Microsoft

log in

Email, phone or Skype

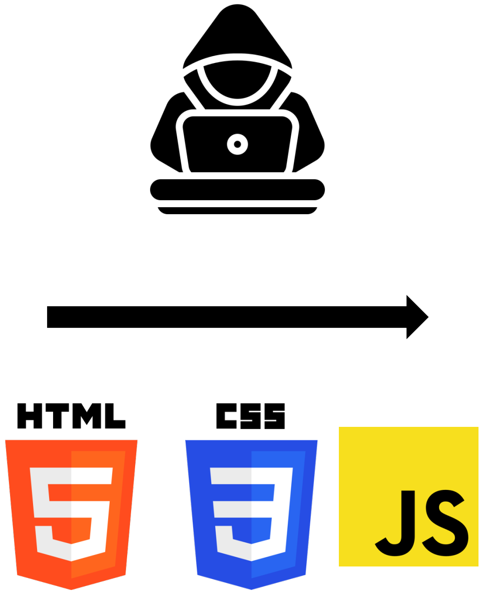
Don't have an account? Create an account!

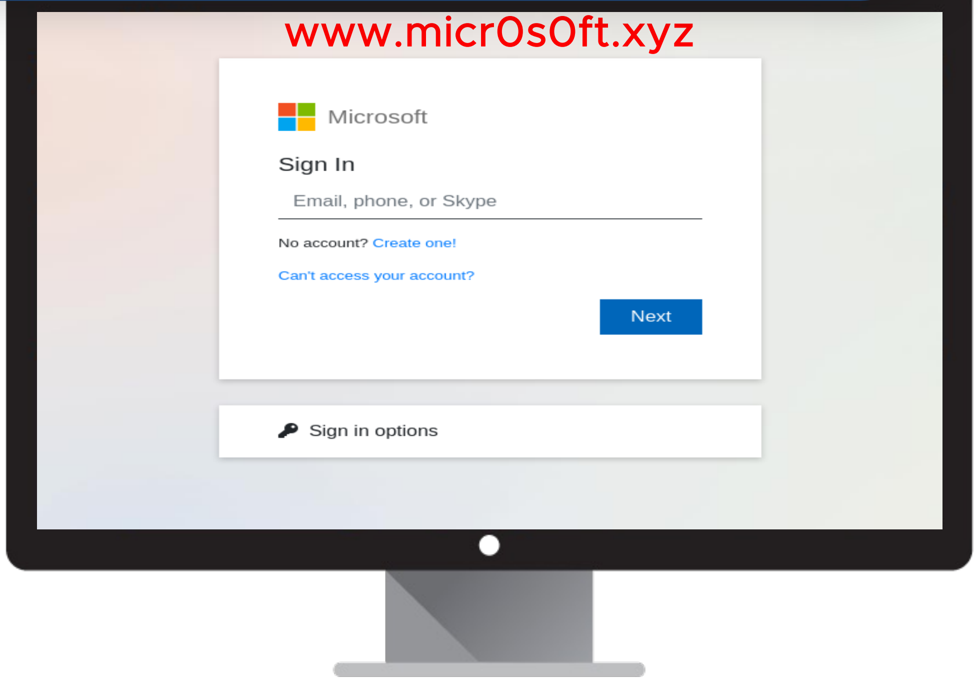
Can't log in to your account?

backwards next

Login Options

Benign




www.micr0s0ft.xyz

Microsoft

Sign In

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

Sign in options

Phishing

Comparison with Previous Work

- No comparison study on client-side resources between benign and phishing websites
  - Not focused on client-side resource in phishing (S&P ‘19, CCS ’22, USENIX ‘21)
- No measurement study on phishing website
  - Experimental study with phishing websites (S&P ‘19, USENIX ’20)

Research Question

RQ1 What kind of client-side resources are employed in phishing websites?

RQ2 Which JavaScript libraries are widely prevalent in phishing websites?

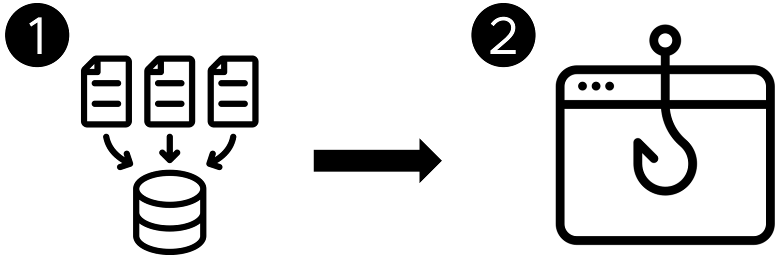
RQ3 How similar are phishing websites and their corresponding legitimate target brand?

To Compare Phishing Vs. Legit

1

APWG Feed
(phishing URLs)

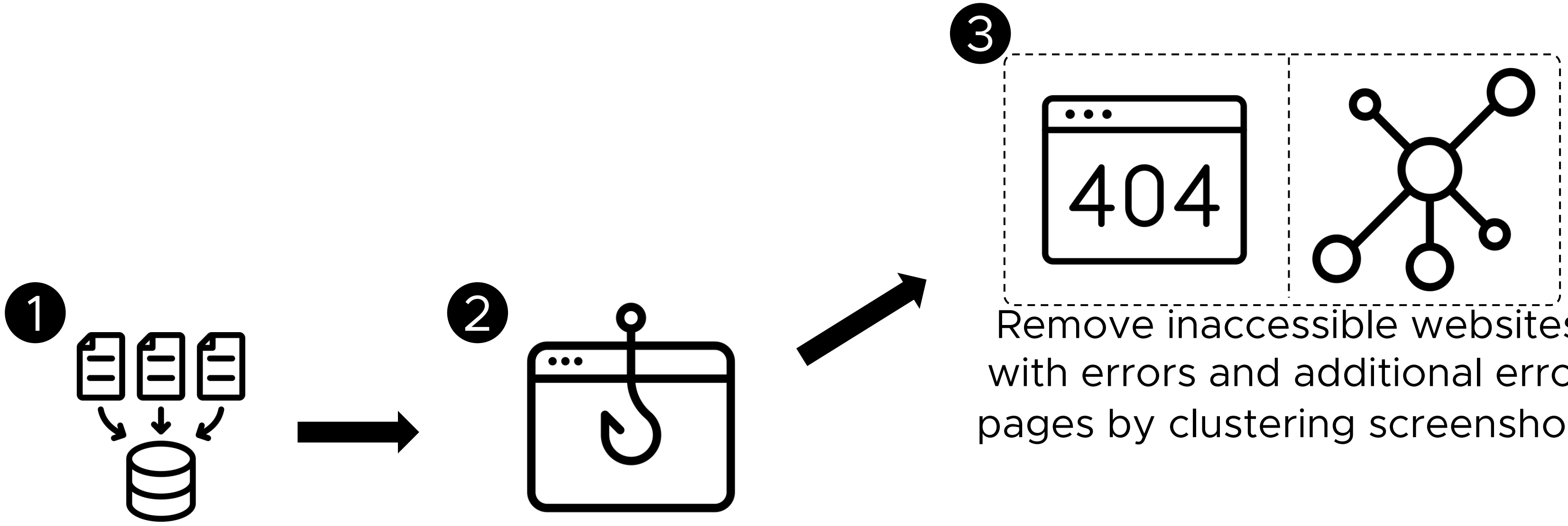
To Compare Phishing Vs. Legit



APWG Feed
(phishing URLs)

Access and collect
phishing websites

To Compare Phishing Vs. Legit

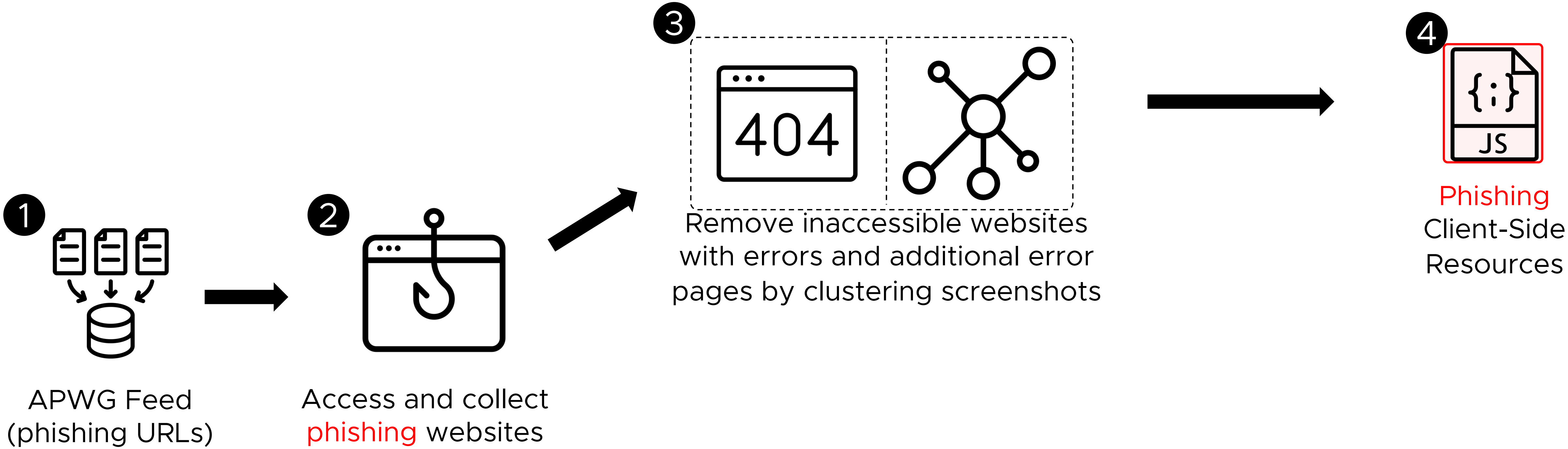


1 APWG Feed (phishing URLs)

2 Access and collect phishing websites

3 Remove inaccessible websites with errors and additional error pages by clustering screenshots

To Compare Phishing Vs. Legit



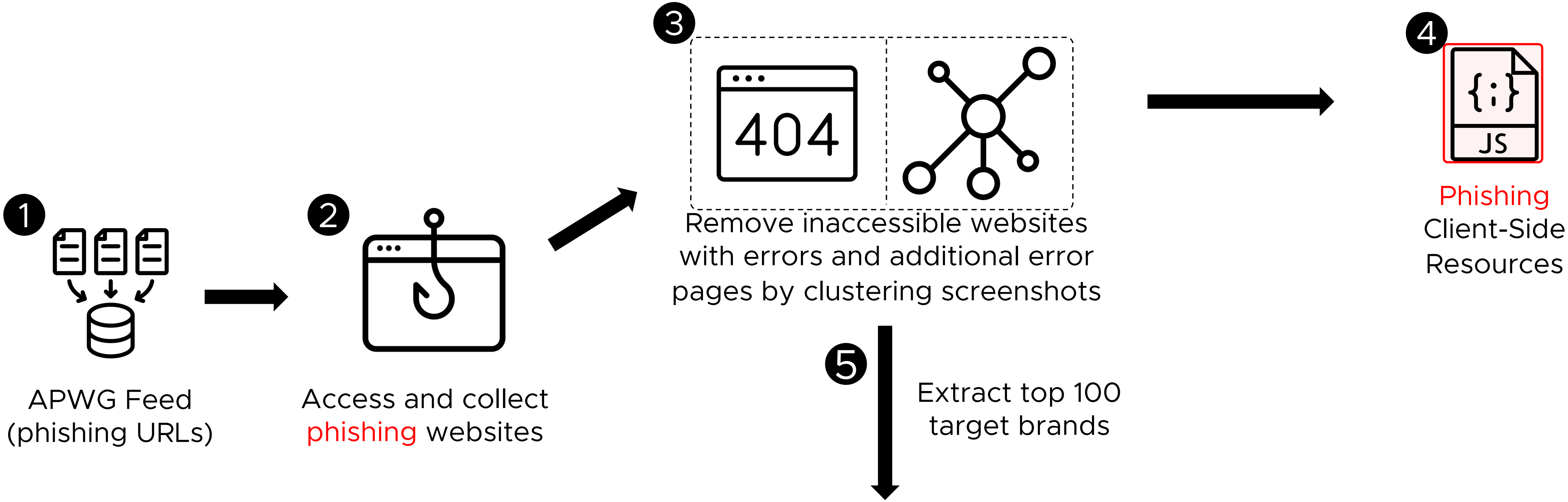
APWG Feed (phishing URLs)

Access and collect phishing websites

Remove inaccessible websites with errors and additional error pages by clustering screenshots

Phishing Client-Side Resources

To Compare Phishing Vs. Legit



1 APWG Feed (phishing URLs)

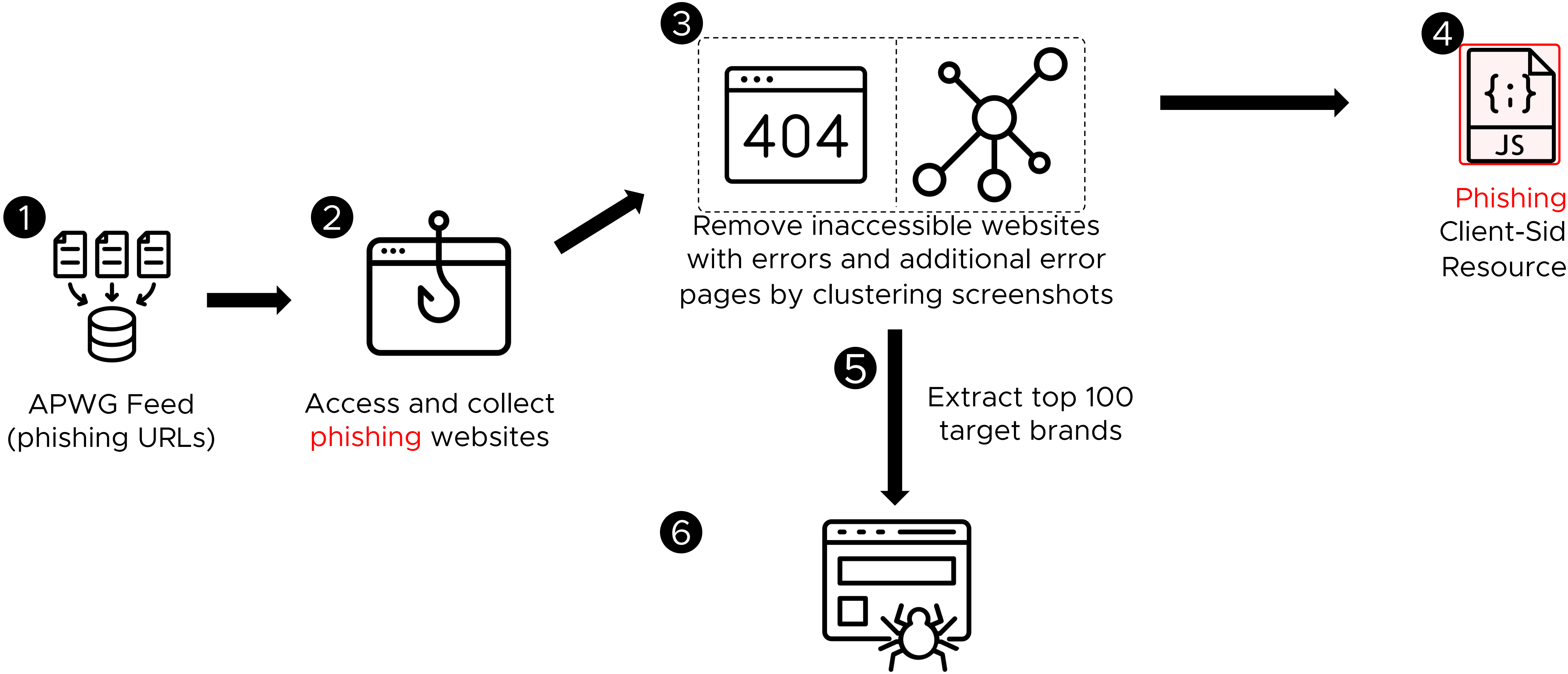
2 Access and collect phishing websites

3 Remove inaccessible websites with errors and additional error pages by clustering screenshots

4 Phishing Client-Side Resources

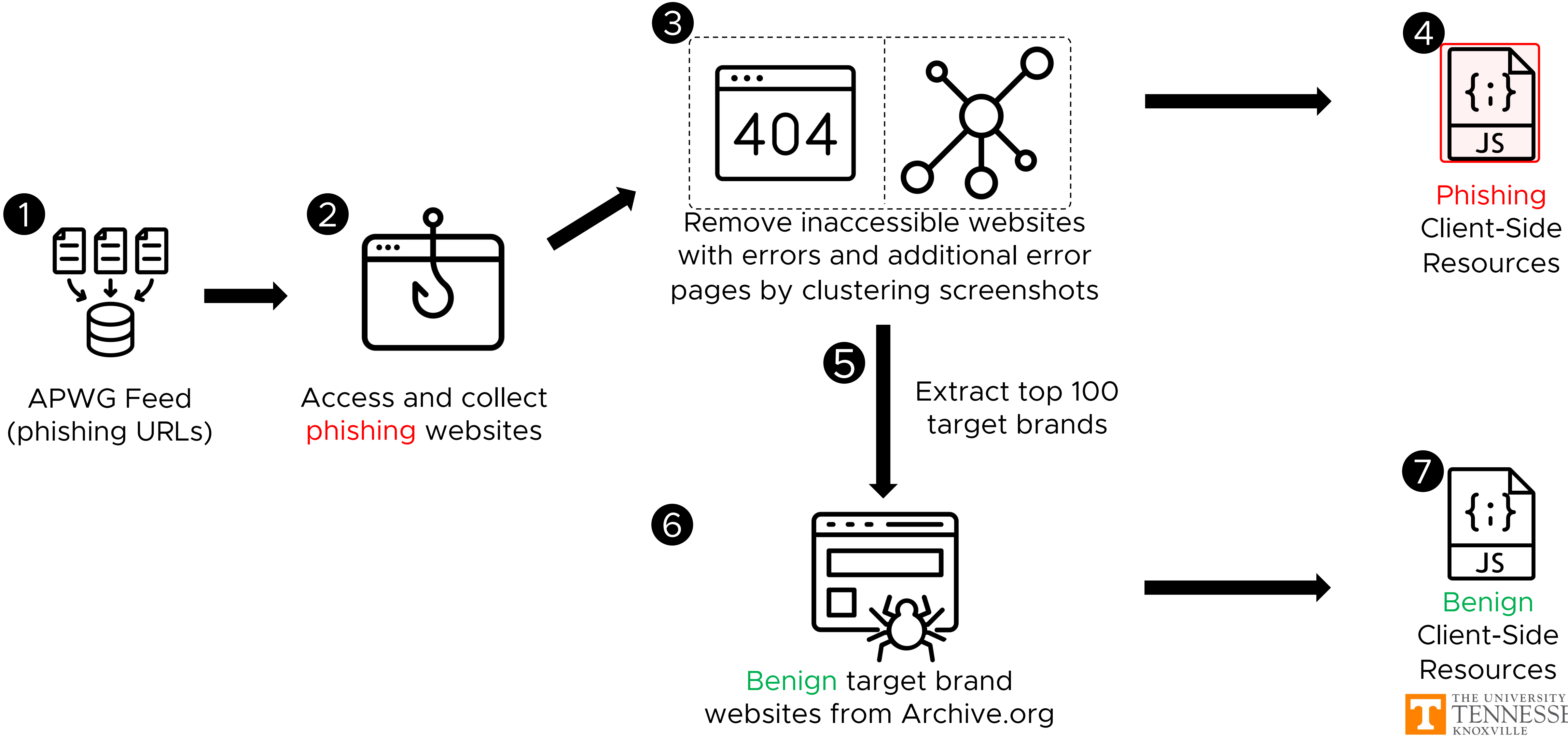
5 Extract top 100 target brands

To Compare Phishing Vs. Legit



1
APWG Feed
(phishing URLs)
2
Access and collect phishing websites
3
404
Remove inaccessible websites with errors and additional error pages by clustering screenshots
4
{;}
JS
Phishing Client-Side Resources
5
Extract top 100 target brands
6
Benign target brand websites from Archive.org

To Compare Phishing Vs. Legit



1 APWG Feed (phishing URLs)

2 Access and collect phishing websites

3 Remove inaccessible websites with errors and additional error pages by clustering screenshots

4 Phishing Client-Side Resources

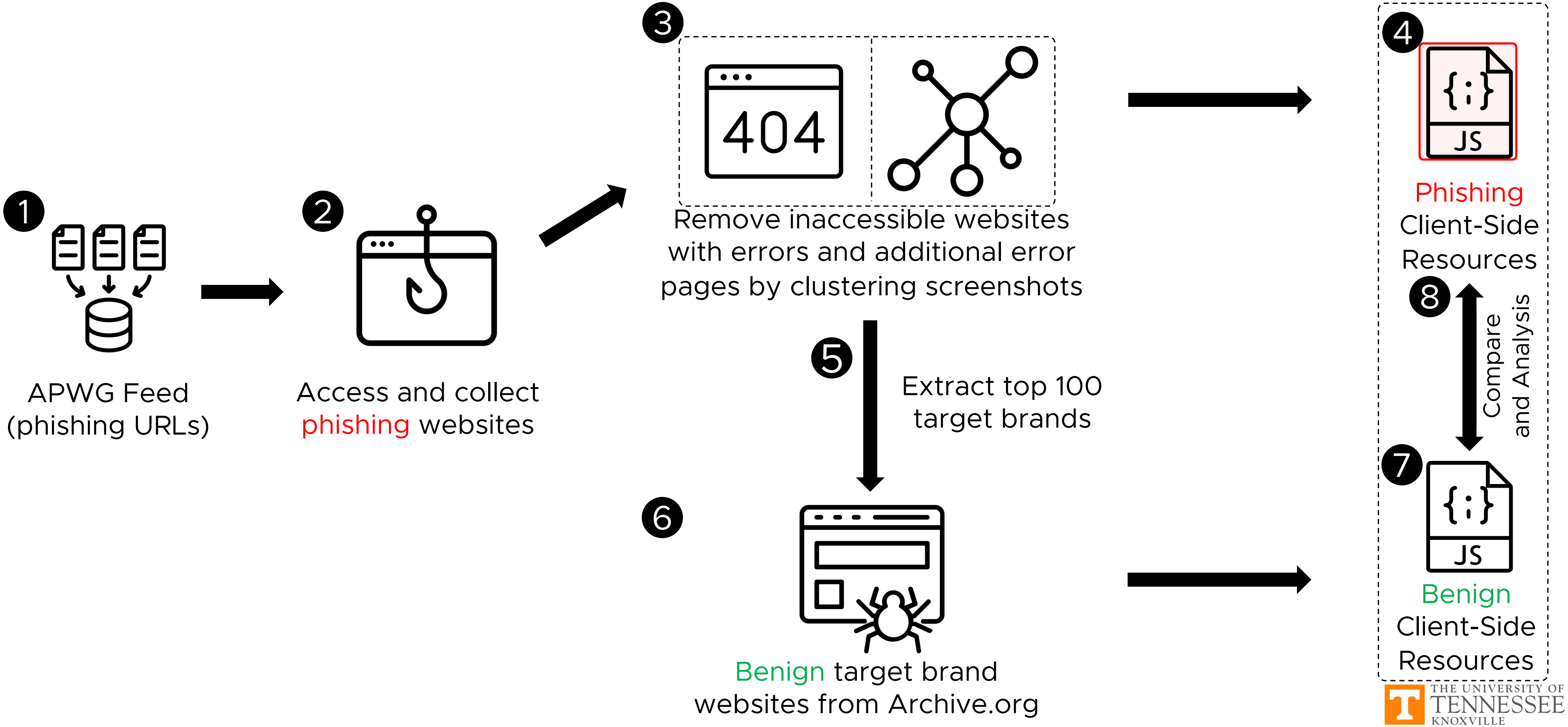
5 Extract top 100 target brands

6 Benign target brand websites from Archive.org

7 Benign Client-Side Resources

THE UNIVERSITY OF TENNESSEE KNOXVILLE

To Compare Phishing Vs. Legit



1 APWG Feed (phishing URLs)

2 Access and collect phishing websites

3 Remove inaccessible websites with errors and additional error pages by clustering screenshots

4 Phishing Client-Side Resources

5 Extract top 100 target brands

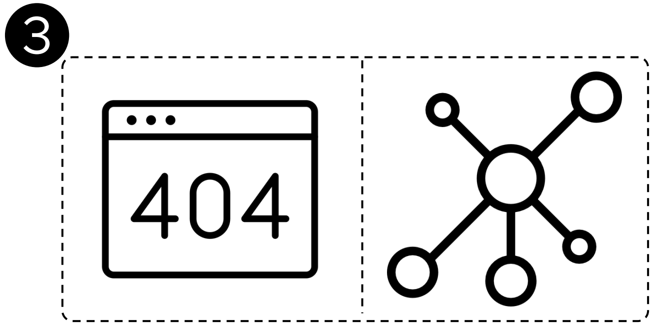
6 Benign target brand websites from Archive.org

7 Benign Client-Side Resources

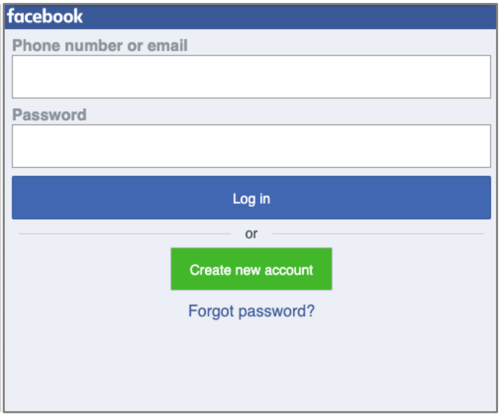
8 Compare and Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

To Compare Phishing Vs. Legit



Remove inaccessible websites with errors and additional error pages by clustering screenshots



facebook

Phone number or email

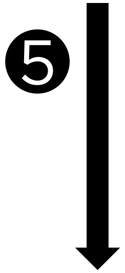
Password

Log in

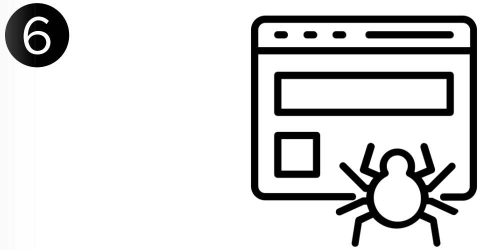
or

Create new account

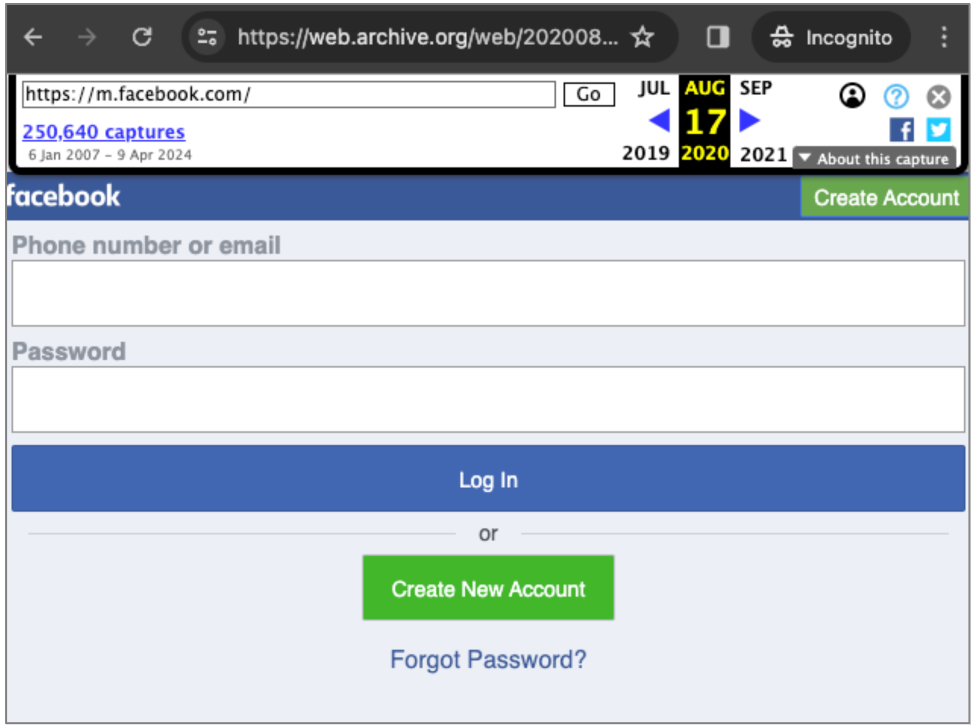
Forgot password?



Extract top 100 target brands



Benign target brand websites from Archive.org



https://web.archive.org/web/202008...

Incognito

https://m.facebook.com/ Go

JUL AUG SEP

250,640 captures

6 Jan 2007 – 9 Apr 2024

17

2019 2020 2021

About this capture

facebook Create Account

Phone number or email

Password

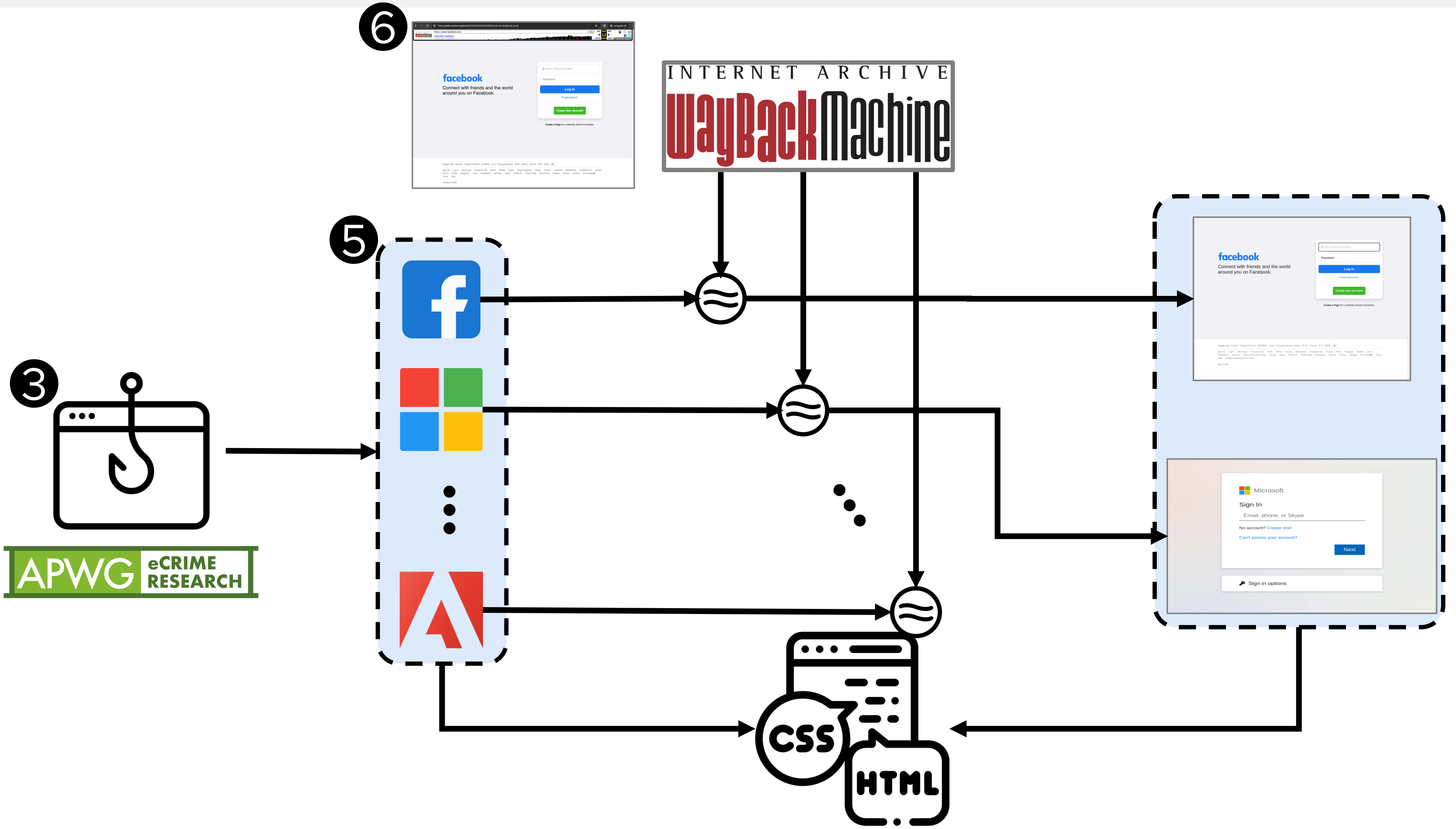
Log In

or

Create New Account

Forgot Password?

Comparison between Phishing vs Legit



Data Collection

Type	# of URLs	# of Domains
APWG Phishing URLs	15,747,193	1,545,253
Accessed URLs	7,067,778	1,135,264
Screenshots	6,125,810	939,103
Refined Dataset	3,388,997	**757,421**
Collection Period	July ‘21 – July ‘23 (25 months)	

Research Question

RQ1 What kind of client-side resources are employed in phishing websites?

RQ2 Which JavaScript libraries are widely prevalent in phishing websites?

RQ3 How similar are phishing websites and their corresponding legitimate target brand?

What Kind of Client-side Resources are Employed in Phishing Websites?

Client-side Resource	Average Usage (%)
JavaScript	82.7%
CSS	72.3%
Favicon	35%
SVC	16.5%
CMS	7.3%
XML	1.5%
…	

Research Question

RQ1 What kind of client-side resources are employed in phishing websites?

RQ2 Which JavaScript libraries are widely prevalent in phishing websites?

RQ3 How similar are phishing websites and their corresponding legitimate target brand?

Dominant Version

- Phishing websites utilize different and outdated versions of JavaScript libraries, compared to their legitimate websites.

Library	Dominant Version (Phishing)	Dominant Version (Legit)
Bootstrap	v4.0.0	v5.0.0
jQuery-UI	v1.10.3	v1.12.1
React	v16.14.0	v17.0.0
Slick	1.6.0	1.8.1

Client-side Resource Comparison

- Phishing websites use specific JavaScript libraries to more effectively attract and trap victims

Library	Usage	Remark
Clipboard.js	13.9%	Popular in phishing
Select2	0.3%	Popular in phishing
SweetAlert2	0.3%	Popular in phishing
Axios	0.9%	Only shown in Phishing
Socket.IO	0.6%	Only shown in Phishing
Hammer.js	0.2%	Only shown in Phishing

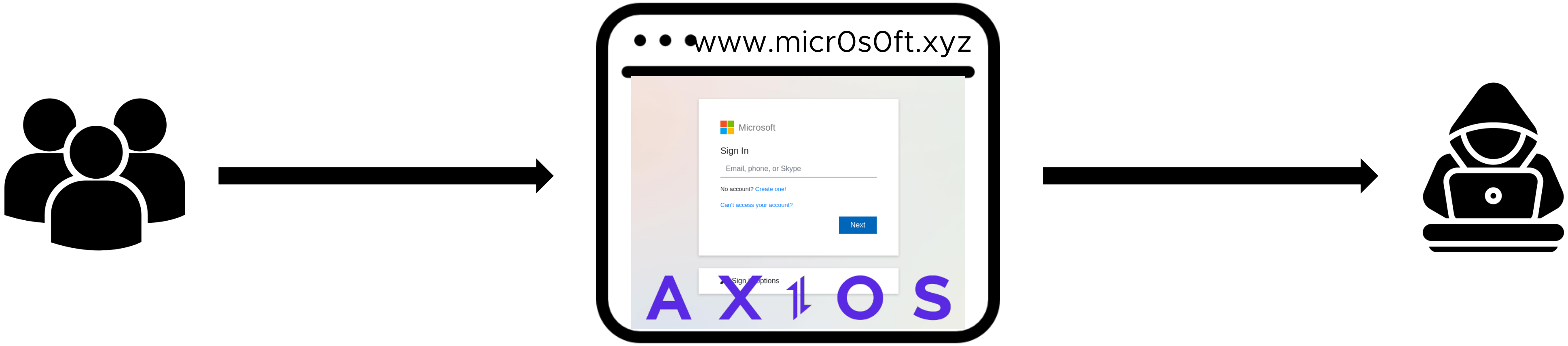
Client-side Resource Comparison

- Phishing websites use specific JavaScript libraries to more effectively attract and trap victims

Library	Usage	Remark
Clipboard.js	13.9%	Popular in phishing
Select2	0.3%	Popular in phishing
SweetAlert2	0.3%	Popular in phishing
Axios	0.9%	Only shown in Phishing
Socket.IO	0.6%	Only shown in Phishing
Hammer.js	0.2%	Only shown in Phishing

Use Case of JS Library in Phishing (Axios)

- Phishing sites use specific JavaScript libraries to more effectively attract and trap victims

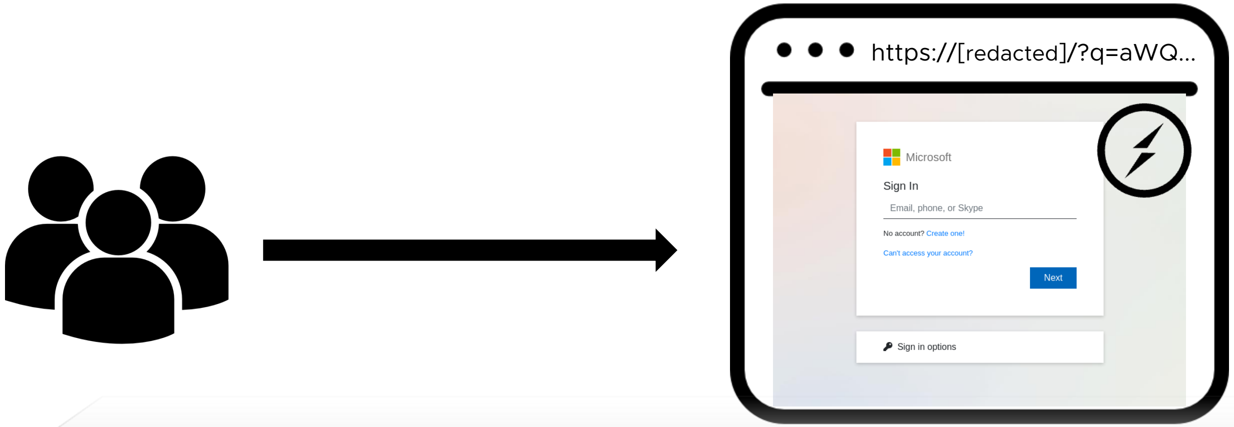


Using Axios library to exfiltrate the user’s information

```
data.append('email', email);
data.append('password', password);
```

Use Case of JS Library in Phishing (Socket.IO)

- Phishing sites use specific JavaScript libraries to more effectively attract and trap victims

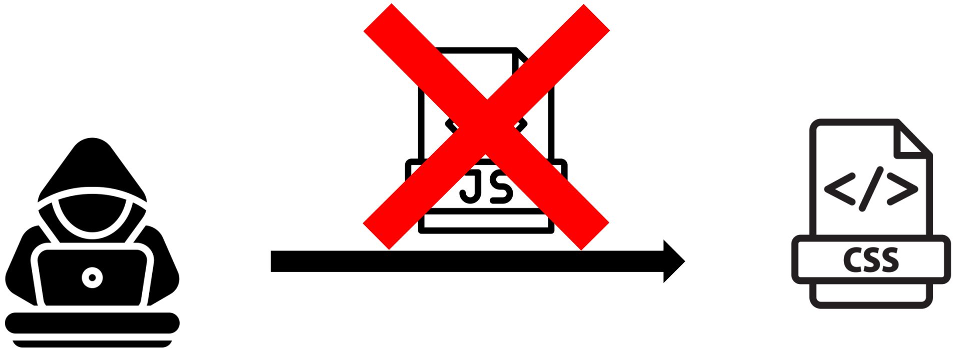


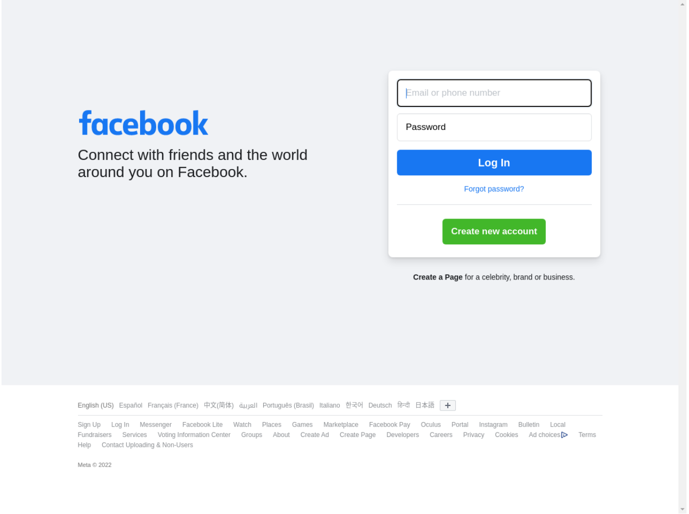
Socket.IO decodes parameter and sends the identification to the external server in real-time

https://[redacted]/?q=aWQ9c2MwbV9sYW5nPWVzX3NjPTc3NV91c2VyPTYyMzc0NjE3NDY%3D

https://[redacted]/?q=d=sc0m_lang=es_sc=775_user=62374617467

Phishing without JavaScript





facebook

Connect with friends and the world around you on Facebook.

Email or phone number

Password

Log In

Forgot password?

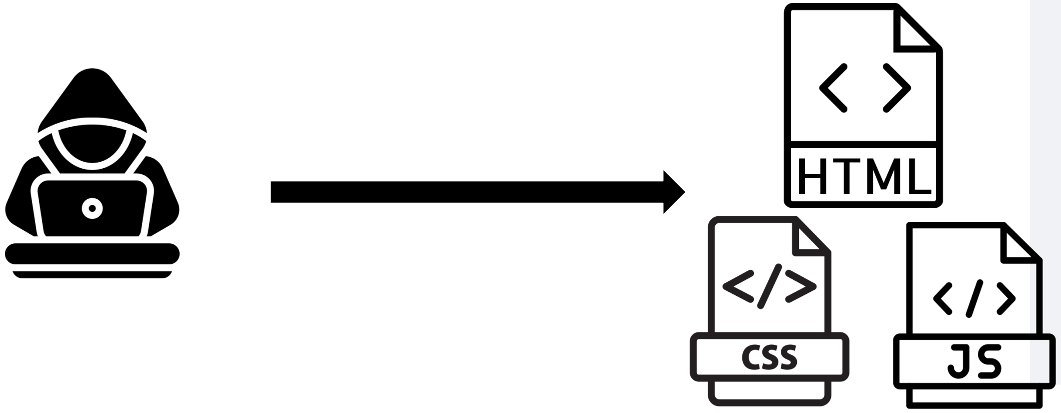
Create new account

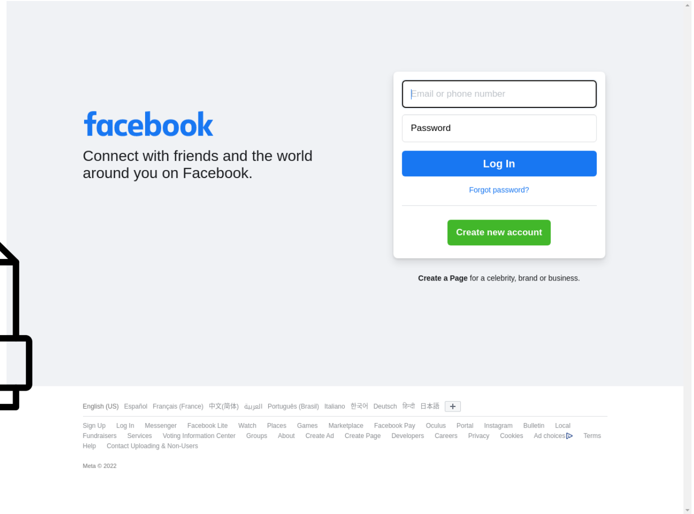
Create a Page for a celebrity, brand or business.

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Oculus Portal Instagram Bulletin Local Fundraisers Services Voting Information Center Groups About Create Ad Create Page Developers Careers Privacy Cookies Ad choices Terms Help Contact Uploading & Non-Users

Meta © 2022





facebook

Connect with friends and the world around you on Facebook.

Email or phone number

Password

Log In

Forgot password?

Create new account

Create a Page for a celebrity, brand or business.

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Oculus Portal Instagram Bulletin Local Fundraisers Services Voting Information Center Groups About Create Ad Create Page Developers Careers Privacy Cookies Ad choices Terms Help Contact Uploading & Non-Users

Meta © 2022

Research Question

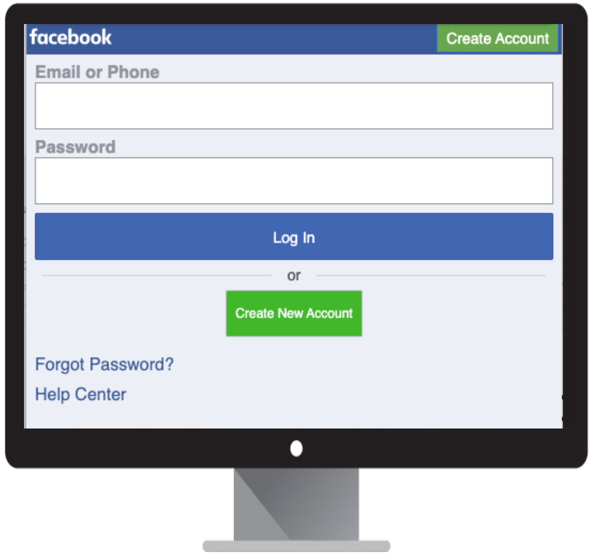
RQ1 What kind of client-side resources are employed in phishing websites?

RQ2 Which JavaScript libraries are widely prevalent in phishing websites?

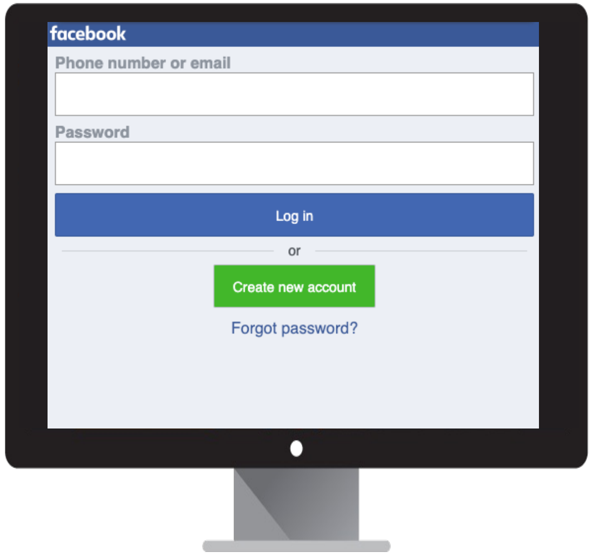
RQ3 How similar are phishing websites and their corresponding legitimate target brand?

Mimicking from Old Versions of Websites

- Phishing websites possibly copied from older version of websites



Benign website on 01/03/2018



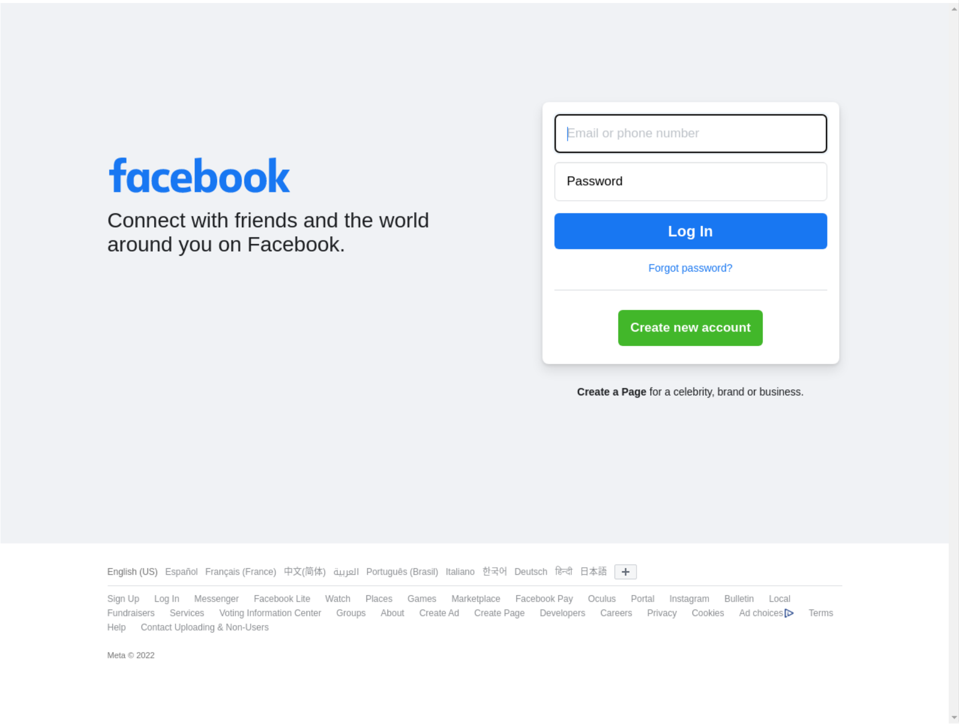
Phishing website detected on 07/14/2022

Mimicking from Old Versions of Websites

Brand	First Seen	Mimicked-Date	Diff.
Facebook	2021-07-11	2020-08-12	333
Microsoft	2021-07-11	2018-01-03	1,285
Instagram	2022-10-20	2022-05-10	163
AT&T	2022-09-11	2022-09-10	1
WhatsApp	2022-02-11	2021-10-08	116
DHL	2023-03-09	2020-03-31	1,073
Ozon	2021-09-30	2021-03-27	187
Yahoo	2021-10-08	2017-01-01	1,741
Wells Fargo	2021-11-08	2019-04-23	930
Adobe	2023-02-12	2023-01-17	26

Mimicking from Old Versions of Websites

Brand	First Seen	Mimicked-Date	Diff.
Facebook	2021-07-11	2020-08-12	333



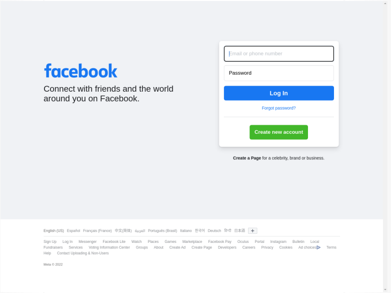
facebook

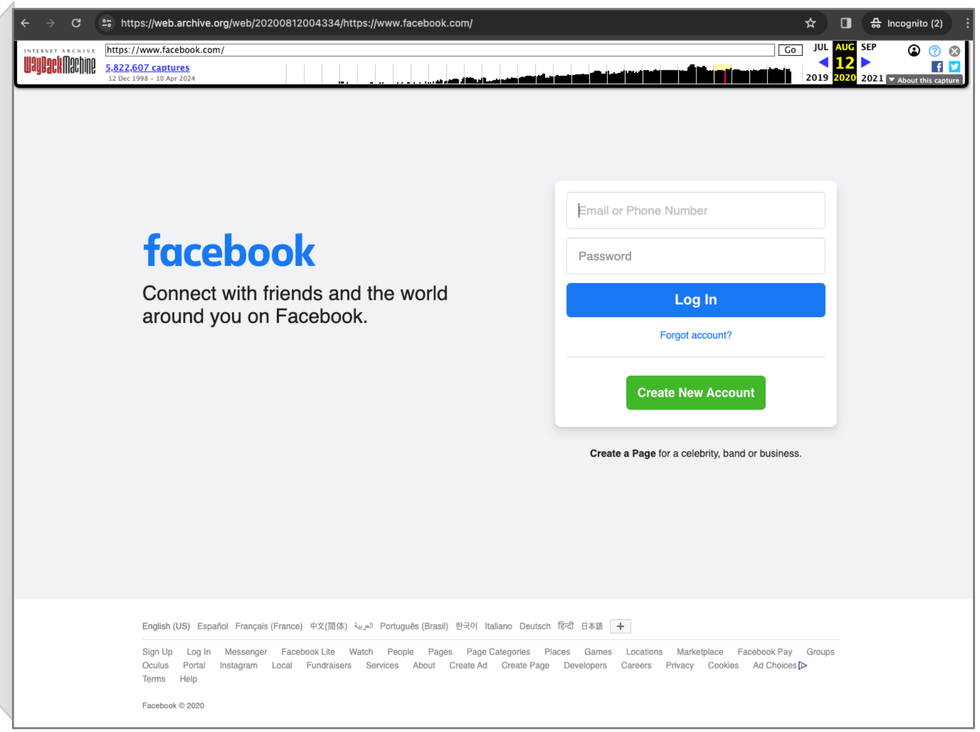
Connect with friends and the world around you on Facebook.

Create a Page for a celebrity, brand or business.

Meta © 2022

Email or phone number
Password
Log In
Forgot password?
Create new account
English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +
Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Oculus Portal Instagram Bulletin Local
Fundraisers Services Voting Information Center Groups About Create Ad Create Page Developers Careers Privacy Cookies Ad choices Terms
Help Contact Uploading & Non-Users





https://web.archive.org/web/20200812004334/https://www.facebook.com/

facebook

Connect with friends and the world around you on Facebook.

Create a Page for a celebrity, band or business.

Facebook © 2020

Incognito (2)
INTERNET ARCHIVE WaybackMachine
https://www.facebook.com/
Go
5,822,607 captures
12 Dec 1998 - 10 Apr 2024
JUL AUG SEP
12
2019 2020 2021
About this capture
Email or Phone Number
Password
Log In
Forgot account?
Create New Account
English (US) Español Français (France) 中文(简体) العربية Português (Brasil) 한국어 Italiano Deutsch हिन्दी 日本語 +
Sign Up Log In Messenger Facebook Lite Watch People Pages Page Categories Places Games Locations Marketplace Facebook Pay Groups
Oculus Portal Instagram Local Fundraisers Services About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices
Terms Help

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Takeaway

T1 Phishing sites often use a broader range of JavaScript libraries than legitimate site

T2 A large proportion of these sites still retain basic designs, like plain login forms without using JS

T3 Phishing websites mimic from older version of target benign websites