Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach

Ruofan Liu, Yun Lin*, Xianglin Yang, Siang Hwee Ng, Dinil Mon Divakaran, Jin Song Dong

Presenter: Yun Lin

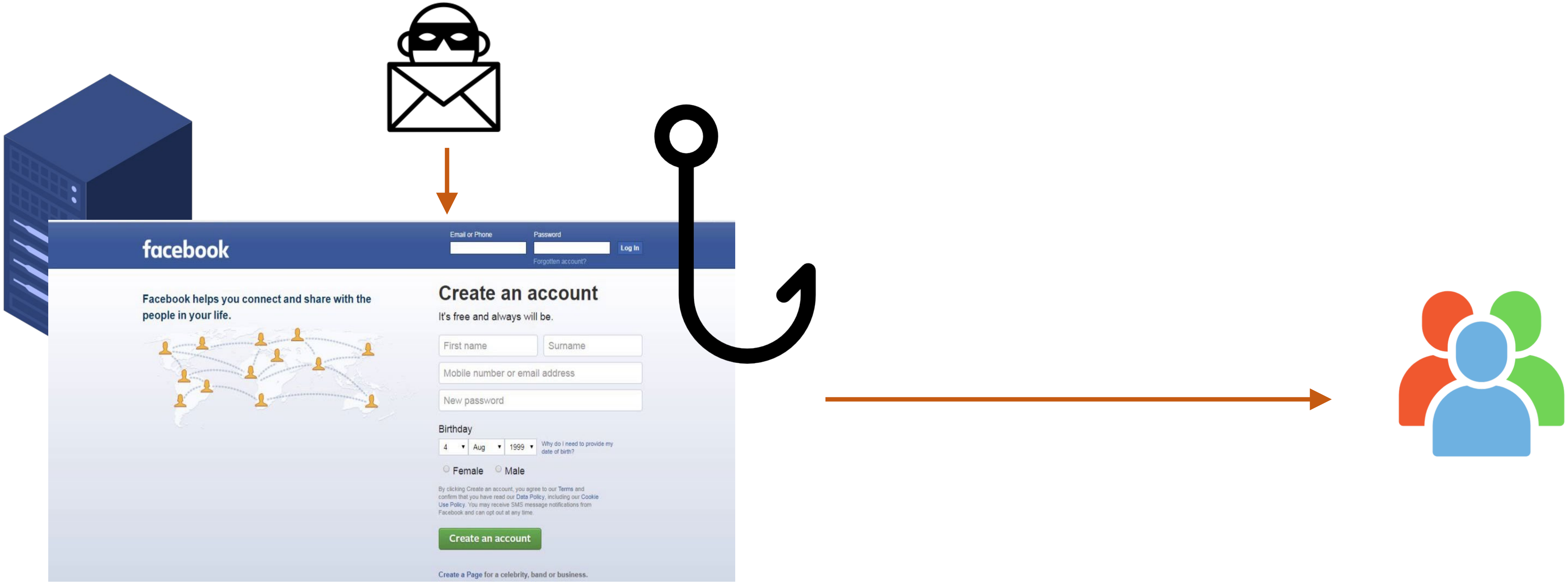
National University of Singapore

(Research Assistant Professor)

Shanghai Jiao Tong University

(incoming Associate Professor)

Phishing Attack



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

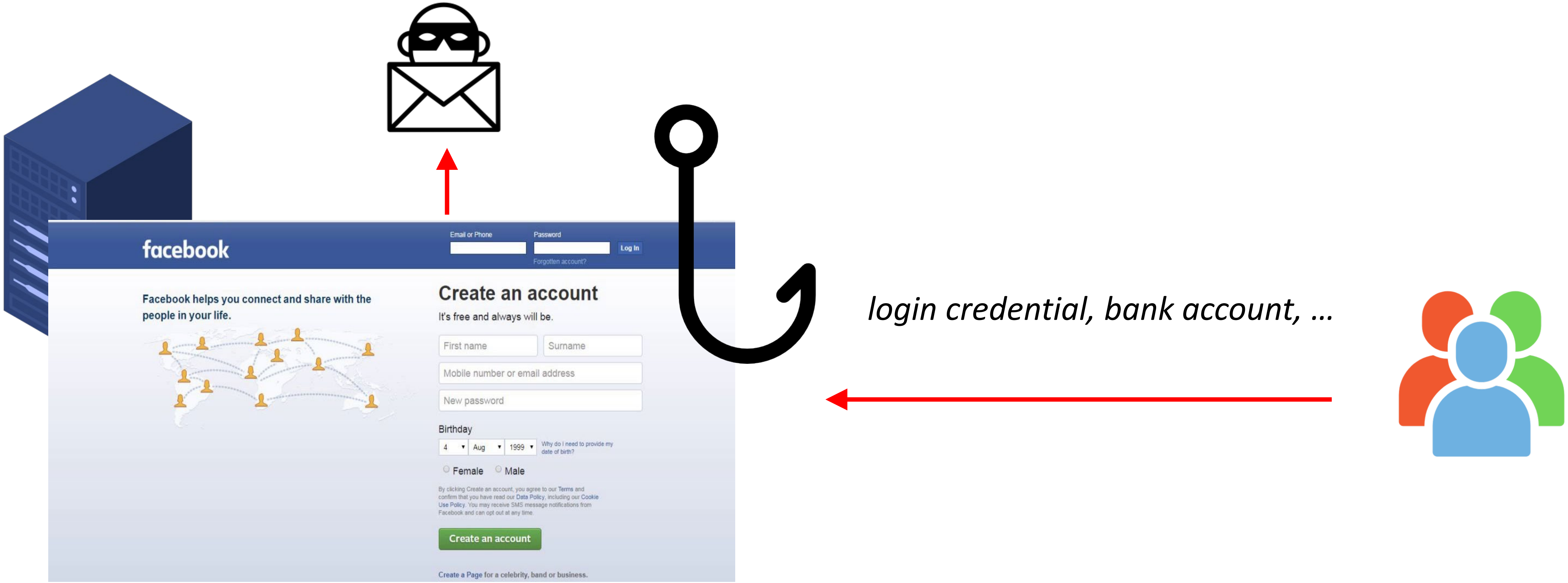
By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

Phishing site

Phishing Attack



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

login credential, bank account, …

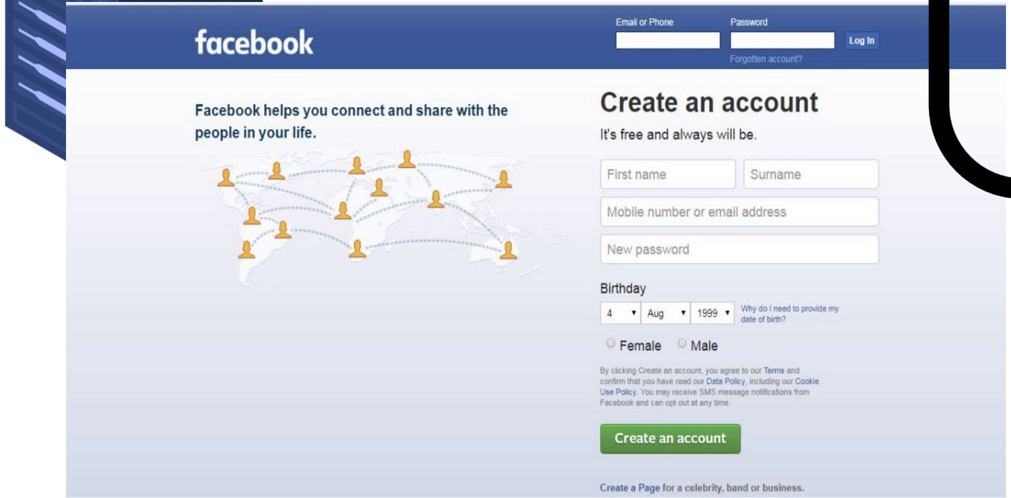
Phishing site

Phishing Attack

transfer money

deliver misinformation

start new attacks (e.g., deploying trojan)



Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

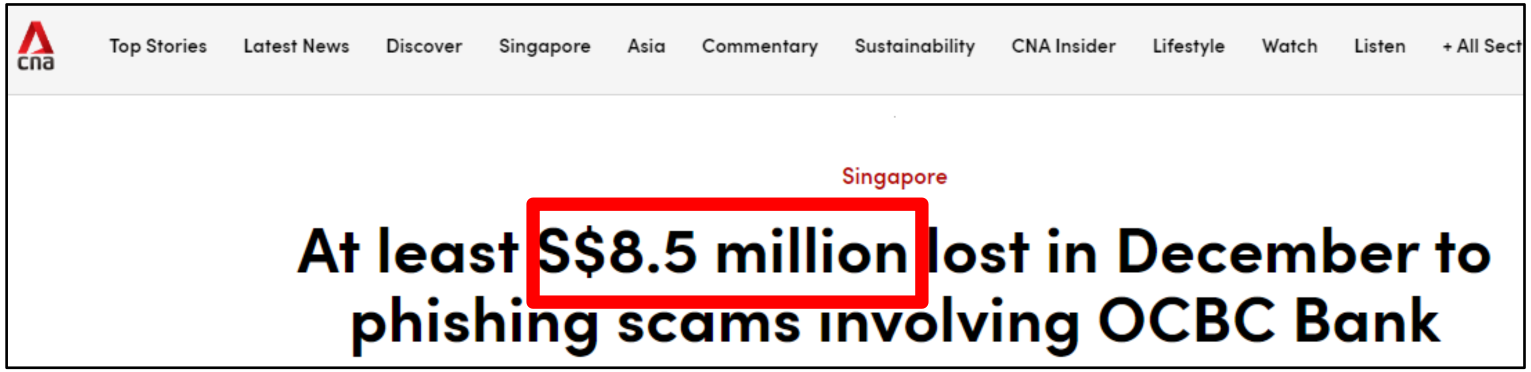
○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create a Page for a celebrity, band or business.

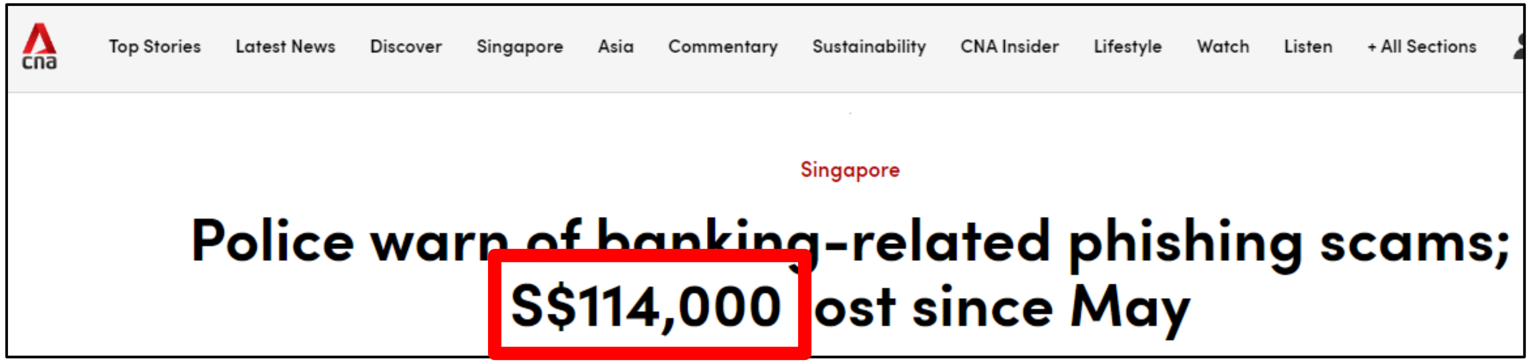
Phishing site

login credential, bank account, …



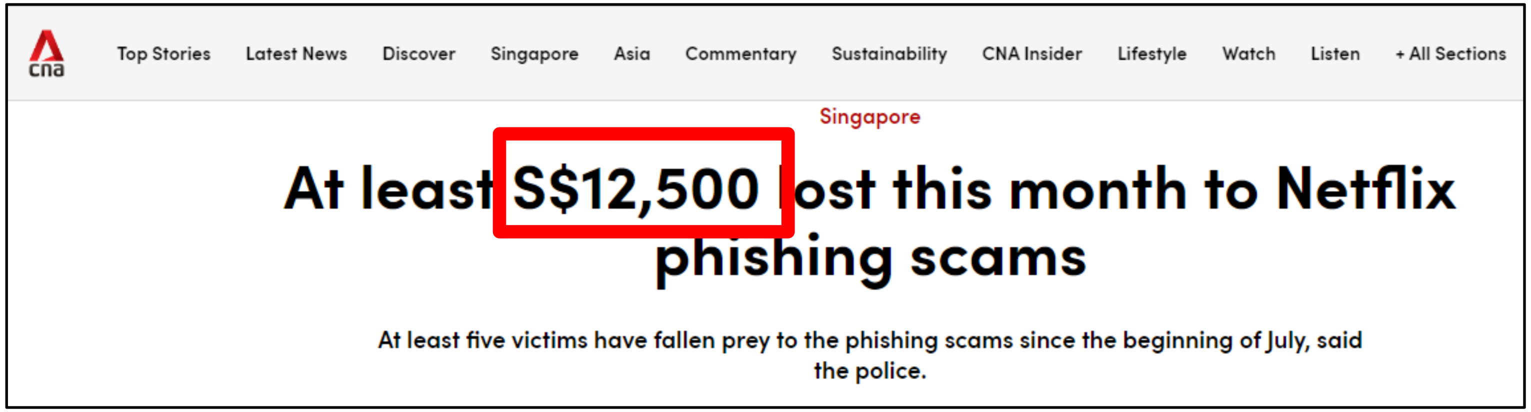
Singapore

At least S$8.5 million lost in December to phishing scams involving OCBC Bank



Singapore

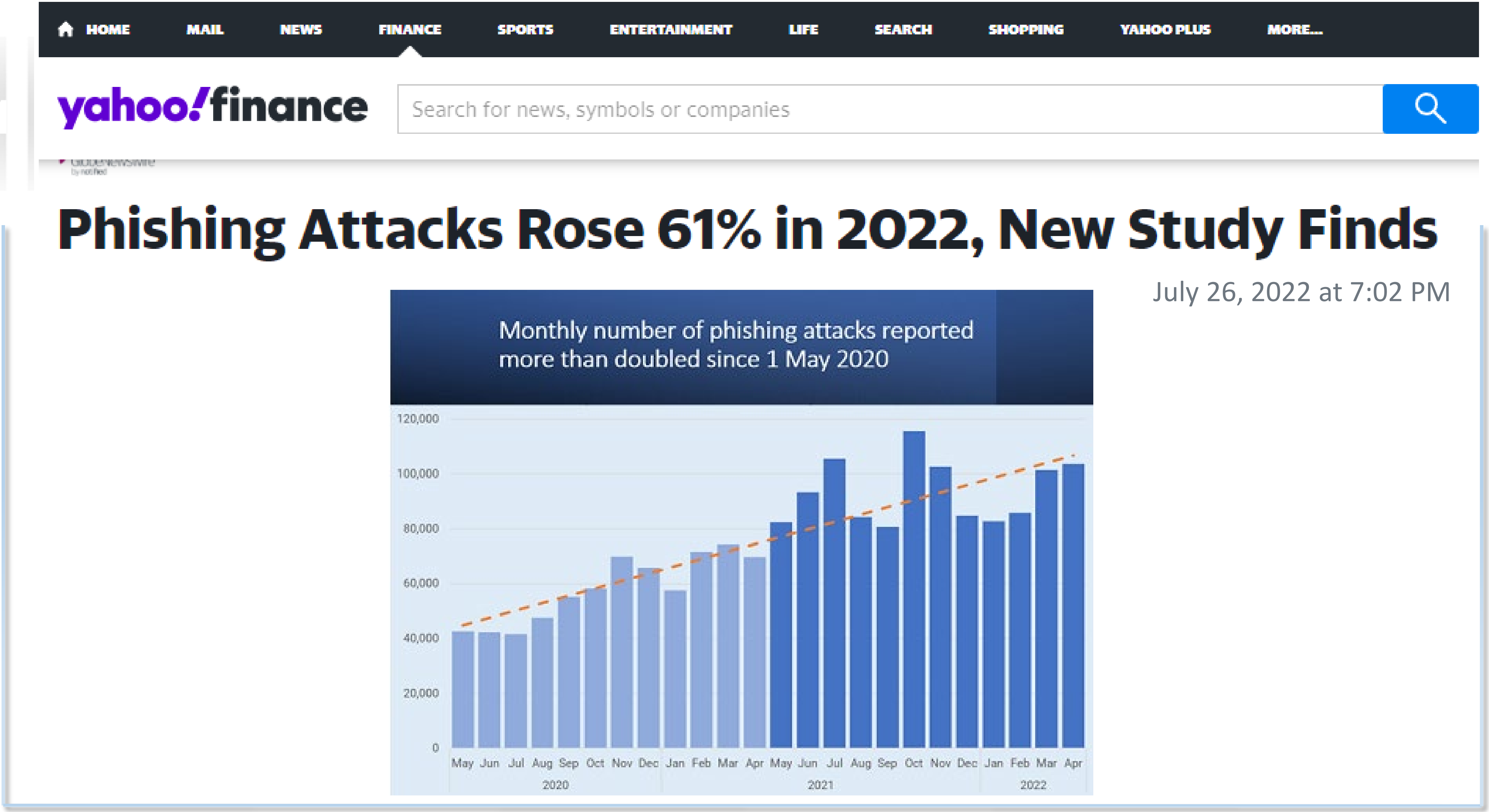
Police warn of banking-related phishing scams; S$114,000 lost since May



Singapore

At least S$12,500 lost this month to Netflix phishing scams

At least five victims have fallen prey to the phishing scams since the beginning of July, said the police.

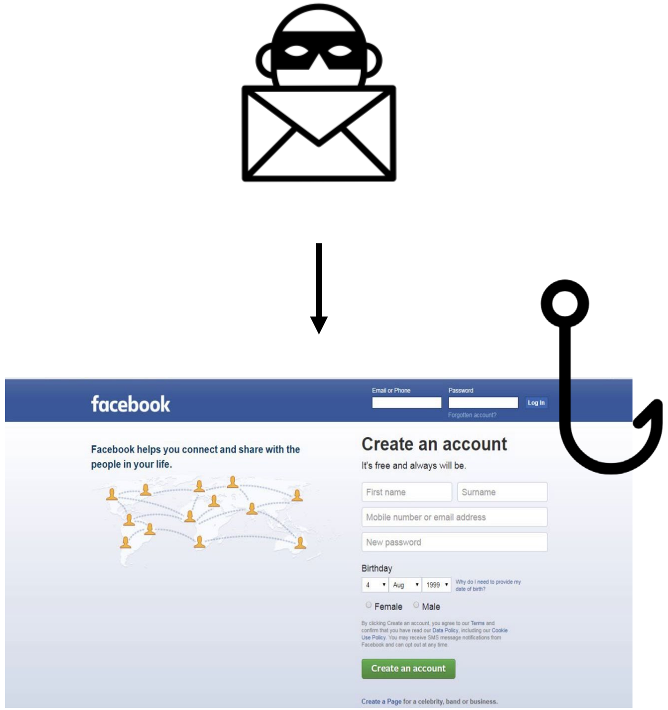


Phishing Attacks Rose 61% in 2022, New Study Finds

July 26, 2022 at 7:02 PM

Monthly number of phishing attacks reported more than doubled since 1 May 2020

Cat-and-mouse Game



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

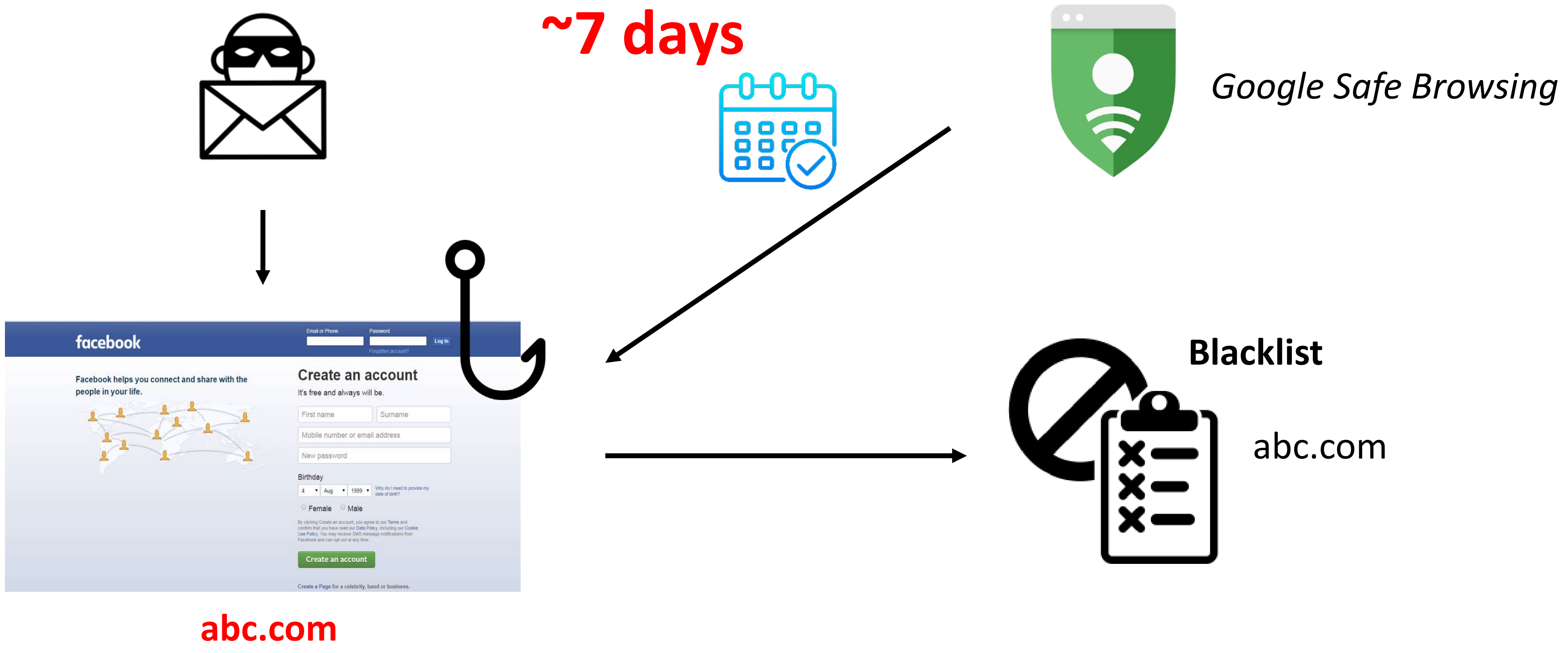
Create a Page for a celebrity, band or business.

abc.com

Google Safe Browsing

Blacklist

Cat-and-mouse Game



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

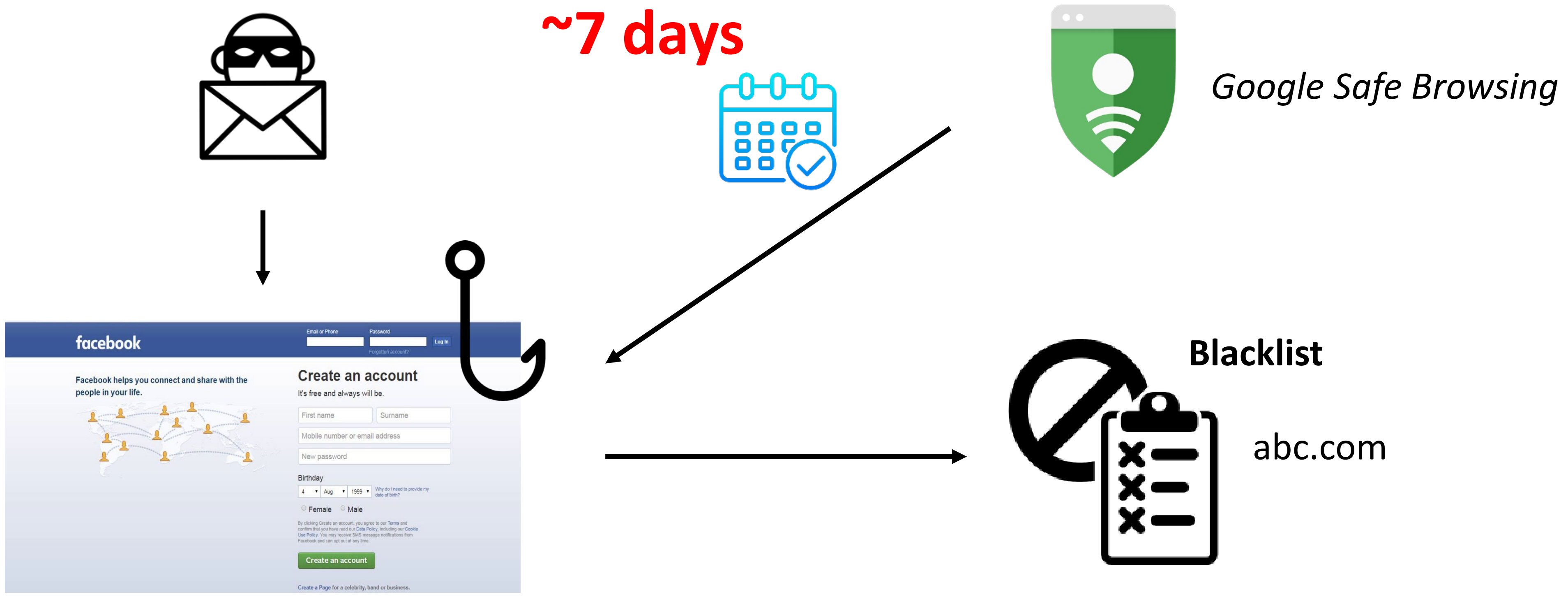
○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

Cat-and-mouse Game



Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name
Surname
Mobile number or email address
New password
Birthday
4
Aug
1999
Why do I need to provide my date of birth?
○ Female
○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create a Page for a celebrity, band or business.

~7 days

Google Safe Browsing

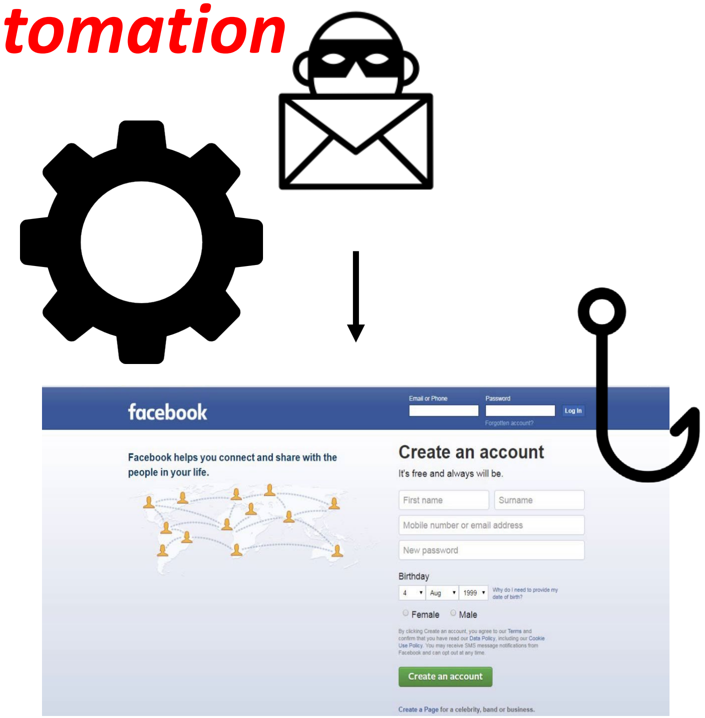
Blacklist

abc.com

~~abc.com~~ efg.com

Cat-and-mouse Game

Full Automation



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

~~abc.com~~ ~~efg.com~~ … xyz.com

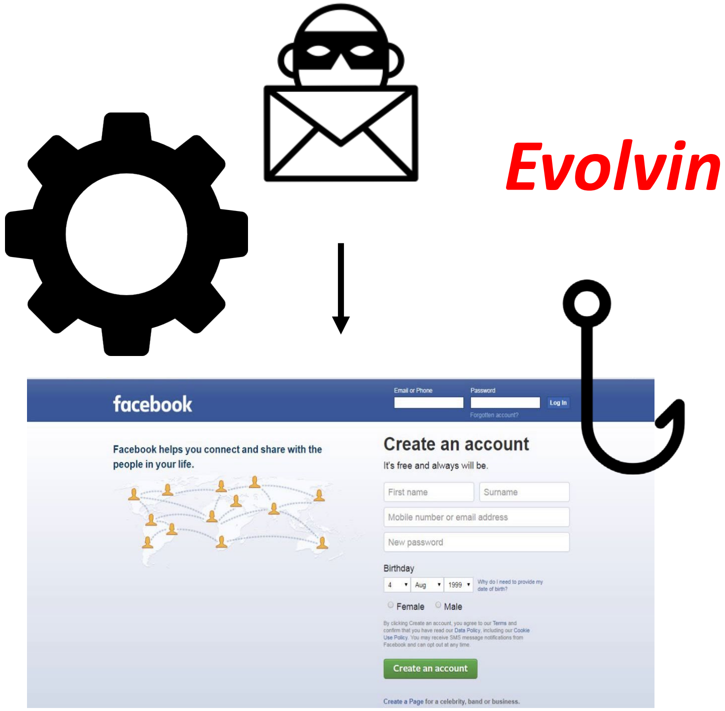
Update every week

Google Safe Browsing

Blacklist

abc.com
efg.com
…

Cat-and-mouse Game



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾

Why do I need to provide my date of birth?

○ Female ○ Male

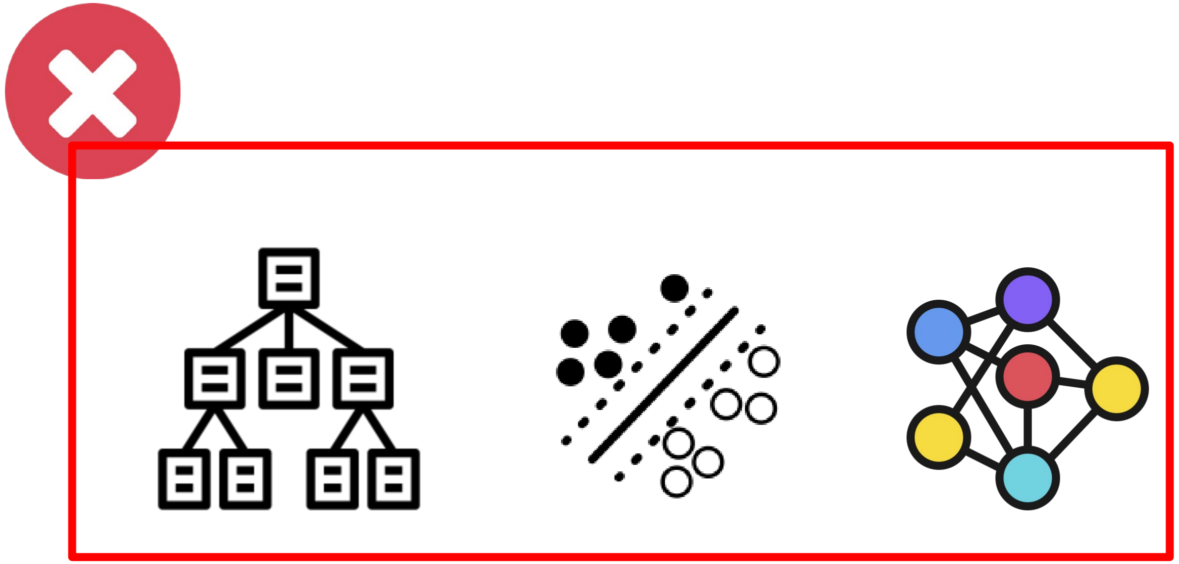
By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

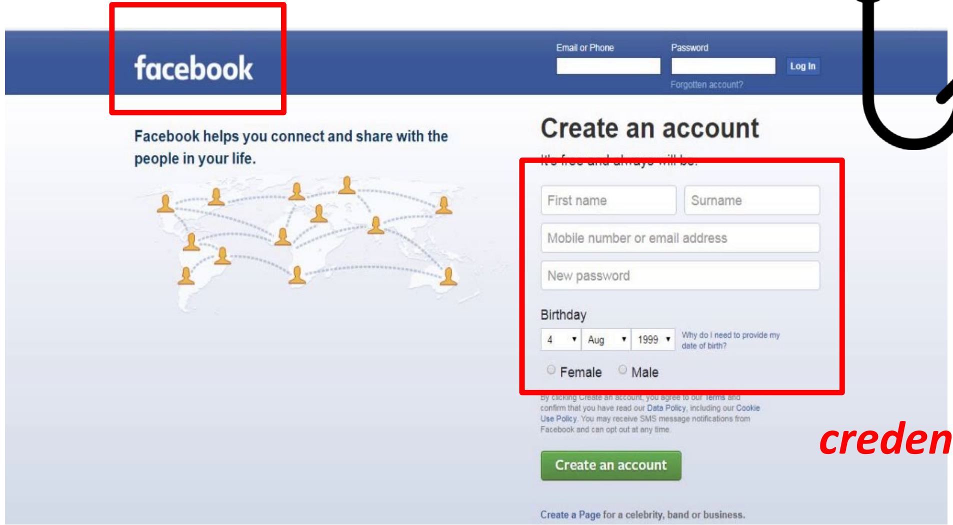
~~abc.com~~ ~~efg.com~~ … xyz.com

Evolving HTML code



PhishIntention Solution

brand intention



Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

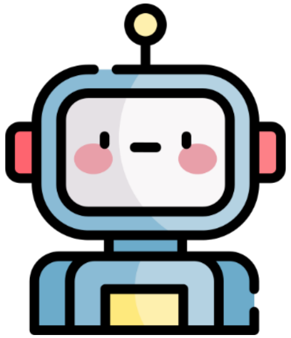
Create an account

Create a Page for a celebrity, band or business.

credential-taking intention

abc.com

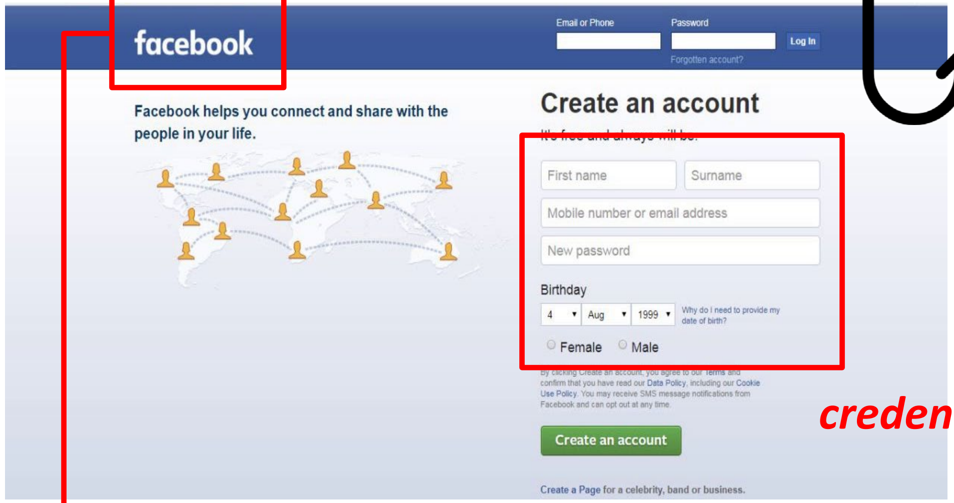
look



PI (PhishIntention)

PhishIntention Solution

brand intention



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

~~It's free and always will be.~~

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

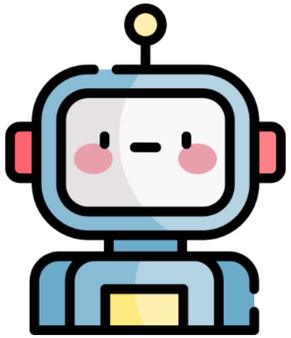
By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

credential-taking intention

look

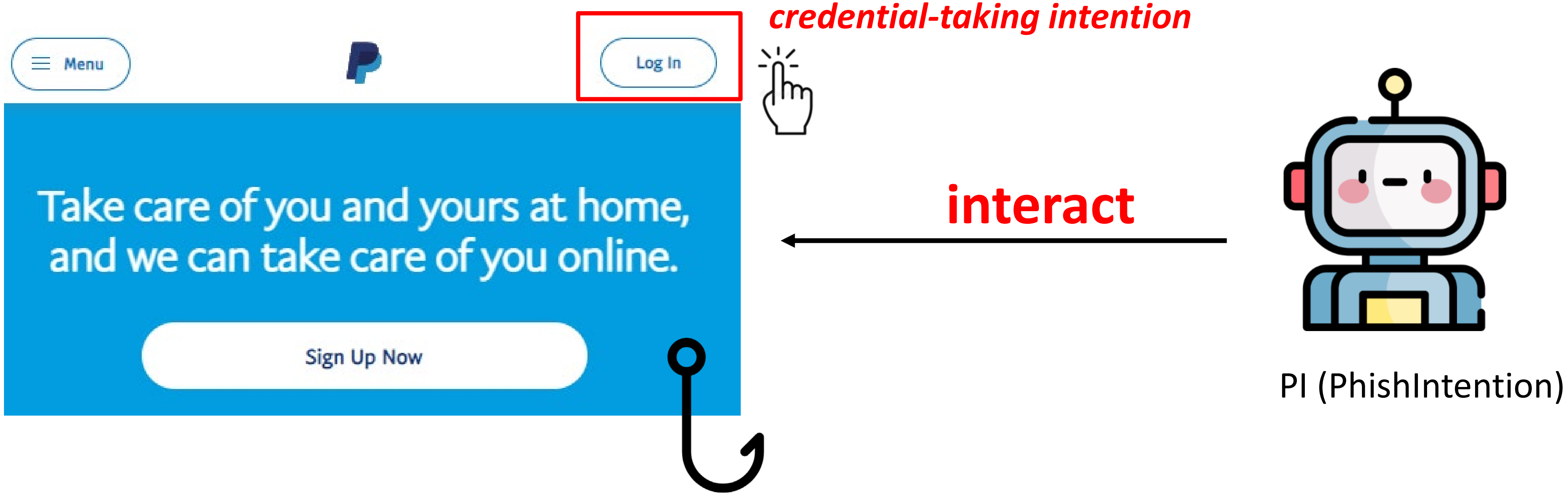


PI (PhishIntention)

abc.com

consistency checking

PhishIntention Solution



Take care of you and yours at home, and we can take care of you online.

credential-taking intention

interact

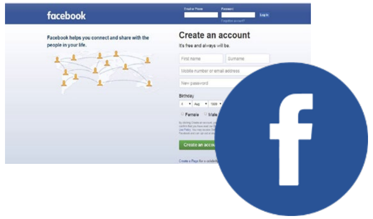
PI (PhishIntention)

Reference-based Phishing Detection

brand reference

Domain | **Representation**

facebook.com



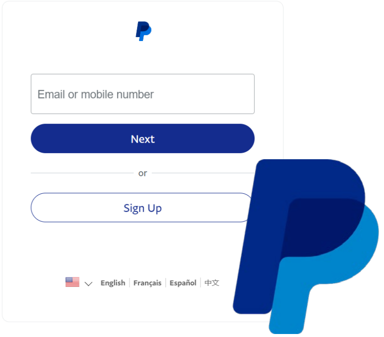
facebook

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

paypal.com



Email or mobile number

Next

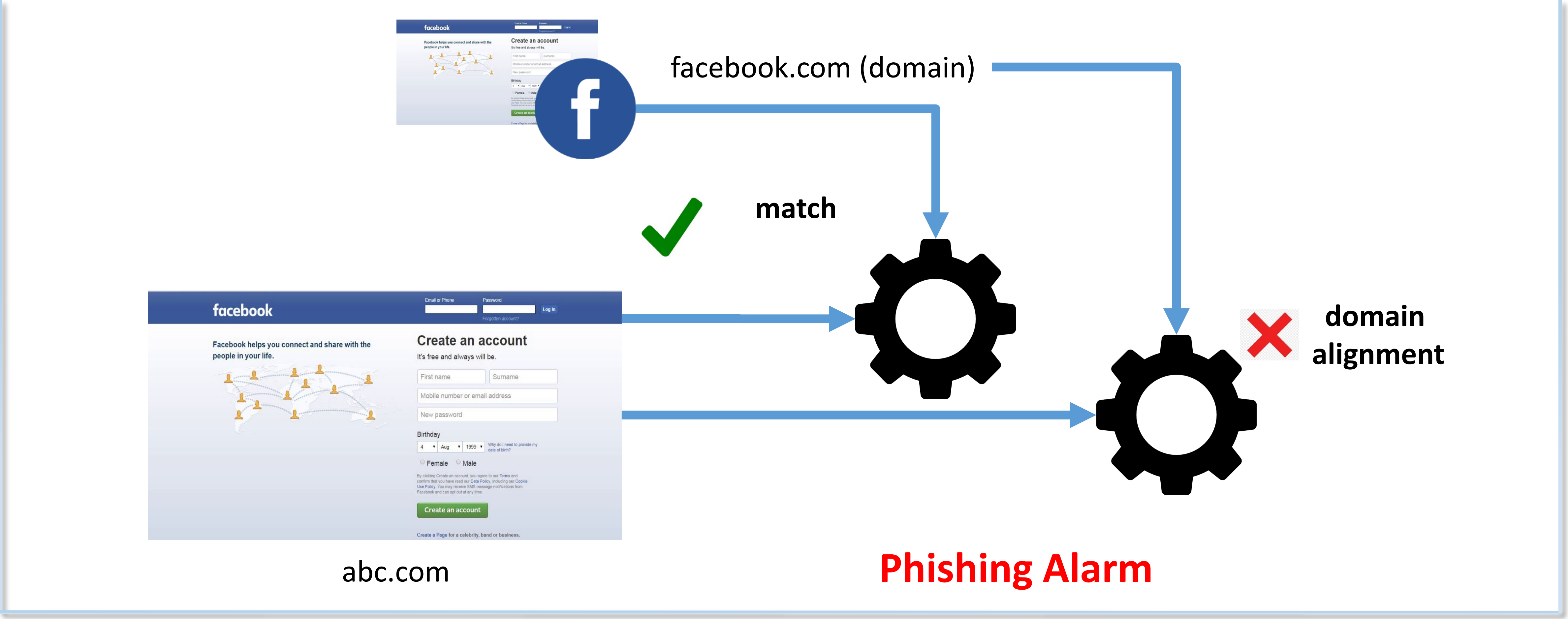
or

Sign Up

English | Français | Español | 中文

... | ...

Reference-based Phishing Detection



facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

facebook.com (domain)

✓ match

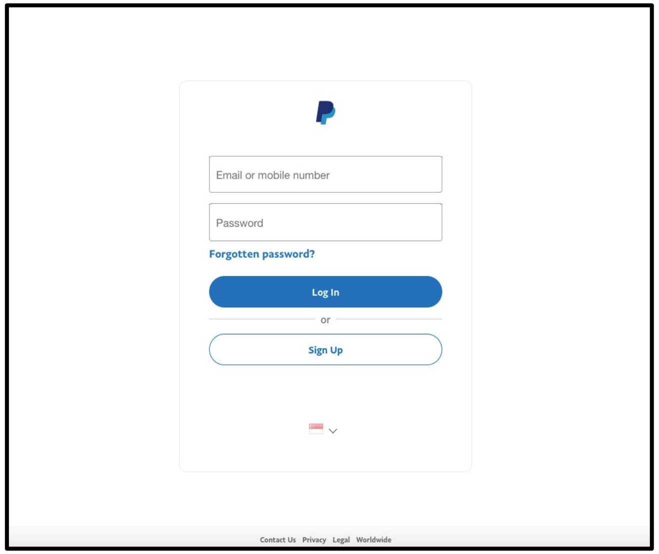
abc.com

✗ domain alignment

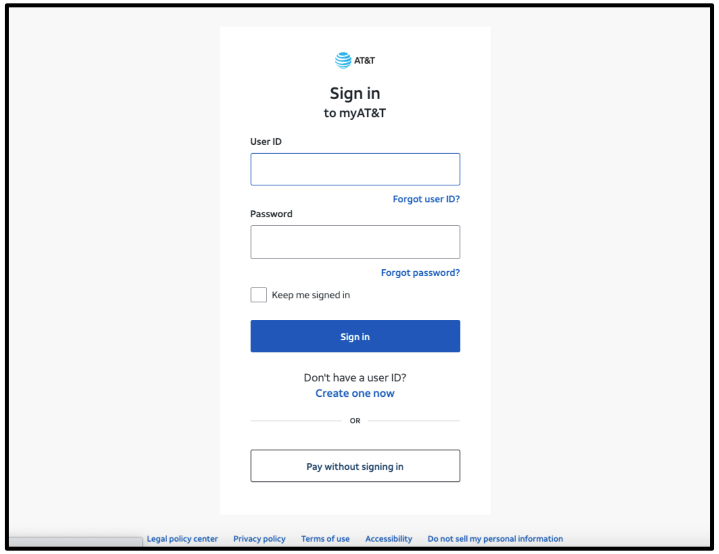
Phishing Alarm

Representation as Screenshot (VisualPhishNet, CCS 2020)

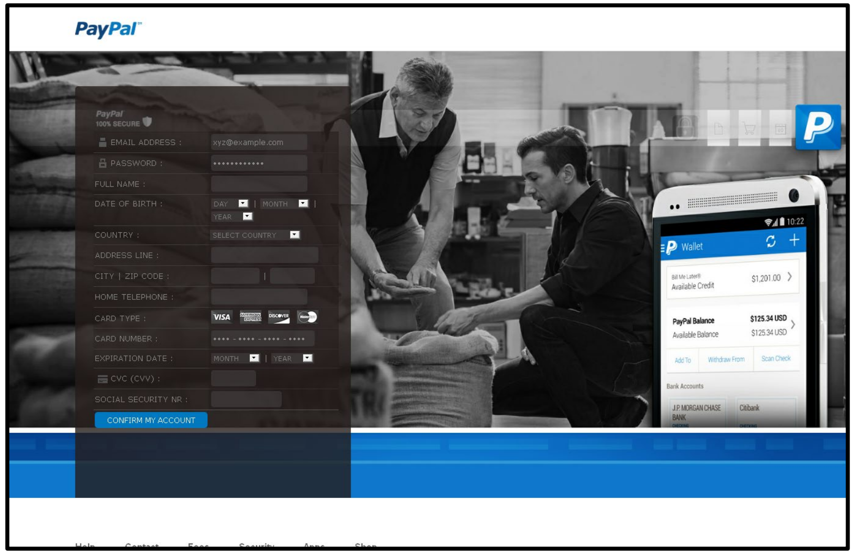
PayPal Screenshot



AT&T Screenshot



PayPal Screenshot


EMAIL ADDRESS : xyz@example.com

PASSWORD : ••••••••••••

Reference

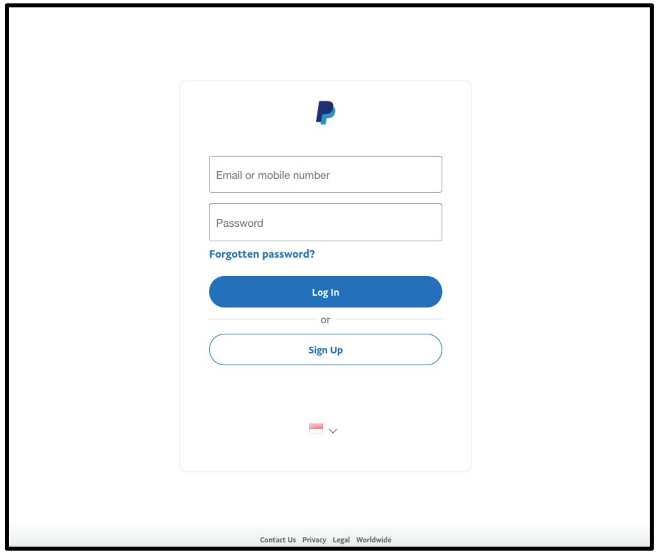
Benign Webpage

Phishing Webpage

false positive (similar screenshot)

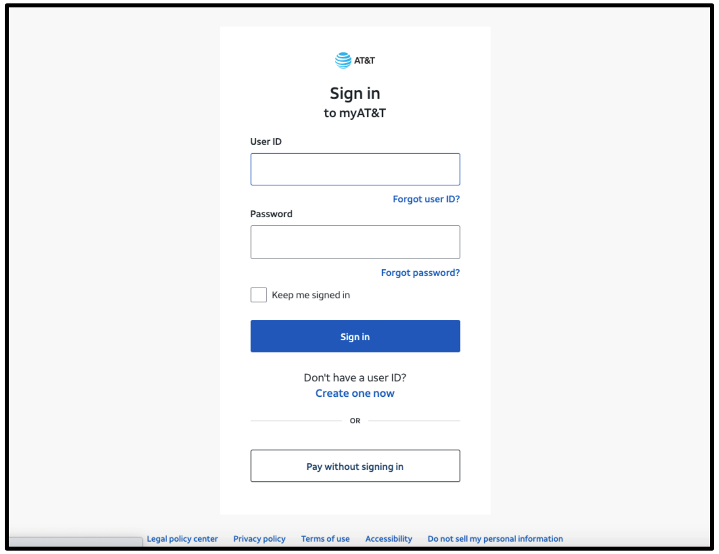
Representation as Screenshot (VisualPhishNet, CCS 2020)

PayPal Screenshot



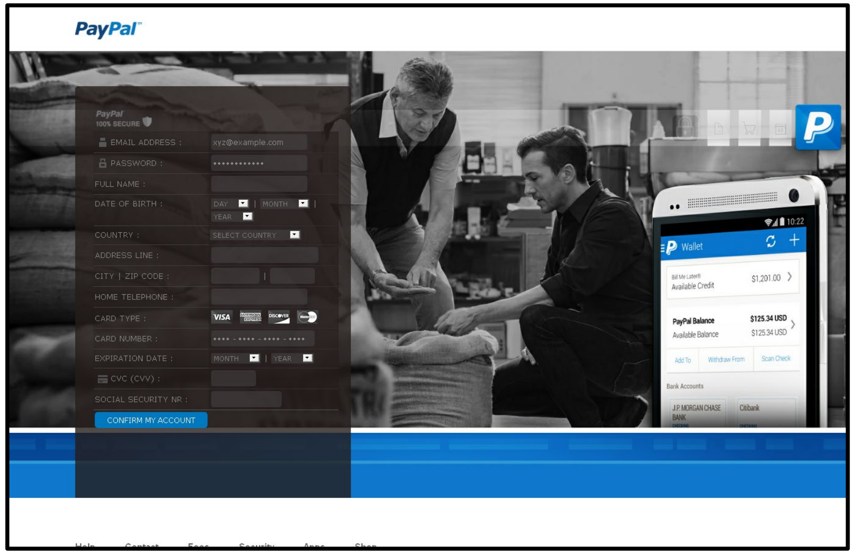
Reference

AT&T Screenshot



Benign Webpage

PayPal Screenshot

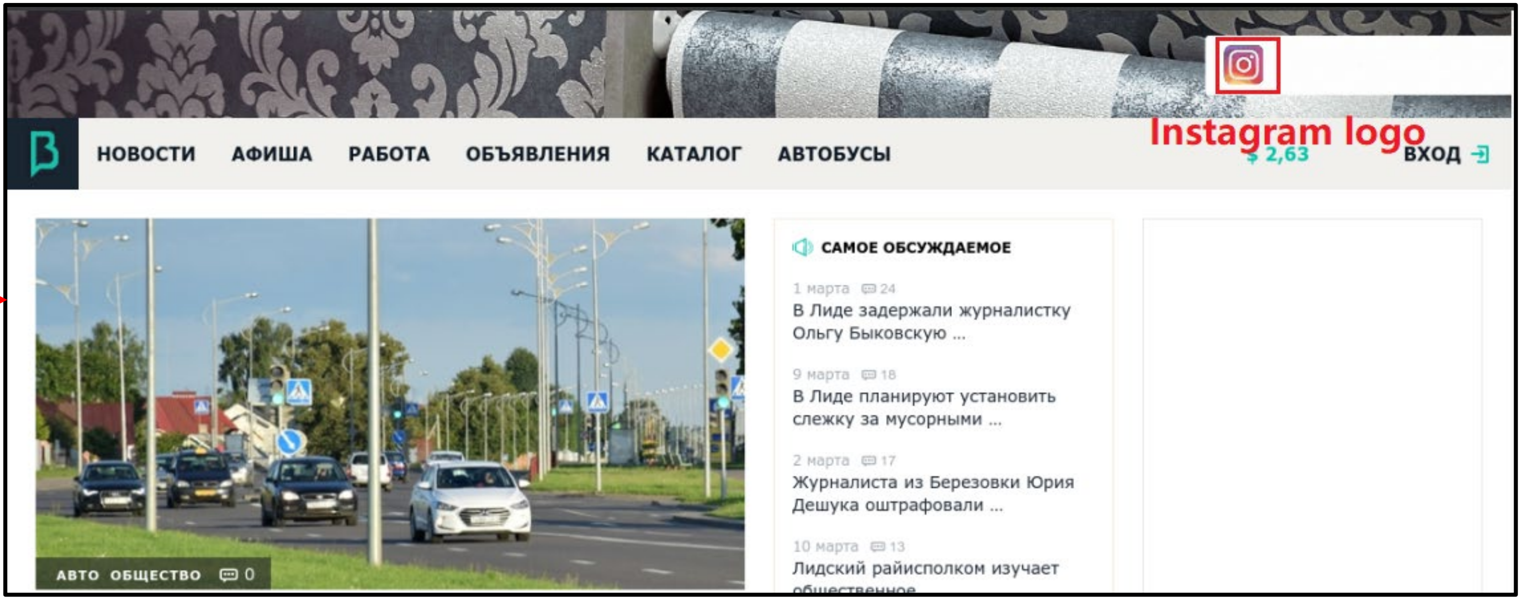


Phishing Webpage

false negative (dissimilar screenshot)

Representation as Logo (Phishpedia, USENIX Security 2021)

false positive



НОВОСТИ АФИША РАБОТА ОБЪЯВЛЕНИЯ КАТАЛОГ АВТОБУСЫ

$ 2,63 ВХОД

АВТО ОБЩЕСТВО 0

САМОЕ ОБСУЖДАЕМОЕ

1 марта 24
В Лиде задержали журналистку Ольгу Быковскую ...

9 марта 18
В Лиде планируют установить слежку за мусорными ...

2 марта 17
Журналиста из Березовки Юрия Дешука оштрафовали ...

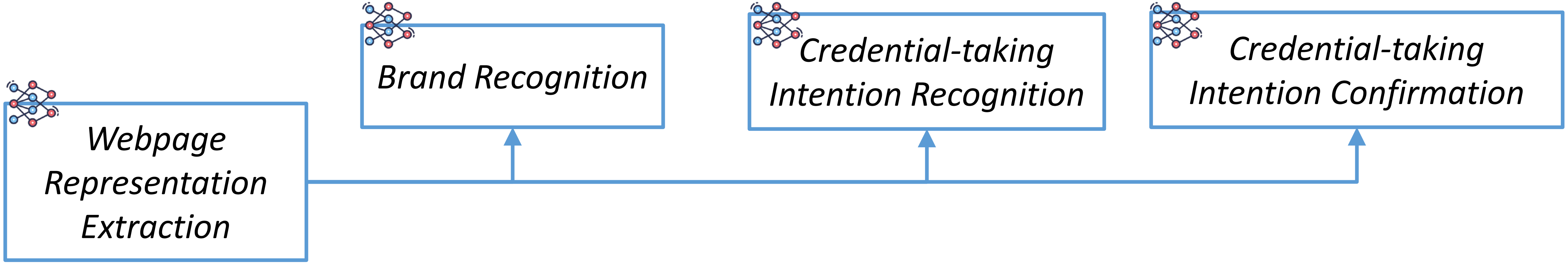
10 марта 13
Лидский райисполком изучает общественное

Benign Webpage

The screenshot and logo can only convey partial webpage intention.

PhishIntention Solution

- ***Comprehensive Intention***
- ***Static and Dynamic Webpage Analysis***

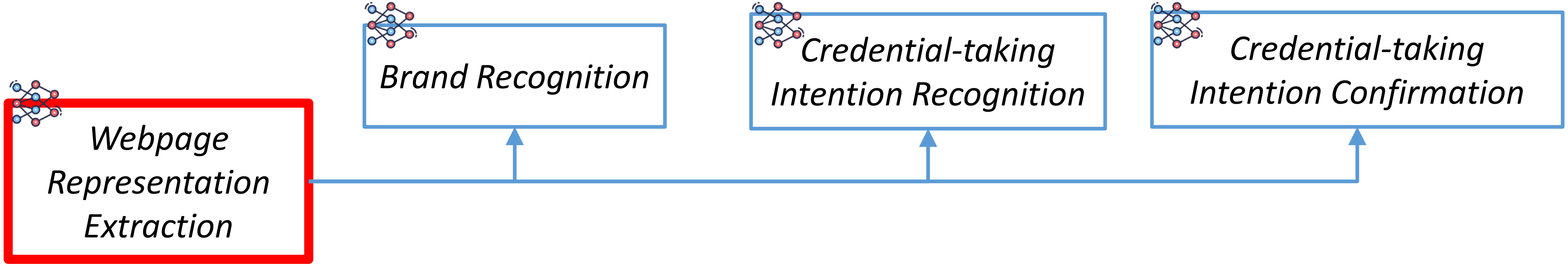


Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation

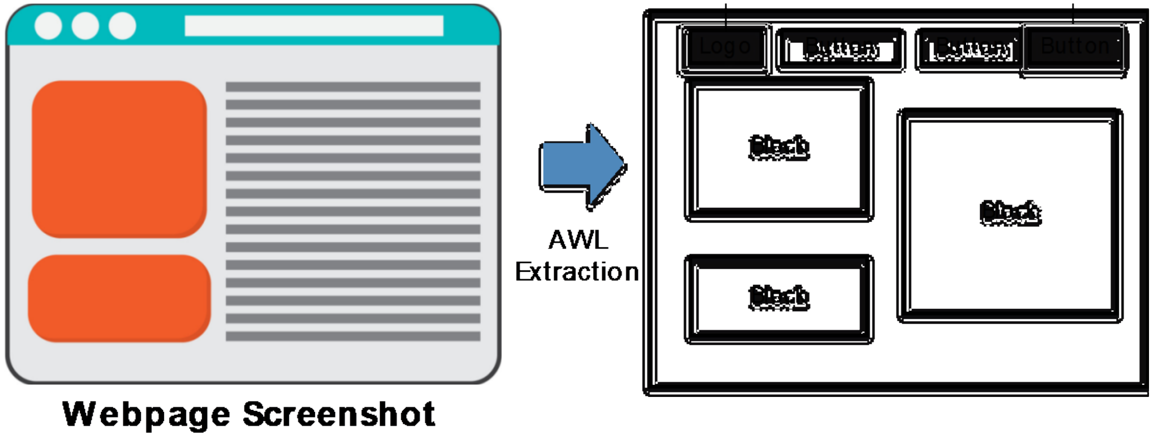


Webpage Representation Extraction

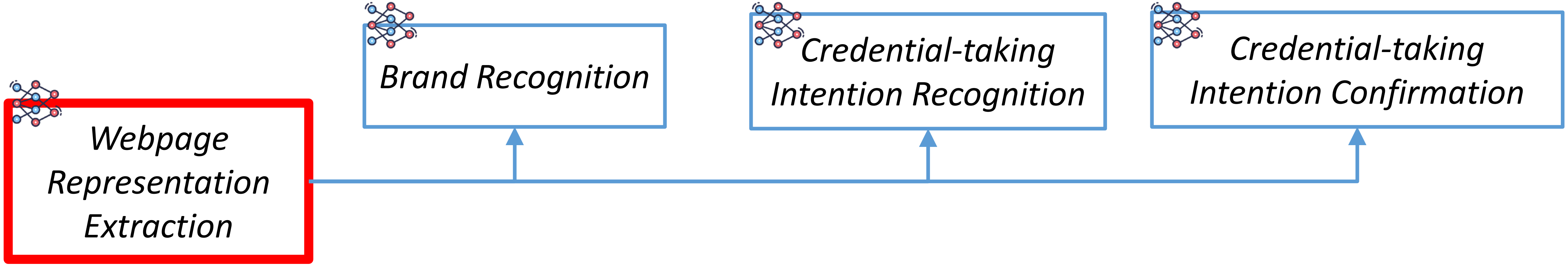
Brand Recognition

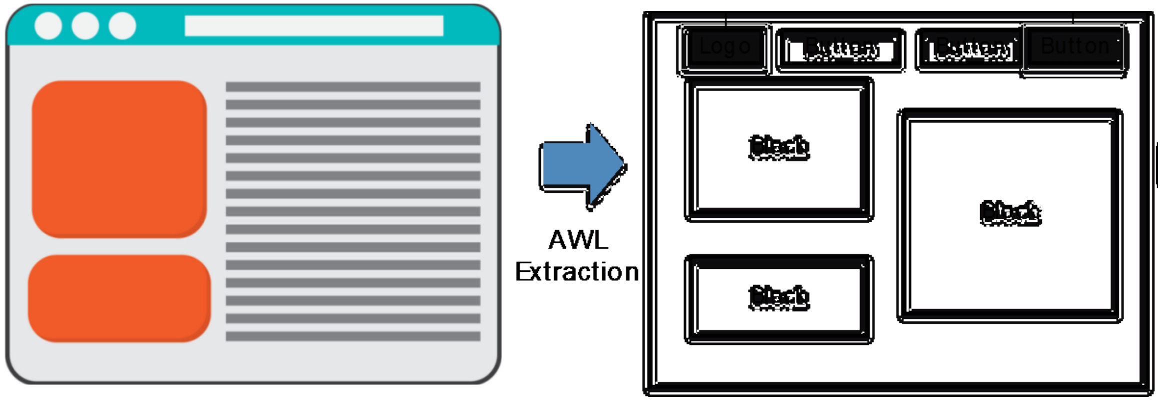
Credential-taking Intention Recognition

Credential-taking Intention Confirmation



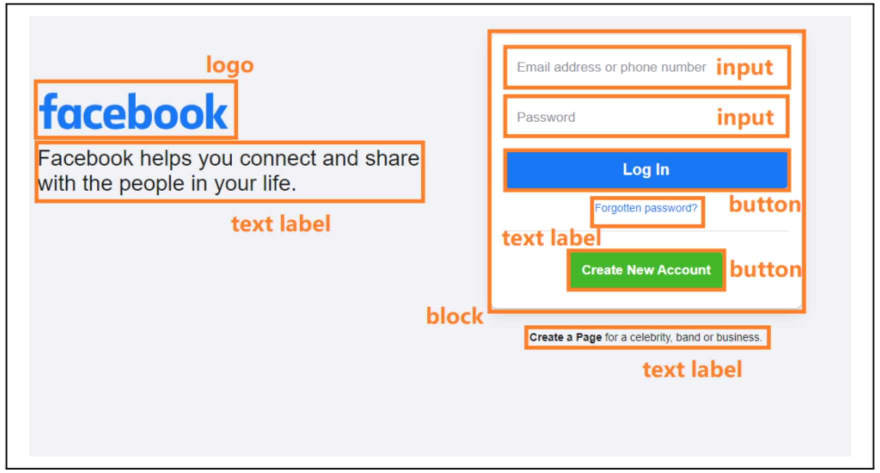
Step 1: Extract the Abstract Webpage Layout (AWL)


Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation



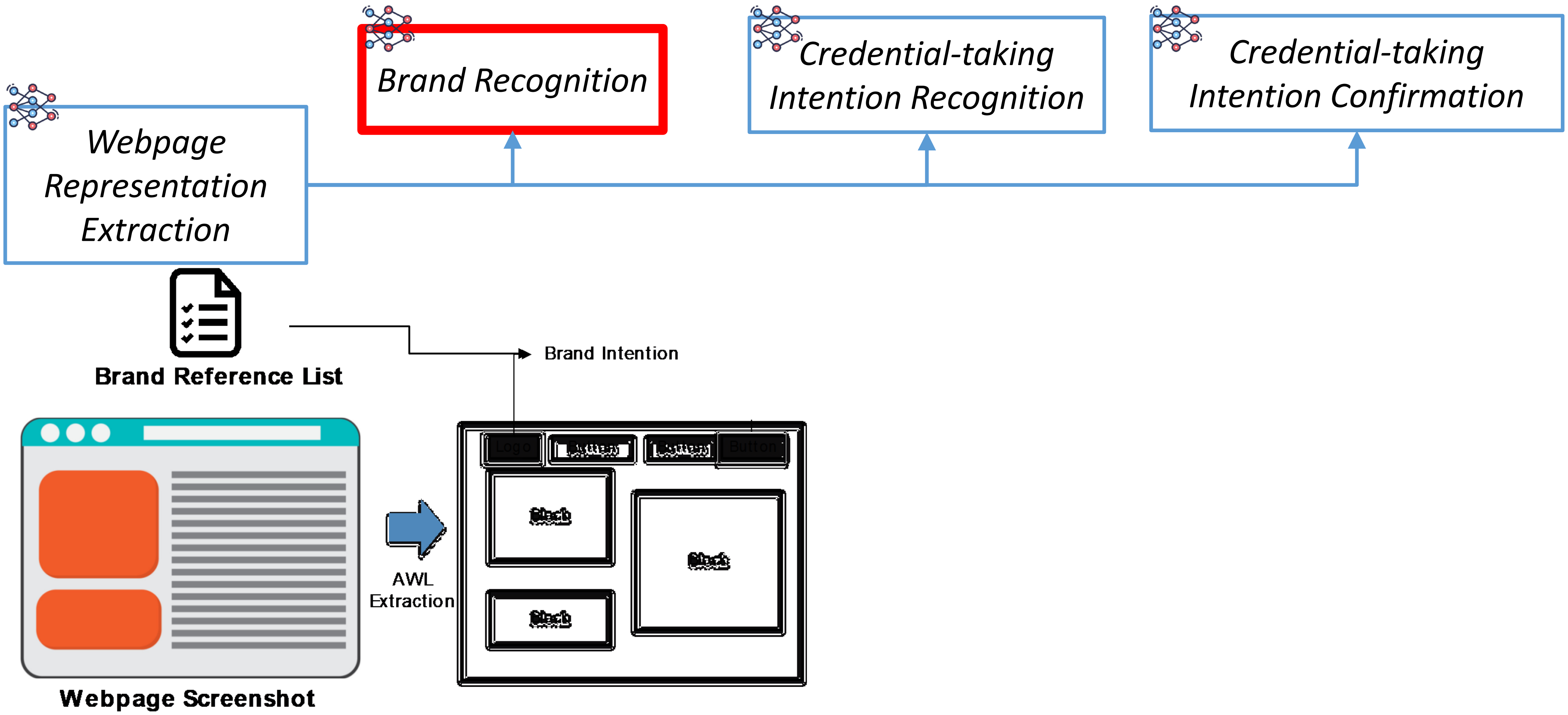
Webpage Screenshot

As an object detection task:


Facebook helps you connect and share with the people in your life.

Create a Page for a celebrity, band or business.

Step 1: Extract the Abstract Webpage Layout (AWL)



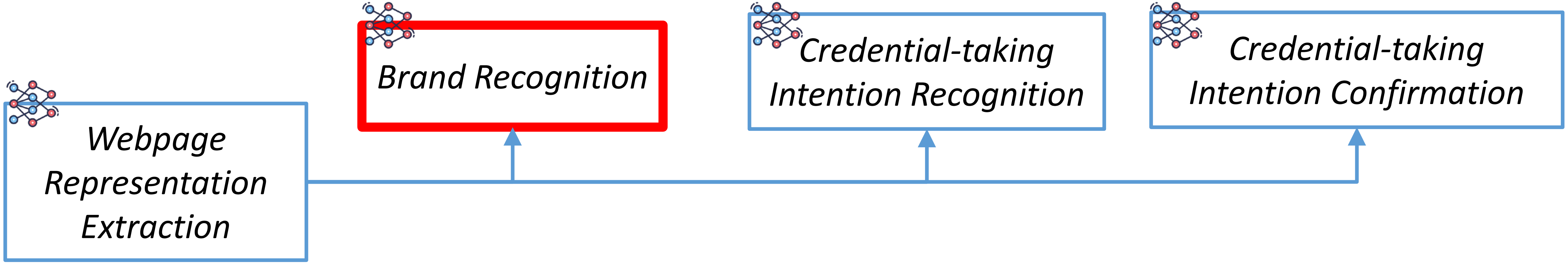
Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation

Step 2: Detecting Brand Intention

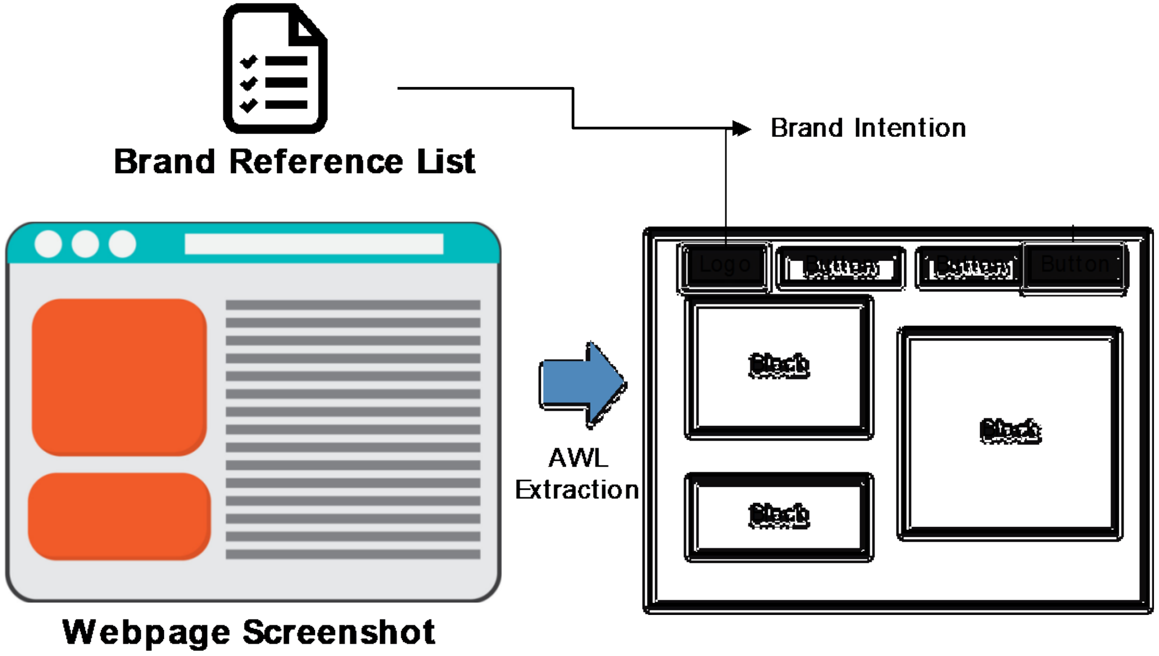


Webpage Representation Extraction

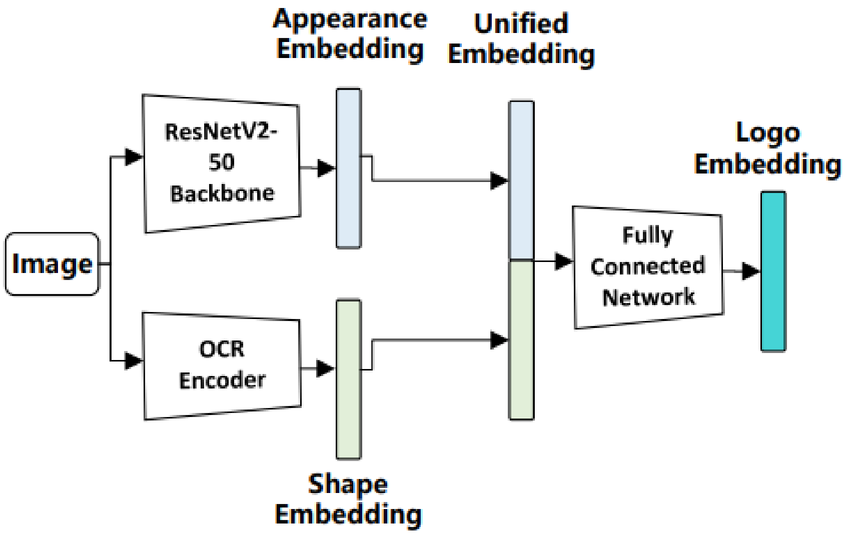
Brand Recognition

Credential-taking Intention Recognition

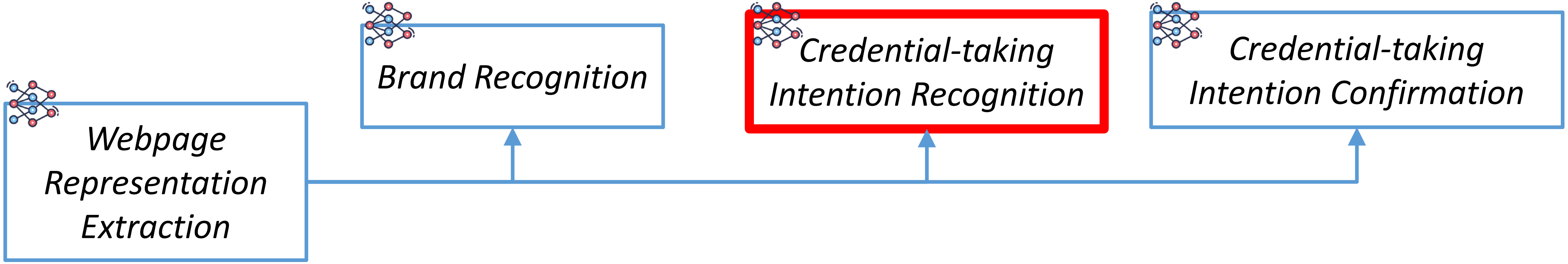
Credential-taking Intention Confirmation



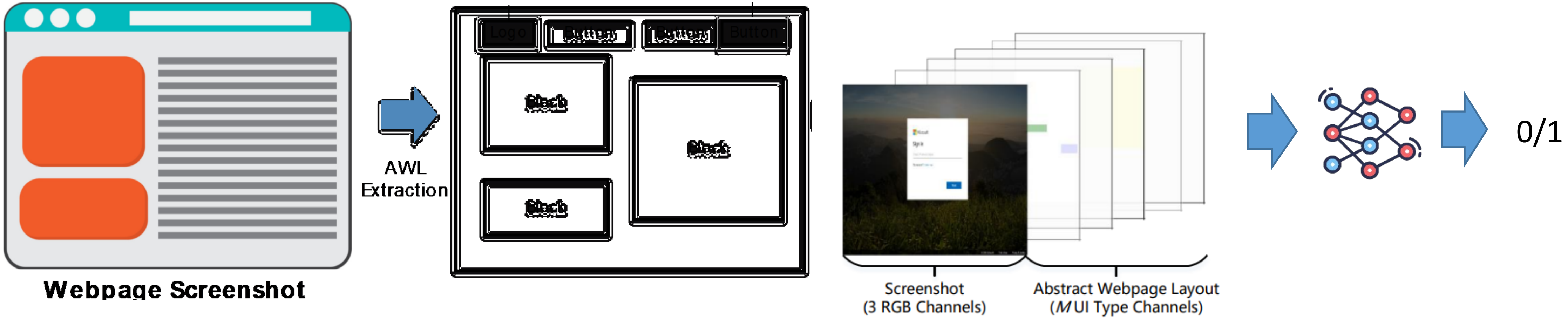
As a metric learning task:



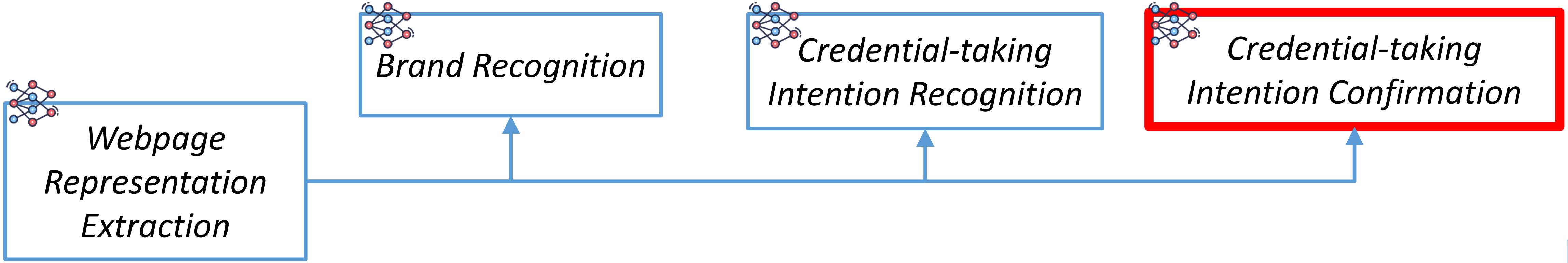
Step 2: Detecting Brand Intention

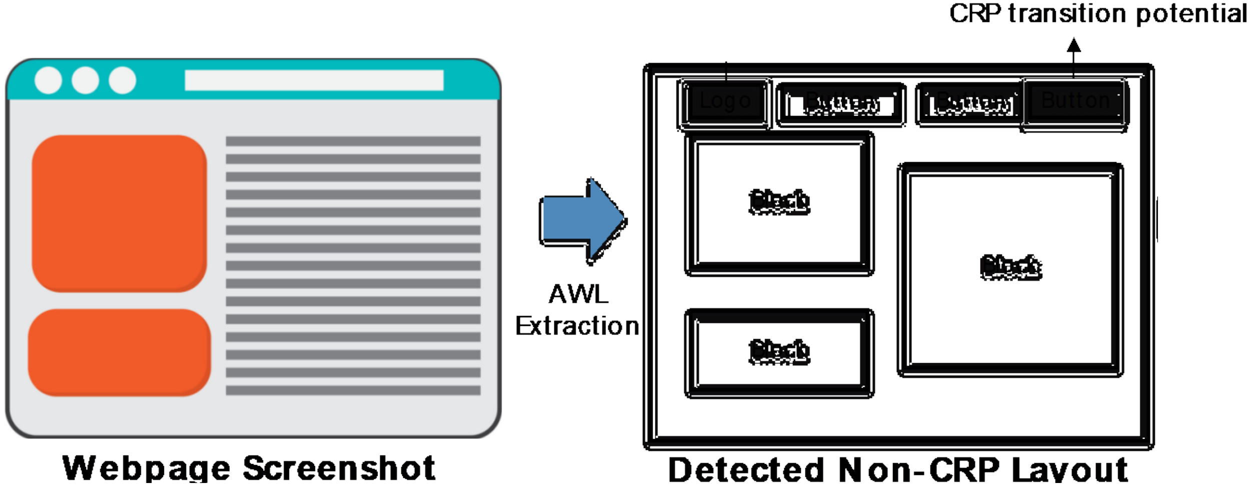

Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation

As a binary classification task:

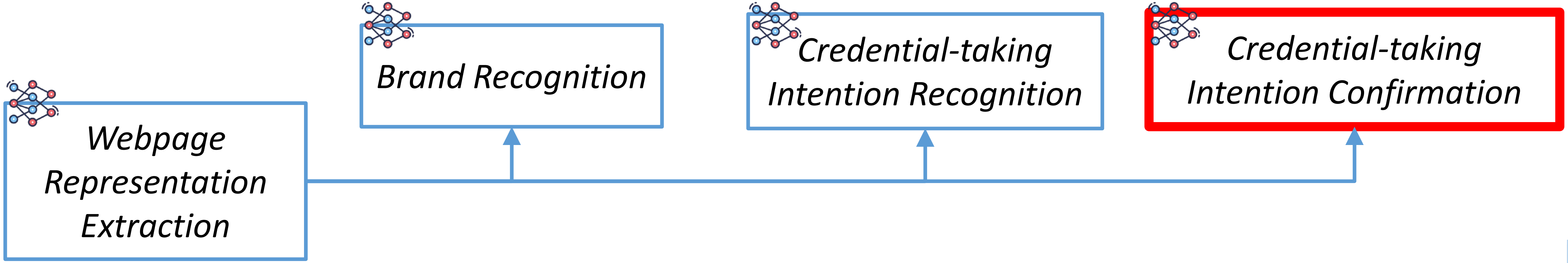


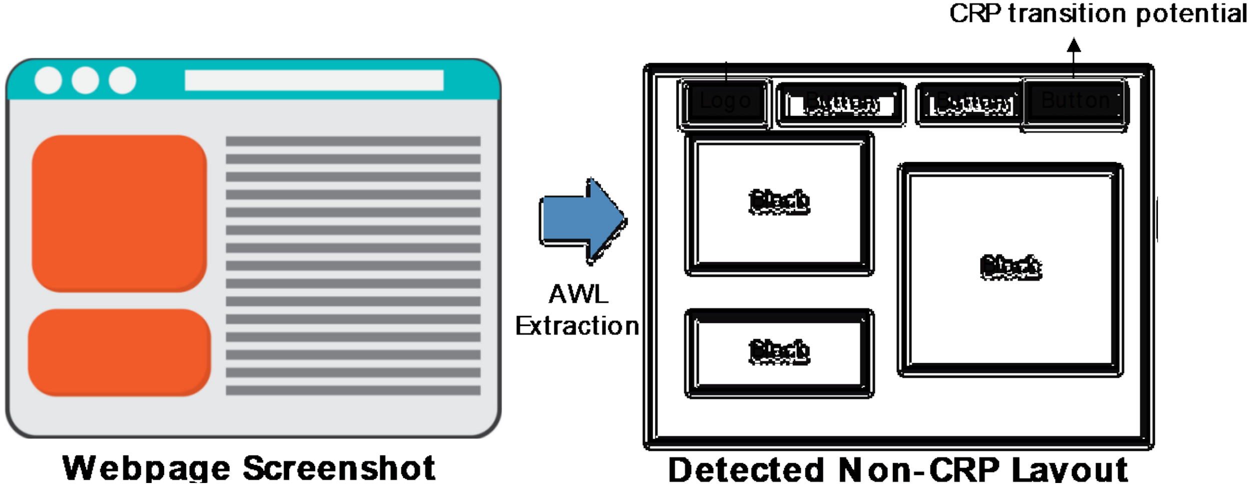
Step 3 : Credential-taking Intention Classification (whether this page takes credential?)


Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation

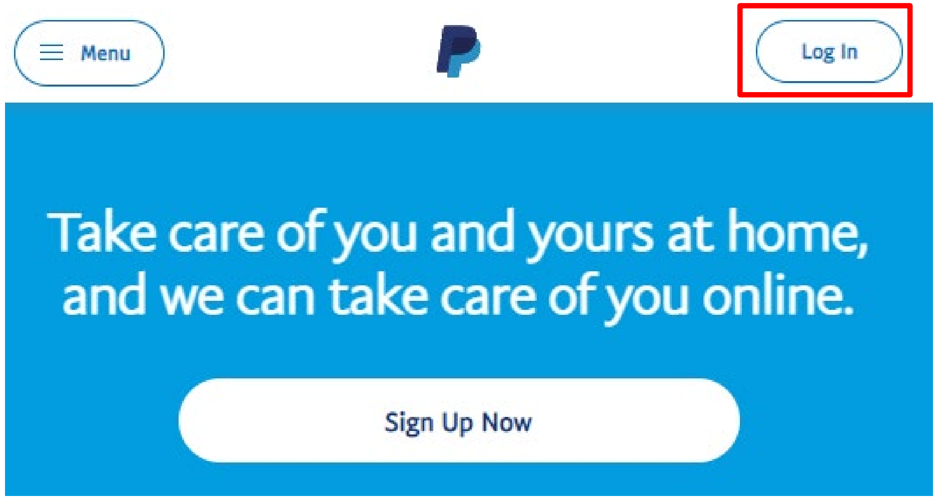


Step 4 : CRP (Credential-requiring Page) transition location (Whether any link/button on this webpage can link to a CRP?)


Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation

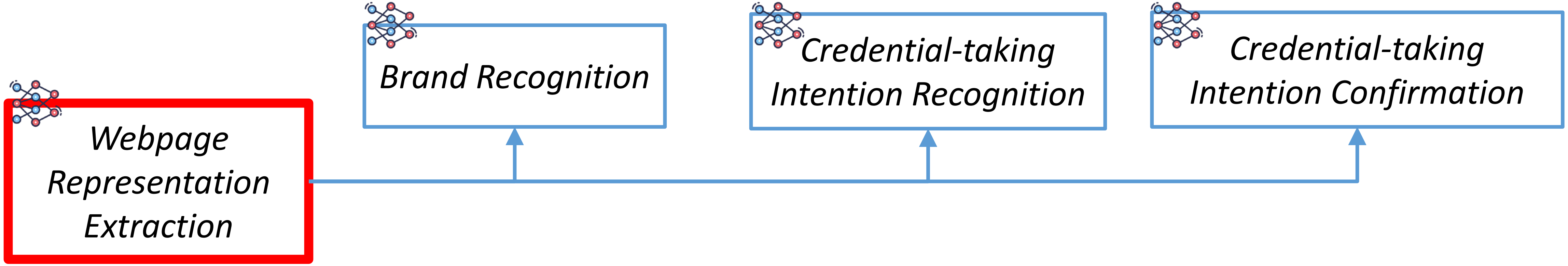


As an object detection task:



Take care of you and yours at home, and we can take care of you online.

Step 4 : CRP (Credential-requiring Page) transition location (Whether any link/button on this webpage can link to a CRP?)

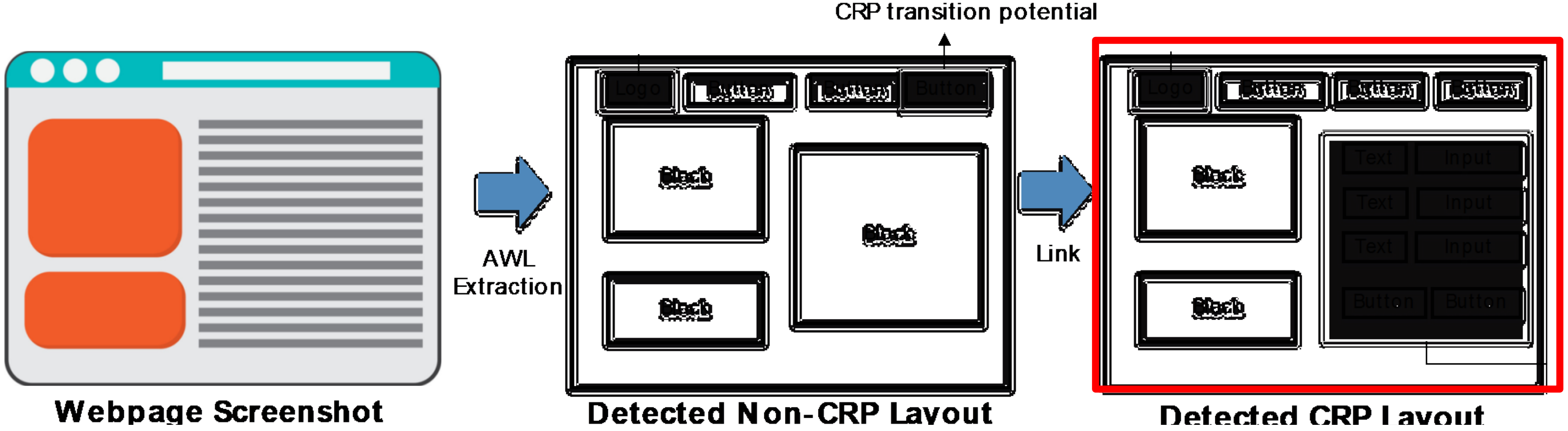


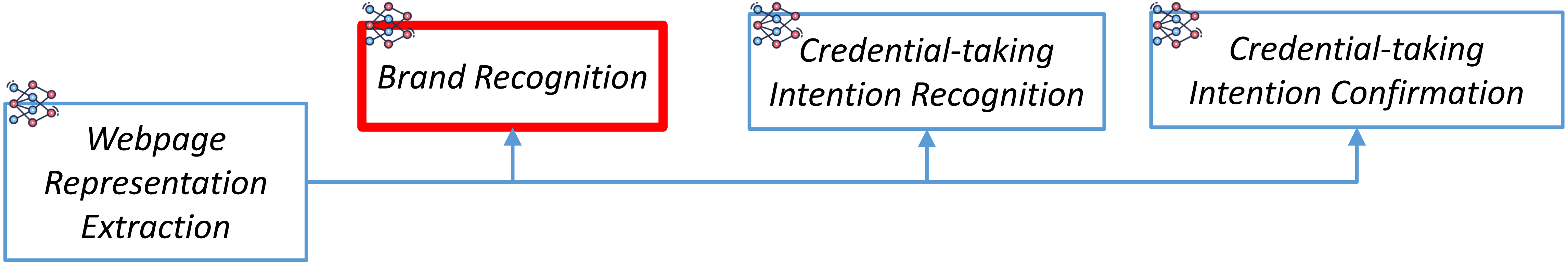
Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation



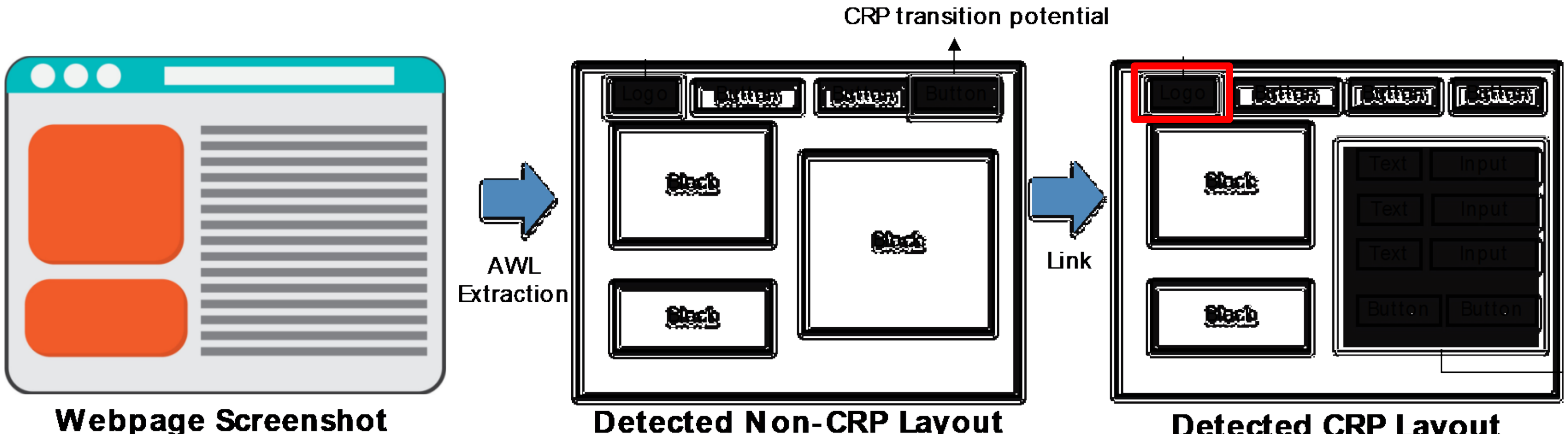


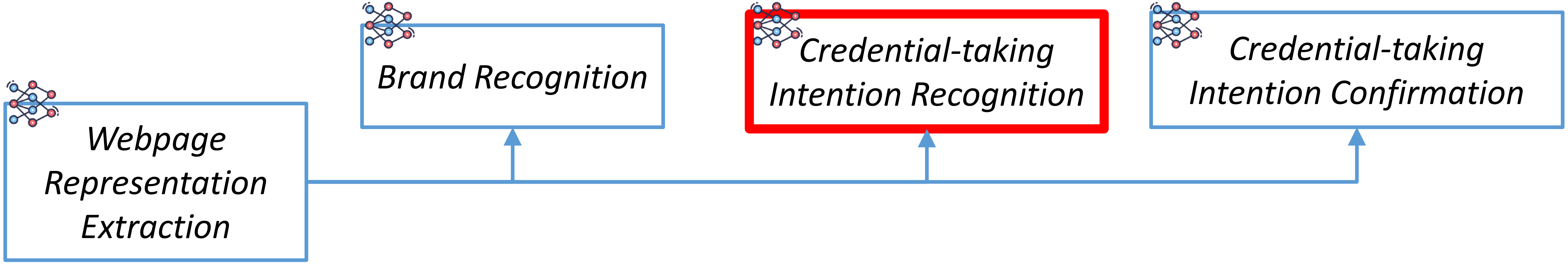
Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation



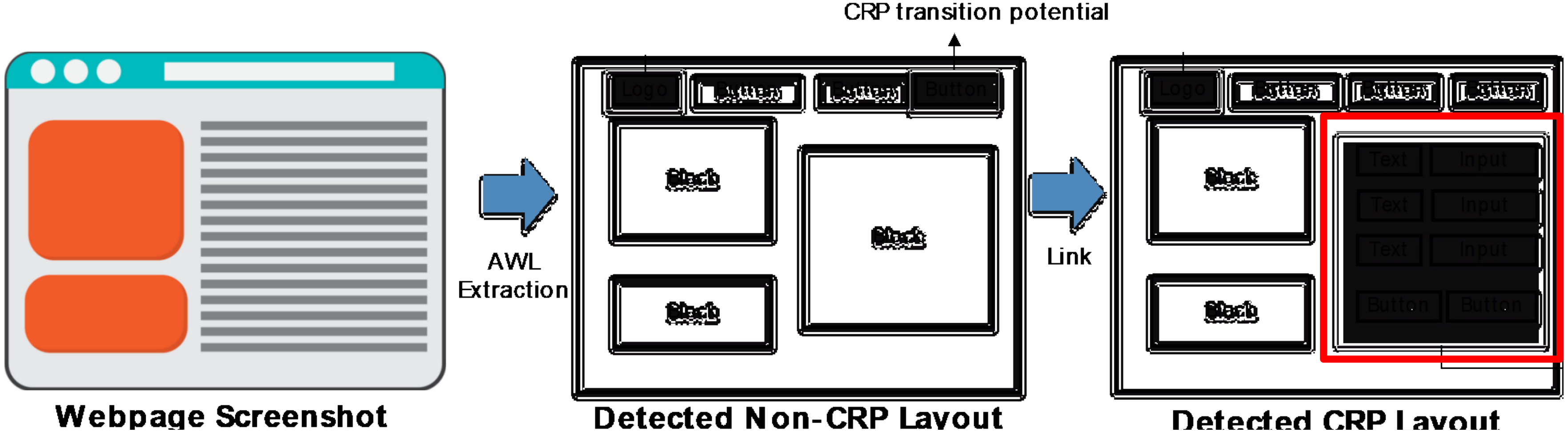


Webpage Representation Extraction

Brand Recognition

Credential-taking Intention Recognition

Credential-taking Intention Confirmation



Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

Experiments

Precision and recall in a collected phishing webpage dataset

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

Experiments

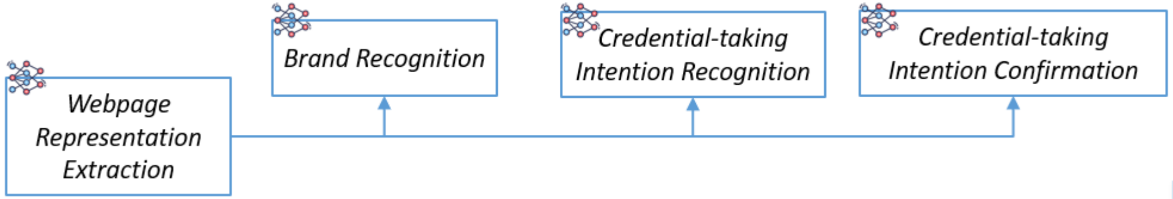
- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance to find a CRP from a non-CRP?

Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

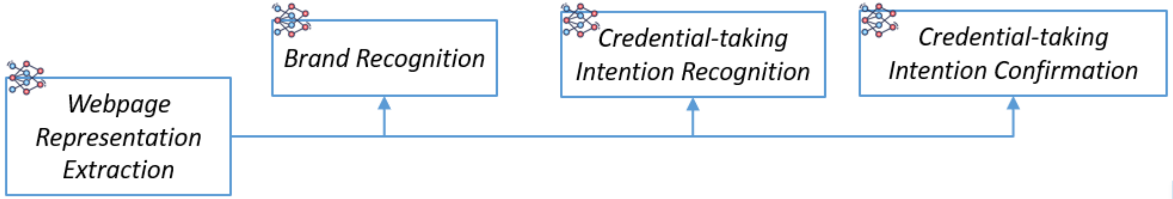
What is the performance of each component?


Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation

Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

How robust is the each of our deep learning model?


Webpage Representation Extraction
Brand Recognition
Credential-taking Intention Recognition
Credential-taking Intention Confirmation

Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance of PI to detect zero-day phishing webpages in the wild?

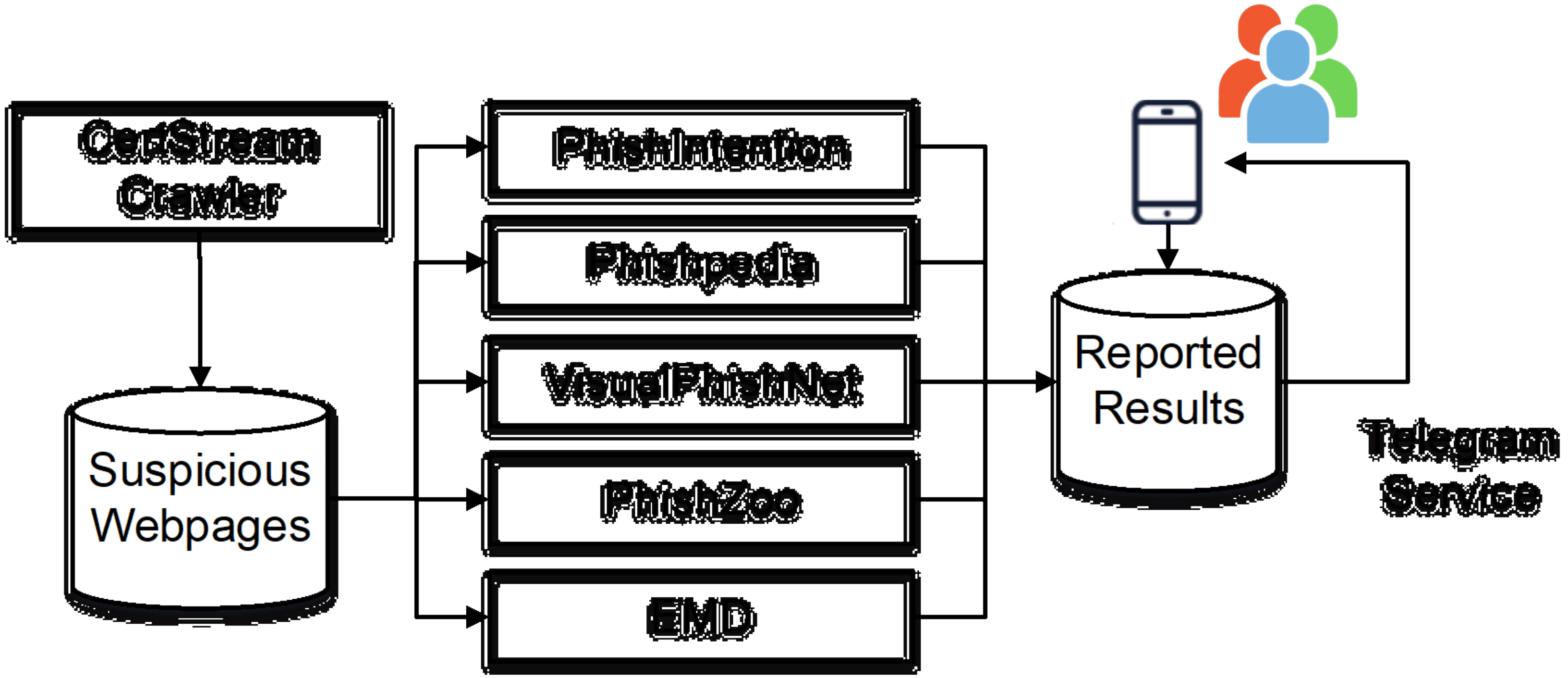
Experiments

- RQ1: Phishing Detection Experiment
- RQ2: CRP Location Experiment
- RQ3: Evaluating Model-wise Performance
- RQ4: Robustness Against Adversaries
- RQ5: Phishing Discovery Experiment

What is the performance of PI to detect zero-day phishing webpages in the wild?

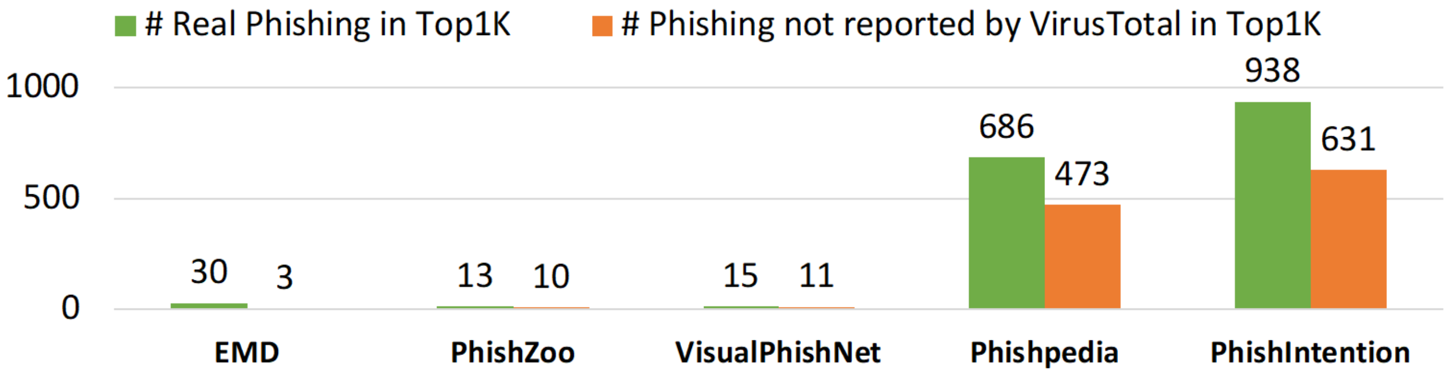
Phishing Discovery Experiment

- Detect phishing in the wild with a Crawling system



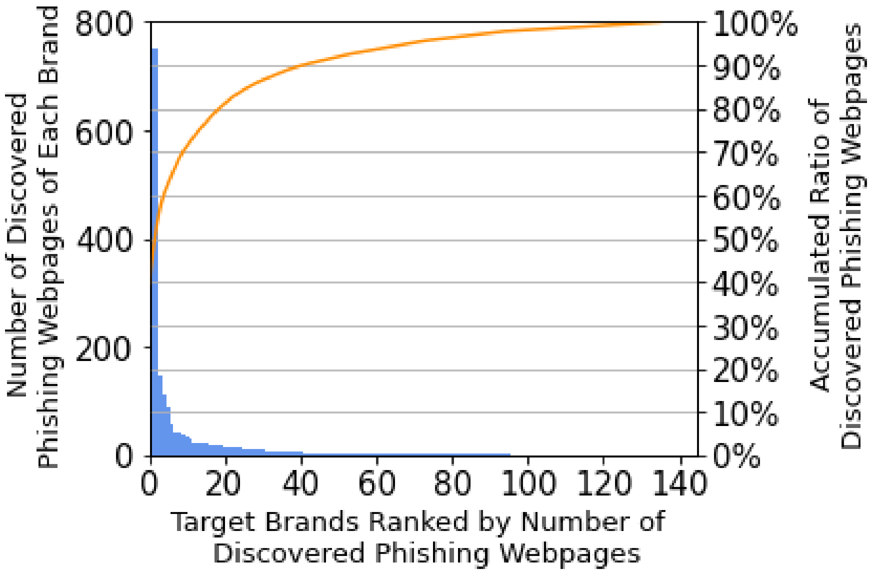
Phishing Discovery Experiment

- Two months starting from April 2021
- PhishIntention reports **1,942** real phishing webpages, **1,368** are zero-day phishing

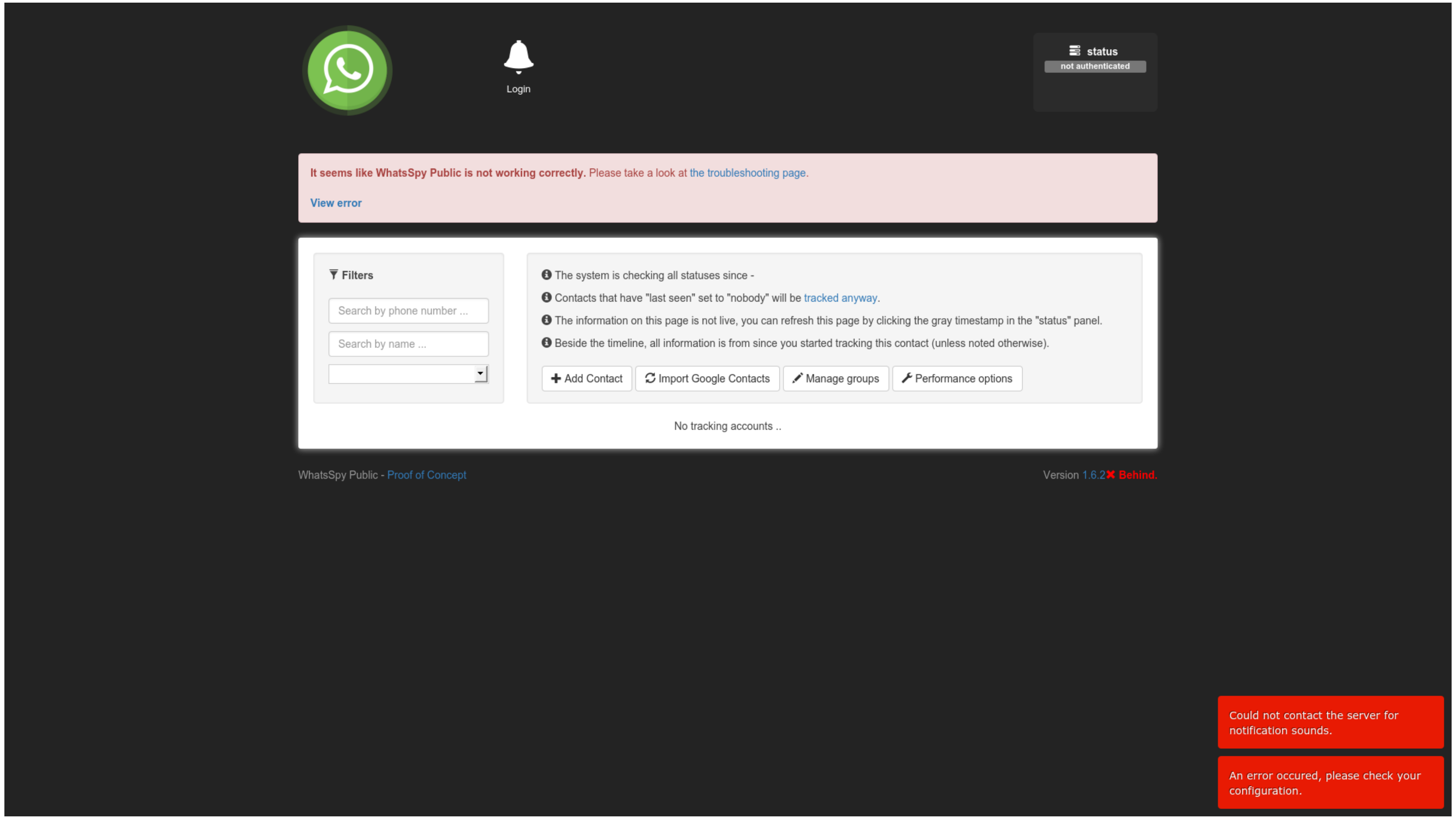


Phishing Discovery Experiment

- Distribution of brands of discovered phishing webpages
  - Top five brands are Microsoft (751), Facebook (146), HSBC Bank (110), Amazon (89), and Instagram (58).



Qualitative Analysis (False Positive)



It seems like WhatsSpy Public is not working correctly. Please take a look at the troubleshooting page.

View error

The system is checking all statuses since -

Contacts that have "last seen" set to "nobody" will be tracked anyway.

The information on this page is not live, you can refresh this page by clicking the gray timestamp in the "status" panel.

Beside the timeline, all information is from since you started tracking this contact (unless noted otherwise).

No tracking accounts ..

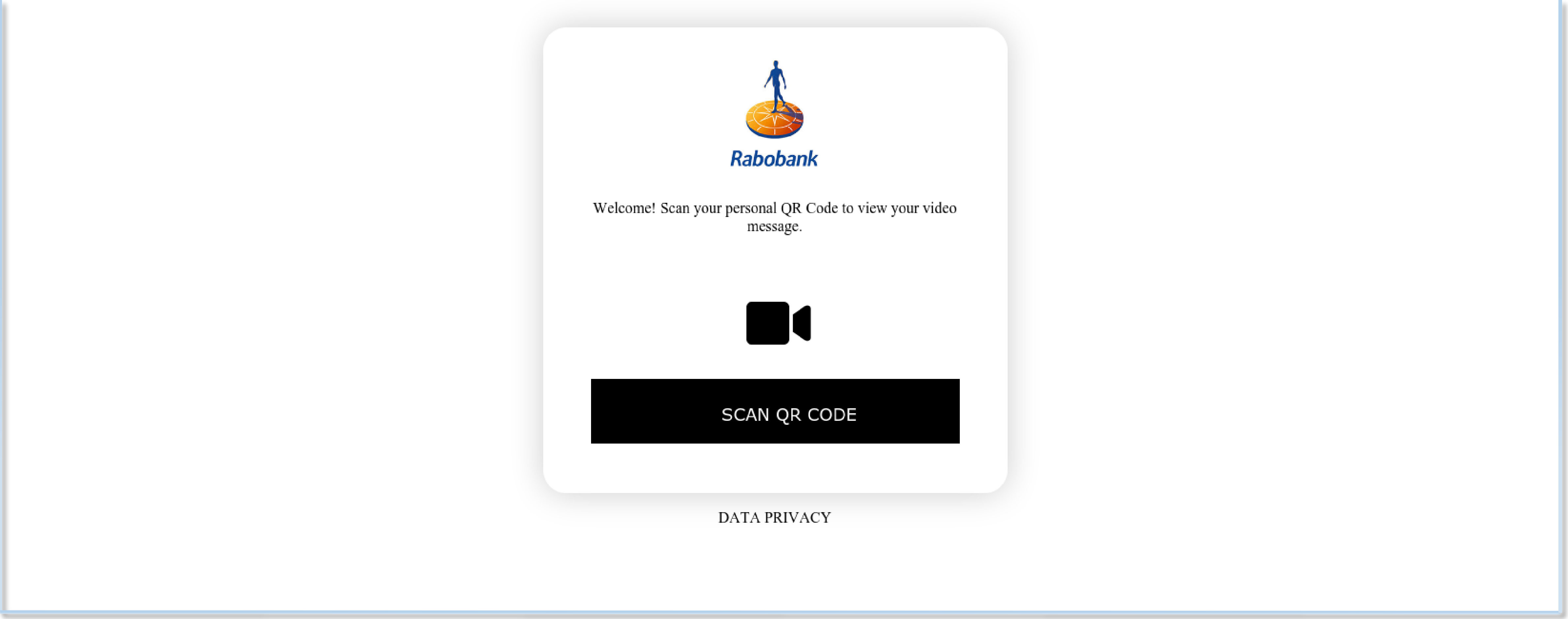
WhatsSpy Public - Proof of Concept

Version 1.6.2✖ Behind.

Could not contact the server for notification sounds.

An error occured, please check your configuration.

Qualitative Analysis (False Negative)

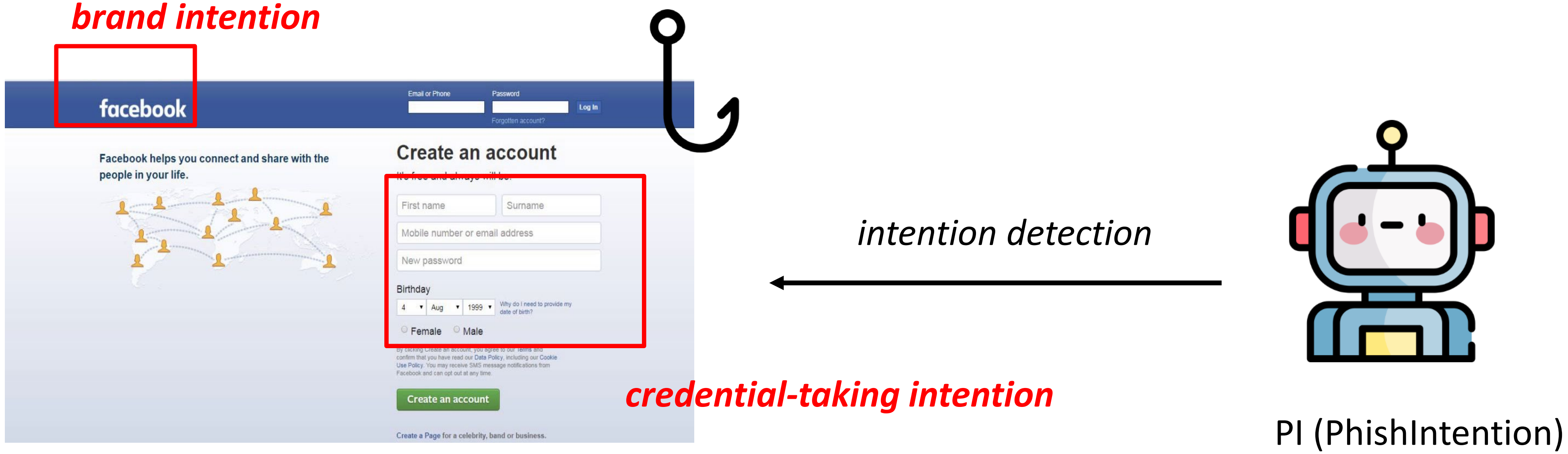


Welcome! Scan your personal QR Code to view your video message.

https://github.com/lindsey98/PhishIntention

Takeaways

- PhishIntention: a visual reference-based phishing detection solution
  - with both brand and credential-taking intentions.
  - with interaction for confirming more credential intentions.
  - with a tool to effectively detect zero-day phishing webpages.



brand intention

facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

4 ▾ Aug ▾ 1999 ▾

Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create an account

Create a Page for a celebrity, band or business.

credential-taking intention

intention detection

PI (PhishIntention)