Analysis of the KAIST Dooray Mailing System: Enhancing Security Against Phishing and Identity Attacks

- **Youri Merzouk** – INSA Centre Val de Loire – KAIST GSIS
- **Ilman Mohammad Al Momin** – EFREI Paris – KAIST GSIS

INSA CENTRE VAL DE LOIRE

KAIST Graduate School of Information Security

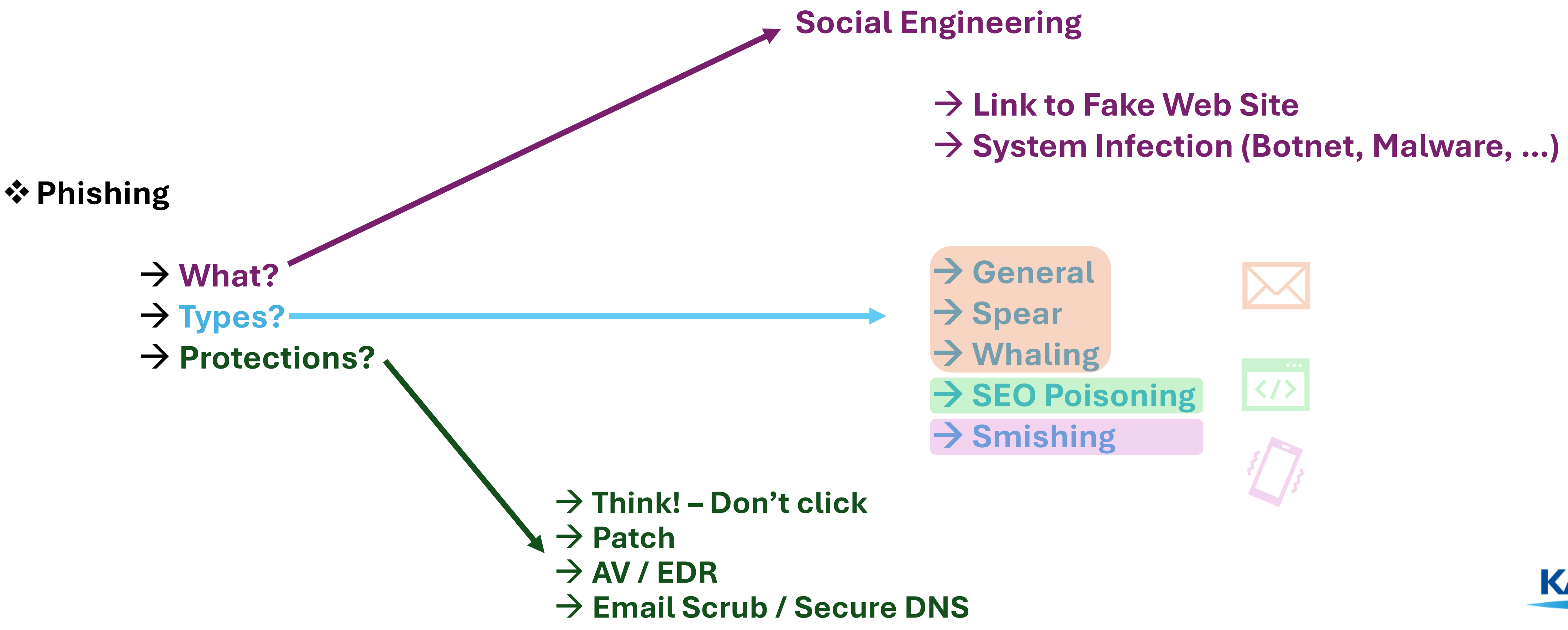
efrei PARIS PANTHÉON-ASSAS UNIVERSITÉ

Summary

- ***Introduction***
- ***Motivation***
- ***Background***
- ***Research Work Contrib.*** – *Zphisher – Dooray Security Mechanism*
- ***Research Work Contrib.*** – ML *Phishing Detection Tool*
- ***Technical Challenges***
- ***Evaluation*** - *Results & Impact*
- ***Limitation & Future Work***

Introduction

○ *What is Phishing?*



❖ **Phishing**

→ **What?**

→ **Types?**

→ **Protections?**

Social Engineering

→ **Link to Fake Web Site**

→ **System Infection (Botnet, Malware, …)**

→ **General**

→ **Spear**

→ **Whaling**

→ **SEO Poisoning**

→ **Smishing**

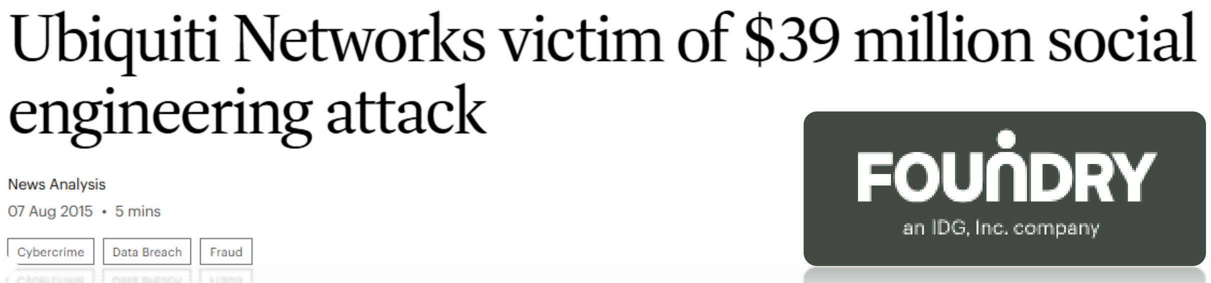
→ **Think! – Don’t click**

→ **Patch**

→ **AV / EDR**

→ **Email Scrub / Secure DNS**

Motivation

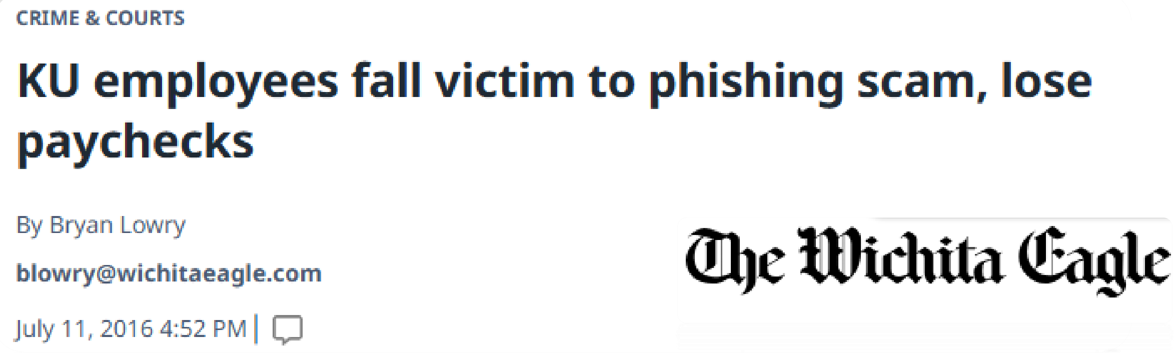


Ubiquiti Networks victim of $39 million social engineering attack

News Analysis

07 Aug 2015 • 5 mins

Cybercrime | Data Breach | Fraud



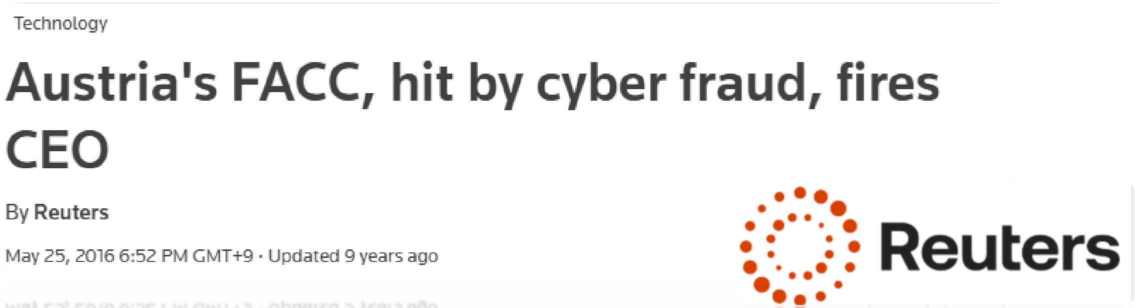
CRIME & COURTS

KU employees fall victim to phishing scam, lose paychecks

By Bryan Lowry

blowry@wichitaeagle.com

July 11, 2016 4:52 PM |



Technology

Austria's FACC, hit by cyber fraud, fires CEO

By Reuters

May 25, 2016 6:52 PM GMT+9 · Updated 9 years ago

Motivation

○ *Assess the Security Mechanisms of KAIST's Dooray Mailing System*

❖ Critical Role of Email Security

→ Over 90% of cyberattacks originate from Phishing emails
→ Securing mailing systems ensure trusted communication

❖ Challenges in Phishing Detection

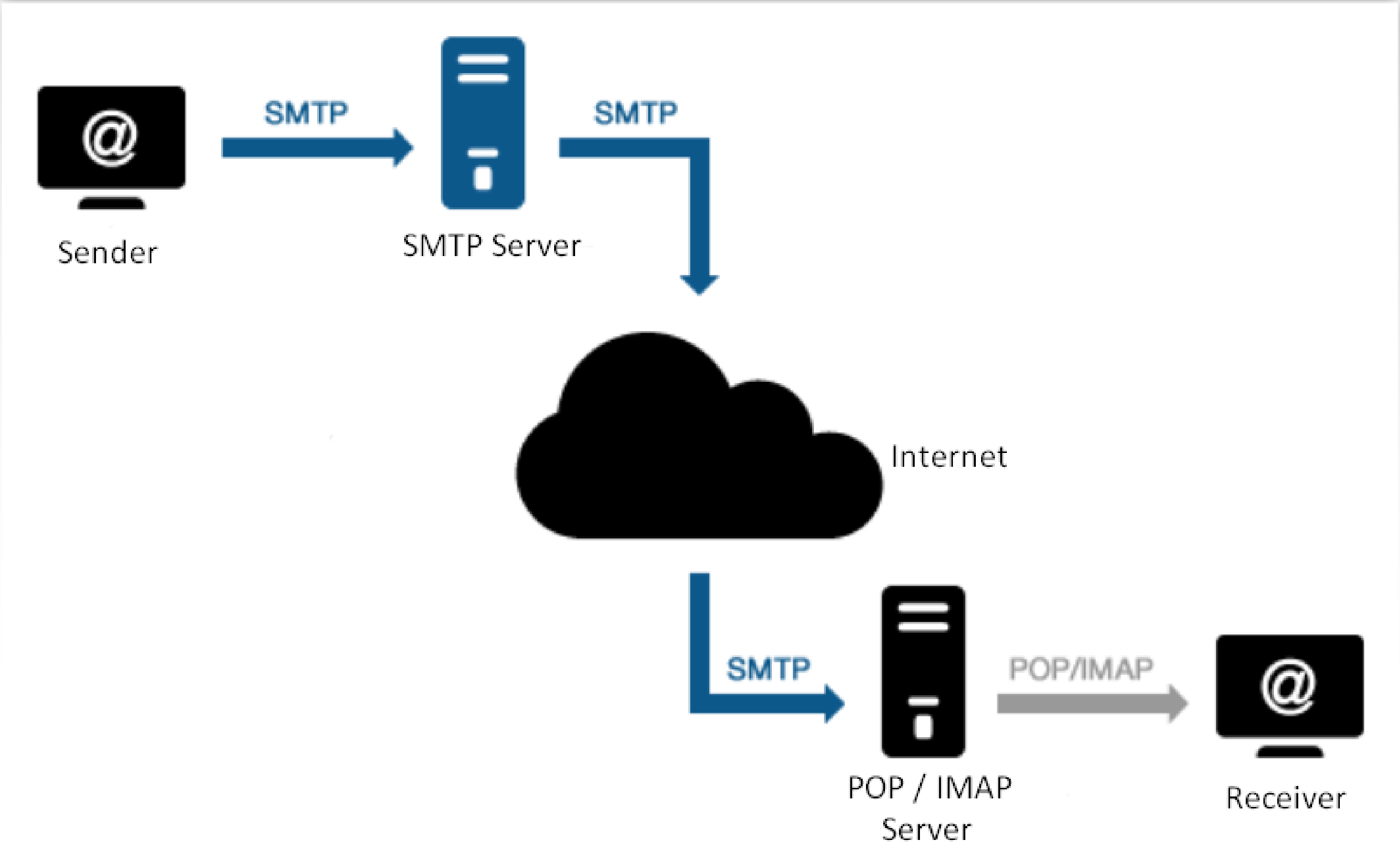
→ Sophisticated attacks bypass traditional defenses
→ Gaps in protocols like SMTP, DKIM, and DMARC can be exploited

❖ Opportunity for Improvement

→ Analyzing Dooray can reveal vulnerabilities and enhance defenses

Background

- *SMTP (Simple Mail Transfer Protocol)*



https://smtpserver.com/blog/smtp-server-what-is-this-and-its-definition/

Background

○ *SMTP (Simple Mail Transfer Protocol)*

❖ Purpose

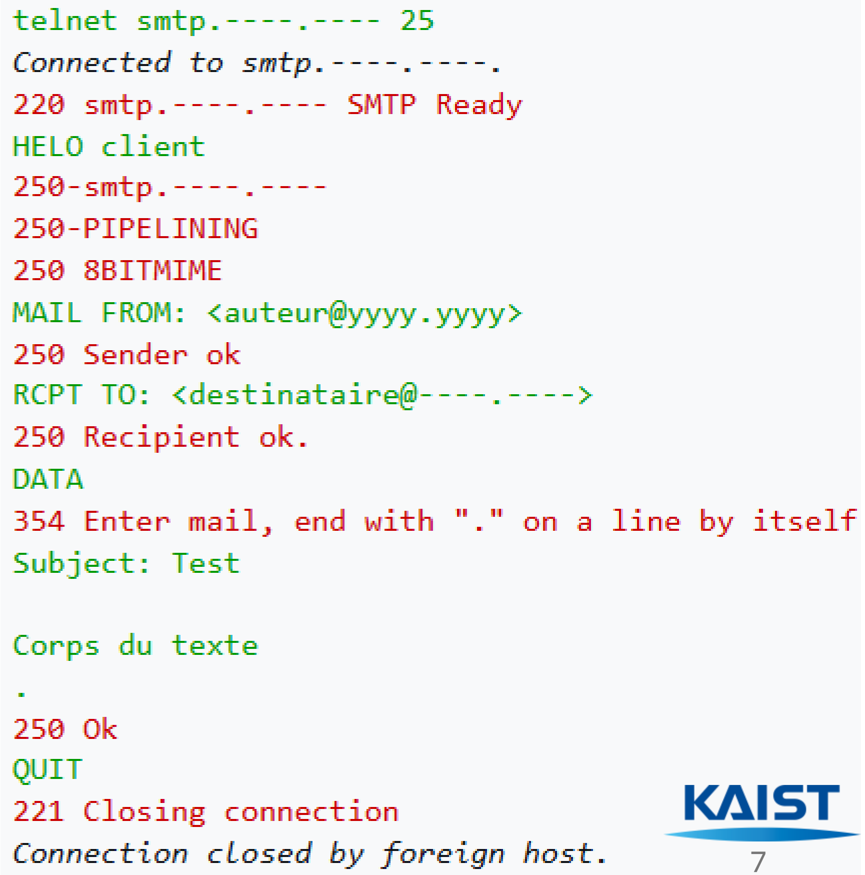
→ Standard protocol for sending emails between servers
→ Ensures email delivery across different domains

❖ Features

→ Relies on plaintext by default (can be encrypted with STARTTLS)
→ Specifies rules for email formatting and transfer

❖ Limitations

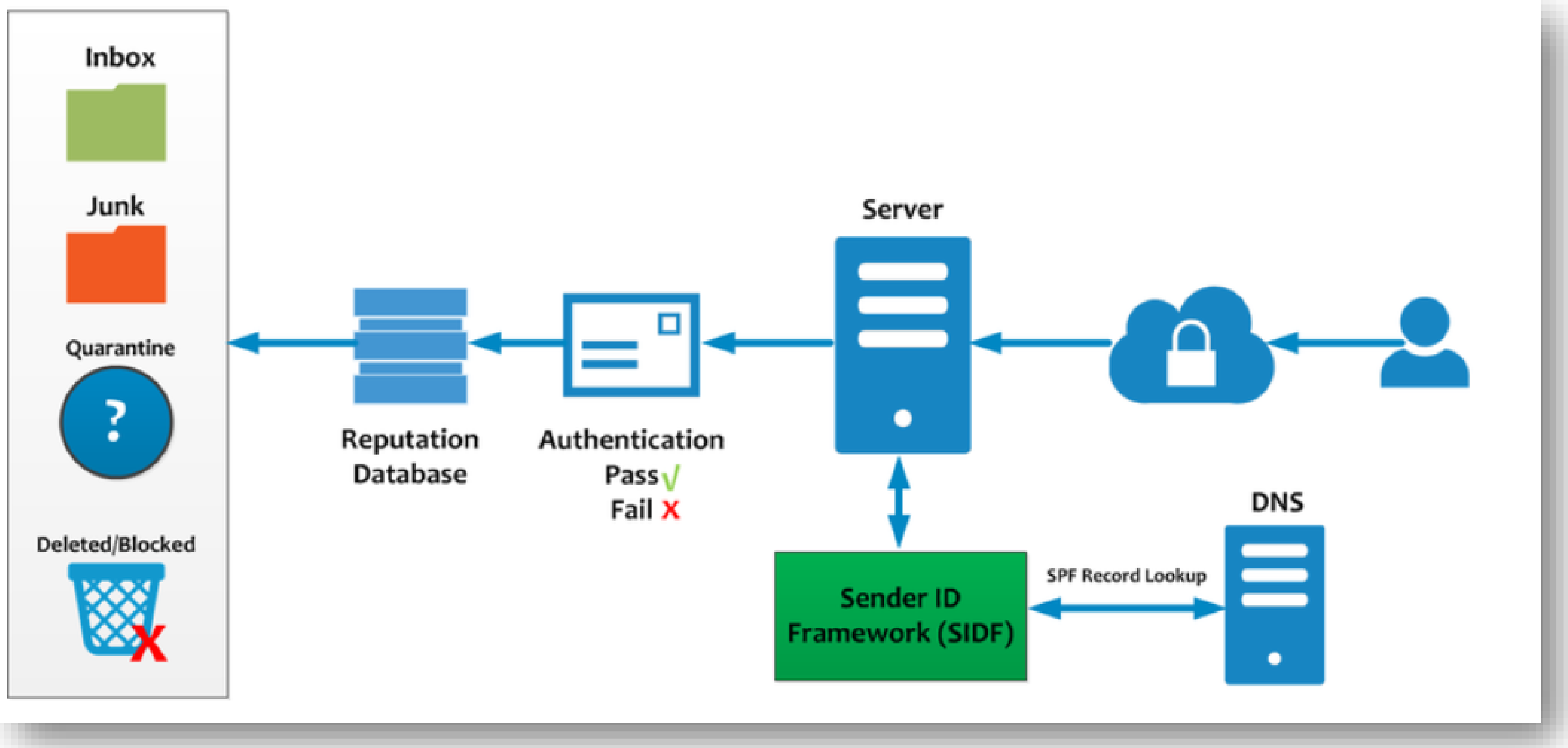
→ Vulnerable to spoofing without additional layers (e.g., SPF, DKIM, DMARC)
→ Does not inherently verify sender authenticity



```
telnet smtp.----.---- 25
Connected to smtp.----.----.
220 smtp.----.---- SMTP Ready
HELO client
250-smtp.----.----
250-PIPELINING
250 8BITMIME
MAIL FROM: <auteur@yyyy.yyyy>
250 Sender ok
RCPT TO: <destinataire@----.---->
250 Recipient ok.
DATA
354 Enter mail, end with "." on a line by itself
Subject: Test

Corps du texte
.
250 Ok
QUIT
221 Closing connection
Connection closed by foreign host.
```

Background

- *SPF (Sender Policy Framework)*



https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC

Background

○ *SPF (Sender Policy Framework)*

❖ Purpose

→ Defines which mail servers are authorized to send emails on behalf of a domain

❖ How It Works

→ Domain owners create SPF records in Public DNS
→ Receiving servers check the SPF record to verify if the sending IP is authorized

Background

- *SPF (Sender Policy Framework)*

❖ Benefits

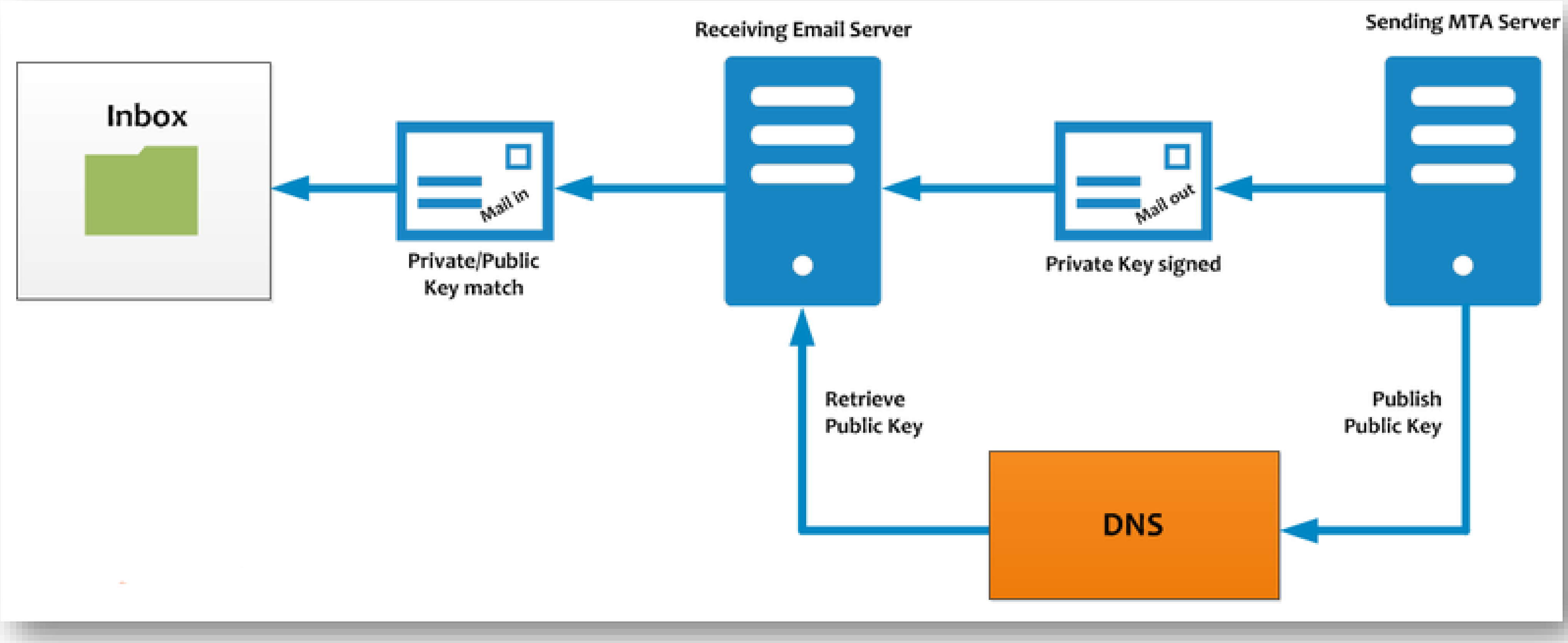
→ Reduces email spoofing
→ Simple to set up compared to other protocols

❖ Limitations

→ Does not work on forwarded emails
→ Cannot prevent phishing if the sender uses an authorized domain

Background

- *DKIM (DomainKey Identified Mail)*



https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC

Background

○ *DKIM (DomainKey Identified Mail)*

❖ Purpose

→ Adds a digital signature to outgoing emails to verify sender authenticity

❖ How It Works

→ The sender's domain generates a cryptographic key pair
→ The private key signs the email, and the public key is published in DNS records
→ The recipient verifies the signature using the public key

Background

○ *DKIM (DomainKey Identified Mail)*

❖ Benefits

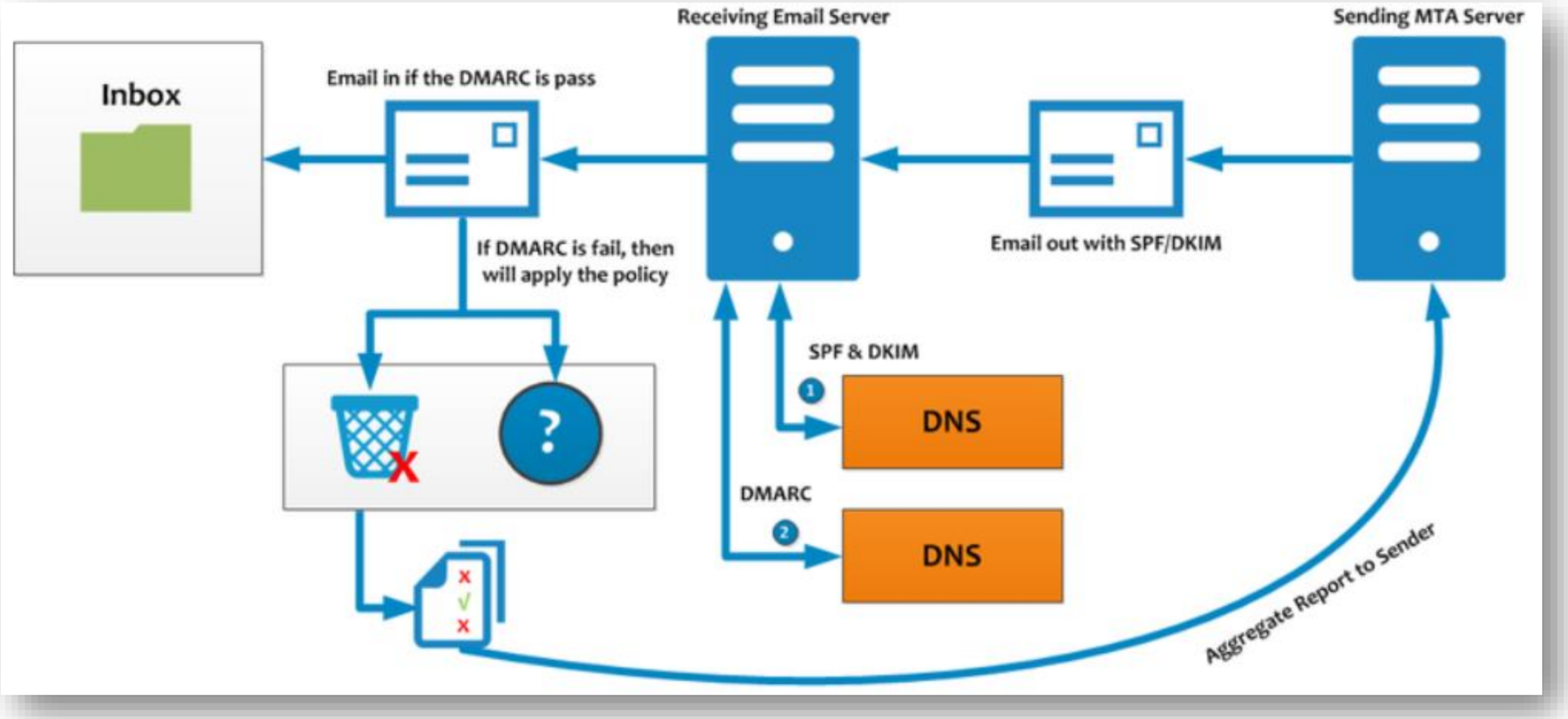
→ Prevents email tampering during transit
→ Establishes trust in sender identity

❖ Limitations

→ Does not directly prevent phishing or spoofing without DMARC
→ Relies on proper DNS configuration

Background

- DMARC (Domain-based Message Authentication, Reporting & Conformance)



Receiving Email Server
Sending MTA Server
Inbox
Email in if the DMARC is pass
If DMARC is fail, then will apply the policy
Email out with SPF/DKIM
SPF & DKIM
1
DNS
DMARC
2
DNS
Aggregate Report to Sender

https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC

Background

○ *DMARC (Domain-based Message Authentication, Reporting & Conformance)*

❖ Purpose

→ Builds on SPF and DKIM to provide policy enforcement for email authentication
→ Specifies how to handle unauthorized emails (reject, quarantine, or none)

❖ How It Works

→ Domain owners publish a DMARC record in DNS
→ Incoming emails are checked against SPF & DKIM
→ A report is generated on email authentication outcomes

Background

- *DMARC (Domain-based Message Authentication, Reporting & Conformance)*

❖ Benefits

→ Combats phishing and spoofing more effectively than SPF/DKIM alone
→ Provides detailed reports on email abuse attempts

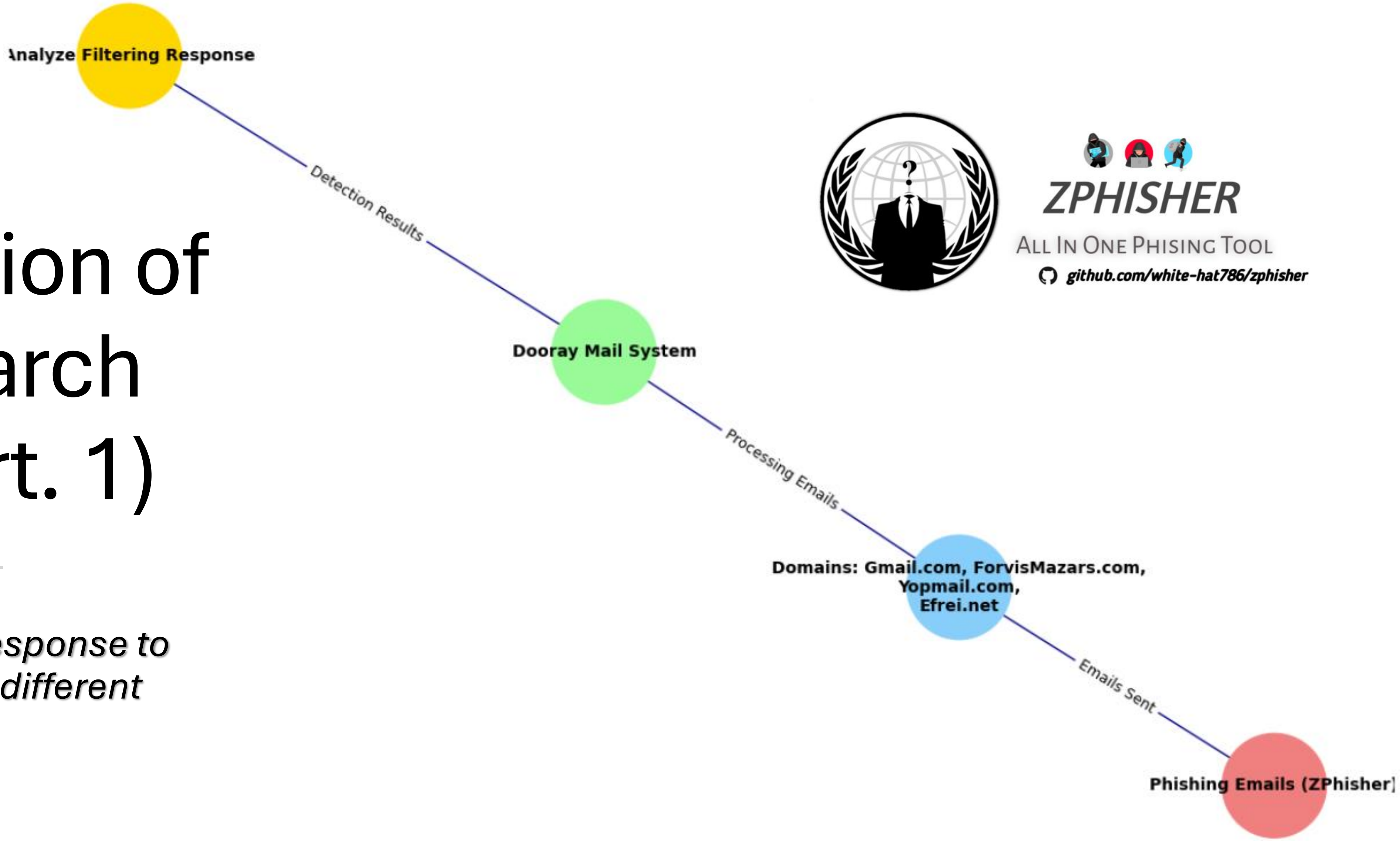
❖ Limitations

→ Requires correct SPF/DKIM configuration to work
→ Complex to implement for organizations with multiple email-sending services

Contribution of our Research Work (Part. 1)

Zphisher - Dooray's response to phishing emails from different domains

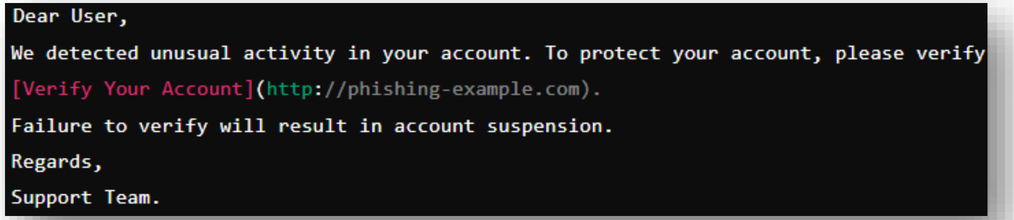
Phishing Email Testing Methodology



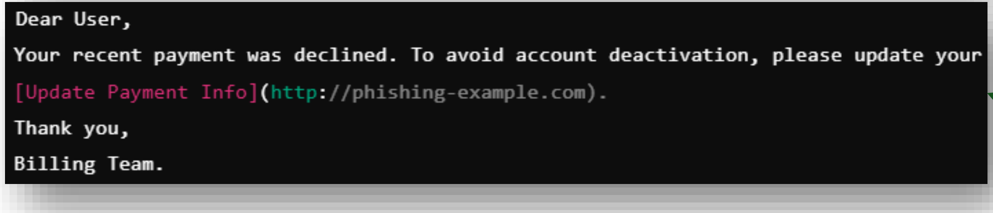
nalyze Filtering Response
Detection Results
Dooray Mail System
Processing Emails
Domains: Gmail.com, ForvisMazars.com, Yopmail.com, Efrei.net
Emails Sent
Phishing Emails (ZPhisher)
ZPHISHER
ALL IN ONE PHISING TOOL
github.com/white-hat786/zphisher

Research Work (Part. 1)

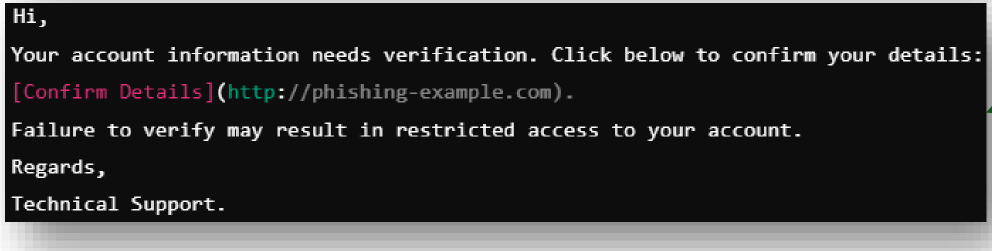
- *Zphisher - Dooray's response to phishing emails from different domains*



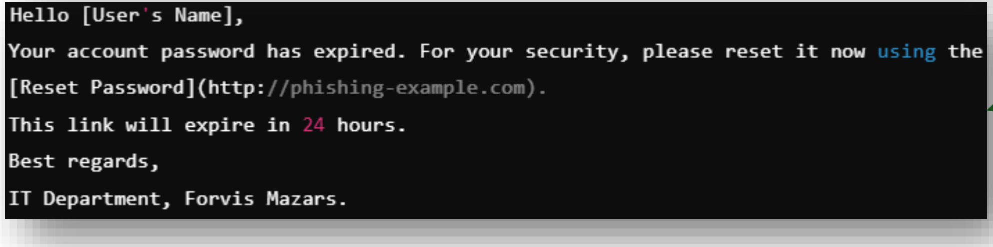
```
Dear User,
We detected unusual activity in your account. To protect your account, please verify
[Verify Your Account](http://phishing-example.com).
Failure to verify will result in account suspension.
Regards,
Support Team.
```



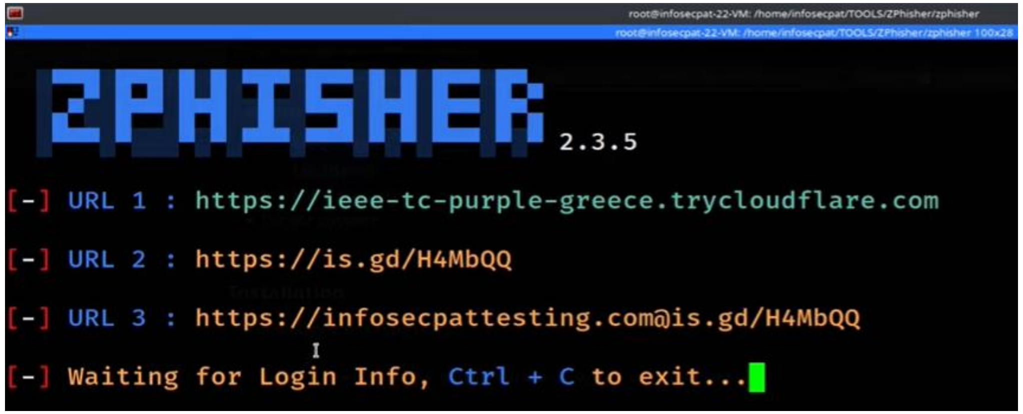
```
Dear User,
Your recent payment was declined. To avoid account deactivation, please update your
[Update Payment Info](http://phishing-example.com).
Thank you,
Billing Team.
```



```
Hi,
Your account information needs verification. Click below to confirm your details:
[Confirm Details](http://phishing-example.com).
Failure to verify may result in restricted access to your account.
Regards,
Technical Support.
```



```
Hello [User's Name],
Your account password has expired. For your security, please reset it now using the
[Reset Password](http://phishing-example.com).
This link will expire in 24 hours.
Best regards,
IT Department, Forvis Mazars.
```



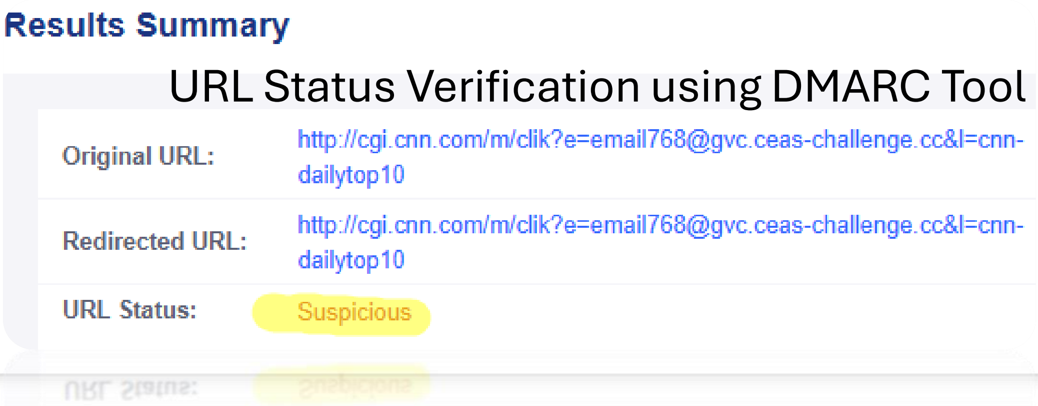
```
root@infosecpat-22-VM: /home/infosecpat/TOOLS/ZPhisher/zphisher
root@infosecpat-22-VM: /home/infosecpat/TOOLS/ZPhisher/zphisher 100x28

ZPHISHER 2.3.5

[-] URL 1 : https://ieee-tc-purple-greece.trycloudflare.com

[-] URL 2 : https://is.gd/H4MbQQ

[-] URL 3 : https://infosecpattesting.com@is.gd/H4MbQQ

[-] Waiting for Login Info, Ctrl + C to exit...
```

Zphisher is used to generate emails
containing fraudulent URLs
for phishing detection testing.

Research Work (Part. 1)

○ *Result – Gmail -> Dooray*

URL Status Verification using DMARC Tool



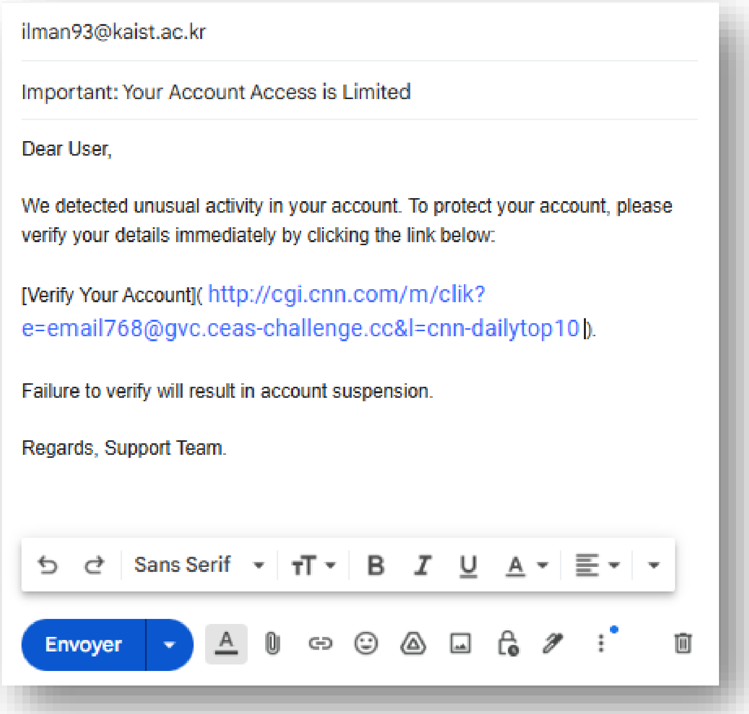
Results Summary

Original URL: http://cgi.cnn.com/m/clik?e=email768@gvc.ceas-challenge.cc&l=cnn-dailytop10

Redirected URL: http://cgi.cnn.com/m/clik?e=email768@gvc.ceas-challenge.cc&l=cnn-dailytop10

URL Status: Suspicious

Sent email from Gmail



ilman93@kaist.ac.kr

Important: Your Account Access is Limited

Dear User,

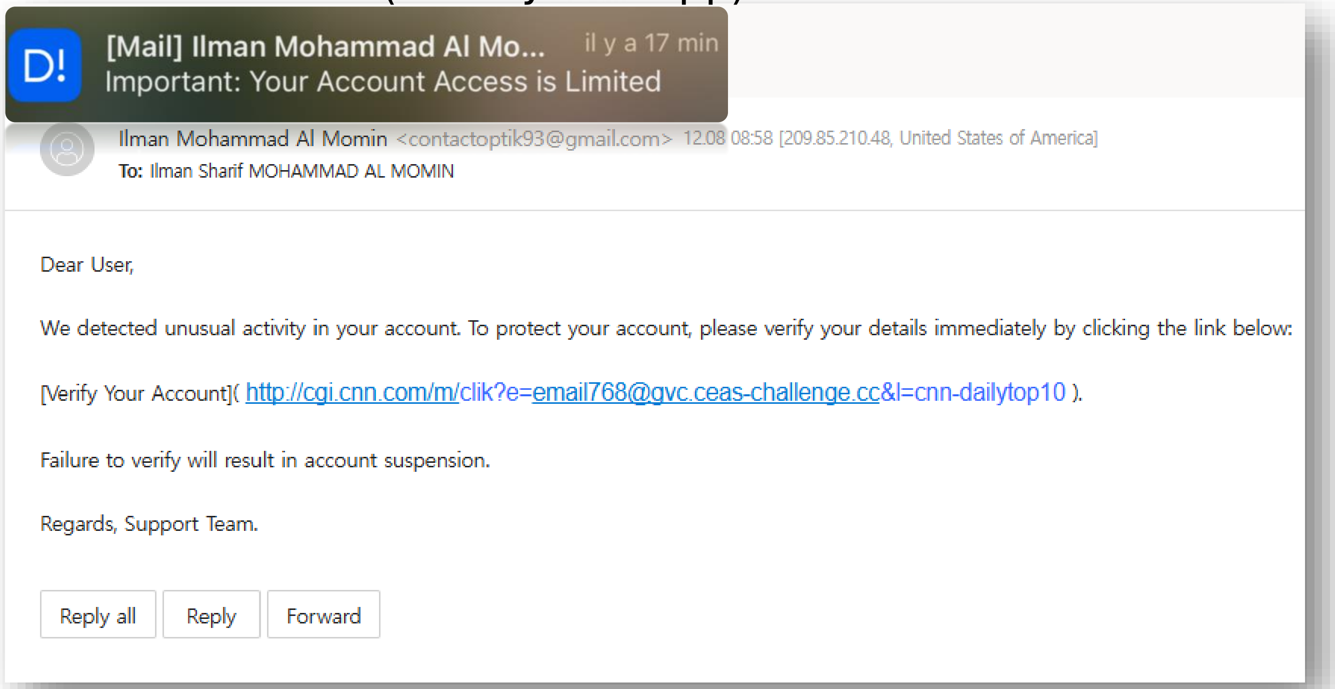
We detected unusual activity in your account. To protect your account, please verify your details immediately by clicking the link below:

[Verify Your Account](http://cgi.cnn.com/m/clik?e=email768@gvc.ceas-challenge.cc&l=cnn-dailytop10).

Failure to verify will result in account suspension.

Regards, Support Team.

Phone Notification (Dooray Mail App)



D! [Mail] Ilman Mohammad Al Mo... il y a 17 min
Important: Your Account Access is Limited

Ilman Mohammad Al Momin <contactoptik93@gmail.com> 12.08 08:58 [209.85.210.48, United States of America]
To: Ilman Sharif MOHAMMAD AL MOMIN

Dear User,

We detected unusual activity in your account. To protect your account, please verify your details immediately by clicking the link below:

[Verify Your Account](http://cgi.cnn.com/m/clik?e=email768@gvc.ceas-challenge.cc&l=cnn-dailytop10).

Failure to verify will result in account suspension.

Regards, Support Team.

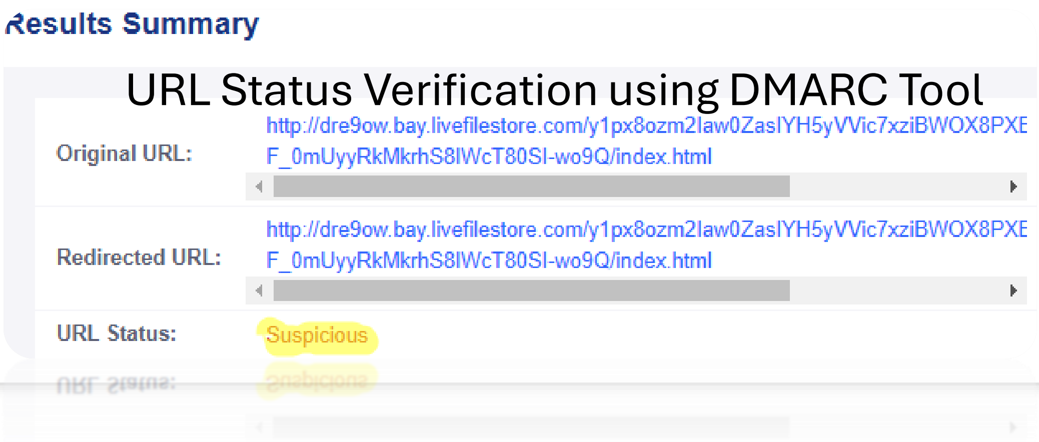
Email Reception on Mailbox (Dooray)

Phishing Email Test: Gmail → Dooray (Not Detected)

Gmail
Dooray (Not Detected

Research Work (Part. 1)

○ *Result – Forvis Mazars -> Dooray*

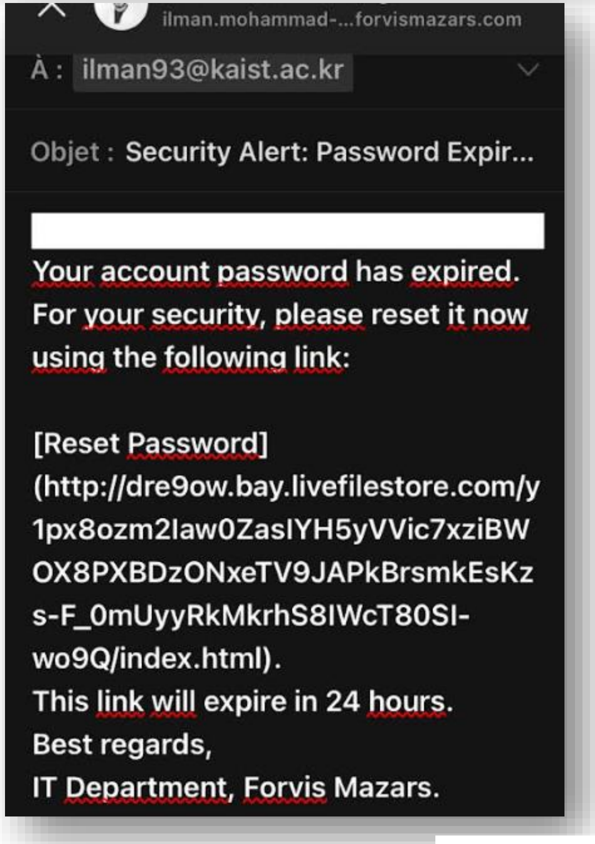


URL Status Verification using DMARC Tool

Results Summary

Original URL:	http://dre9ow.bay.livefilestore.com/y1px8ozm2law0ZasIYH5yVVic7xziBWOX8PXBF_0mUyyRkMkrhS8IWcT80SI-wo9Q/index.html
Redirected URL:	http://dre9ow.bay.livefilestore.com/y1px8ozm2law0ZasIYH5yVVic7xziBWOX8PXBF_0mUyyRkMkrhS8IWcT80SI-wo9Q/index.html
URL Status:	Suspicious

Sent email from Work Domain



ilman.mohammad-...forvismazars.com

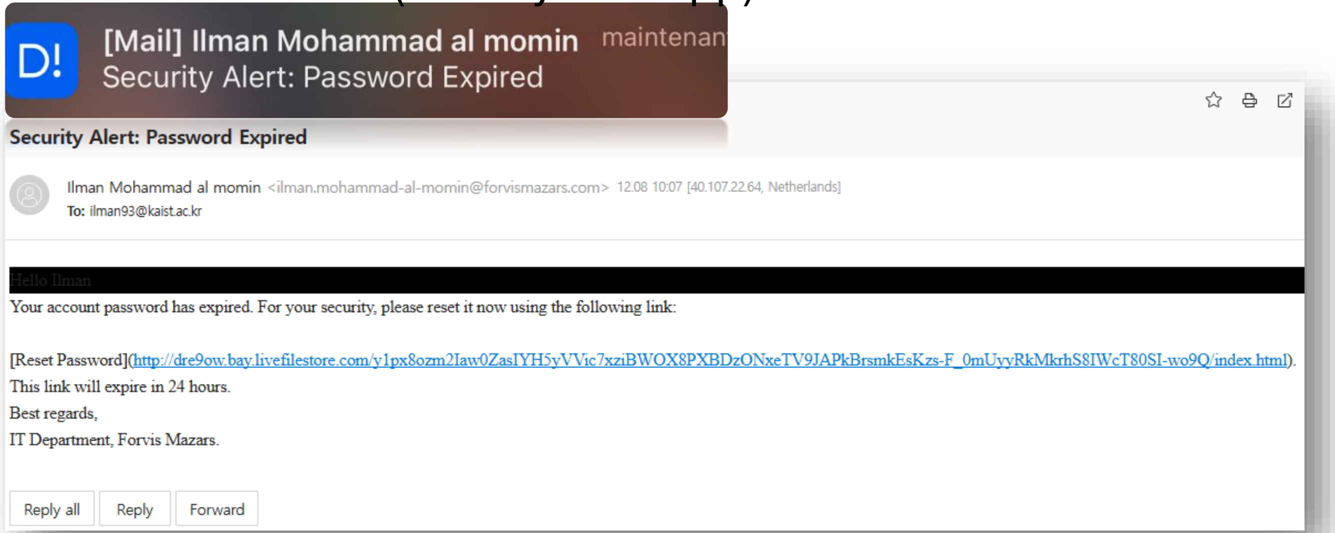
À : ilman93@kaist.ac.kr

Objet : Security Alert: Password Expir...

Your account password has expired. For your security, please reset it now using the following link:

[Reset Password](http://dre9ow.bay.livefilestore.com/y1px8ozm2law0ZasIYH5yVVic7xziBWOX8PXBDzONxeTV9JAPkBrsmkEsKzs-F_0mUyyRkMkrhS8IWcT80SI-wo9Q/index.html).
This link will expire in 24 hours.
Best regards,
IT Department, Forvis Mazars.

Phone Notification (Dooray Mail App)



[Mail] Ilman Mohammad al momin   maintenan
Security Alert: Password Expired

Security Alert: Password Expired

Ilman Mohammad al momin <ilman.mohammad-al-momin@forvismazars.com> 12.08 10:07 [40.107.22.64, Netherlands]
To: ilman93@kaist.ac.kr

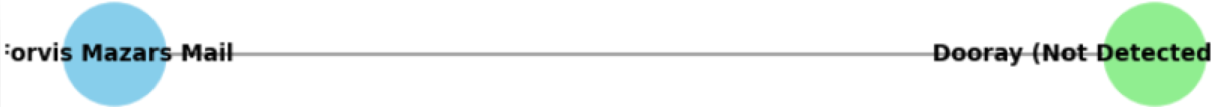
[redacted]

Your account password has expired. For your security, please reset it now using the following link:

[Reset Password](http://dre9ow.bay.livefilestore.com/y1px8ozm2law0ZasIYH5yVVic7xziBWOX8PXBDzONxeTV9JAPkBrsmkEsKzs-F_0mUyyRkMkrhS8IWcT80SI-wo9Q/index.html).
This link will expire in 24 hours.
Best regards,
IT Department, Forvis Mazars.

Email Reception on Mailbox (Dooray)

Phishing Email Test: Forvis Mazars Mail → Dooray (Not Detected)

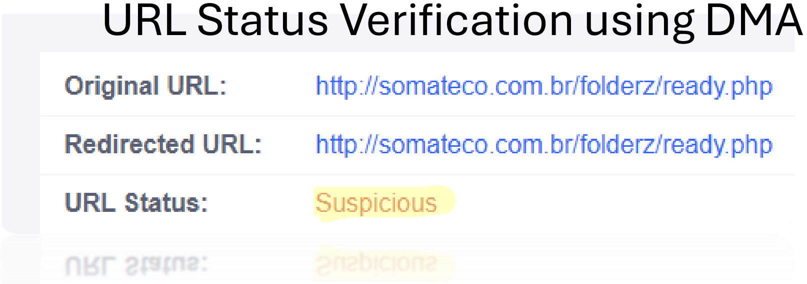


Research Work (Part. 1)

○ *Result – EFREI.net -> Dooray*

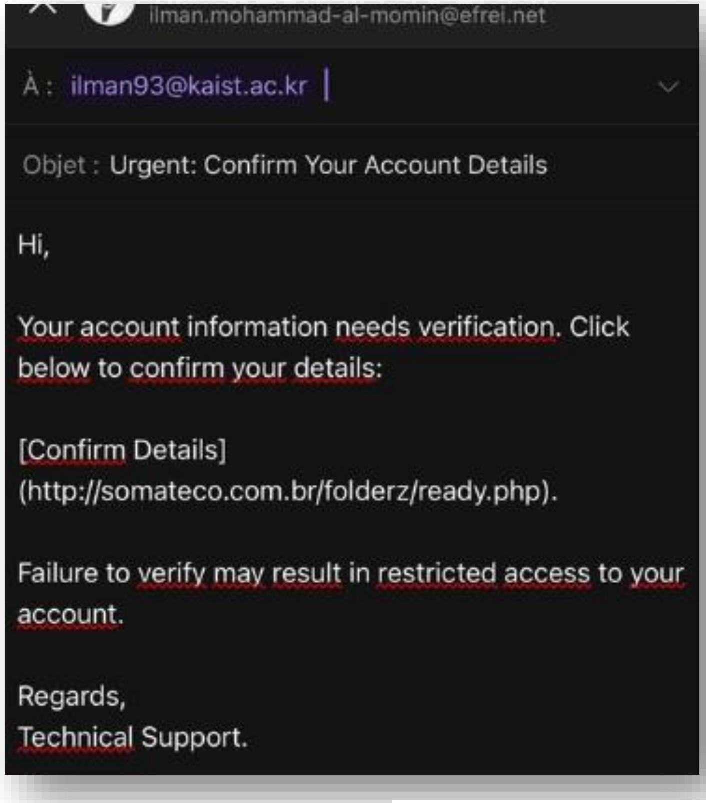
Results Summary

URL Status Verification using DMARC Tool



Original URL:	http://somateco.com.br/folderz/ready.php
Redirected URL:	http://somateco.com.br/folderz/ready.php
URL Status:	Suspicious

Sent email from home university domain



ilman.mohammad-al-momin@efrei.net

À : ilman93@kaist.ac.kr

Objet : Urgent: Confirm Your Account Details

Hi,

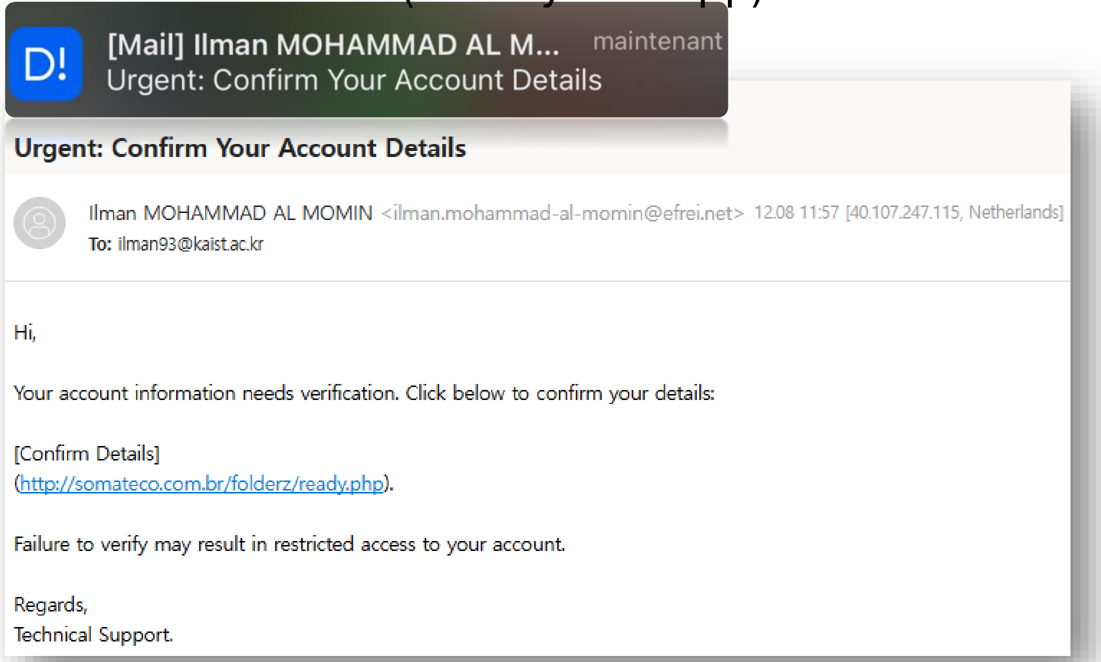
Your account information needs verification. Click below to confirm your details:

[Confirm Details]
(http://somateco.com.br/folderz/ready.php).

Failure to verify may result in restricted access to your account.

Regards,
Technical Support.

Phone Notification (Dooray Mail App)



D! [Mail] Ilman MOHAMMAD AL M... maintenant
Urgent: Confirm Your Account Details

Urgent: Confirm Your Account Details

Ilman MOHAMMAD AL MOMIN <ilman.mohammad-al-momin@efrei.net> 12.08 11:57 [40.107.247.115, Netherlands]
To: ilman93@kaist.ac.kr

Hi,

Your account information needs verification. Click below to confirm your details:

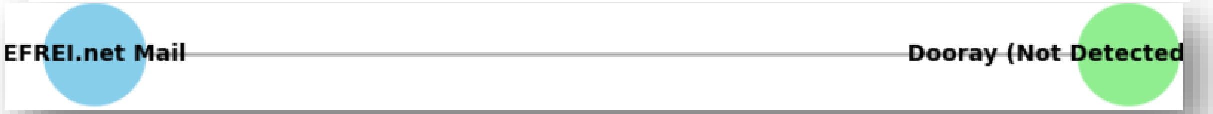
[Confirm Details]
(http://somateco.com.br/folderz/ready.php).

Failure to verify may result in restricted access to your account.

Regards,
Technical Support.

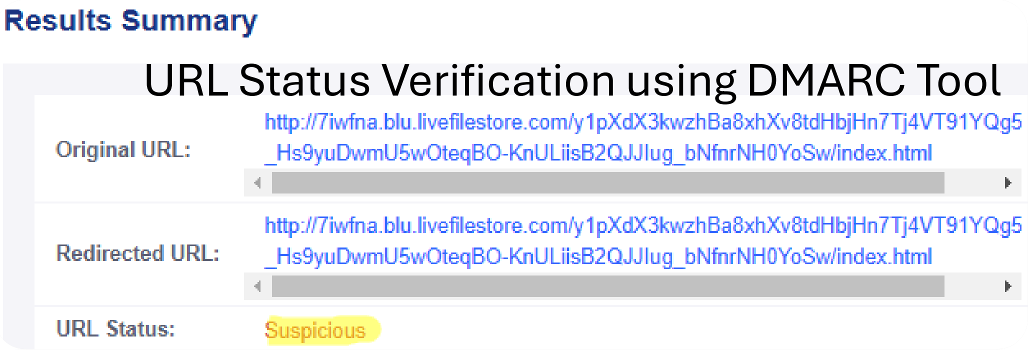
Email Reception on Mailbox (Dooray)

Phishing Email Test: EFREI.net Mail → Dooray (Not Detected)



Research Work (Part. 1)

○ *Result – YopMail -> Dooray*

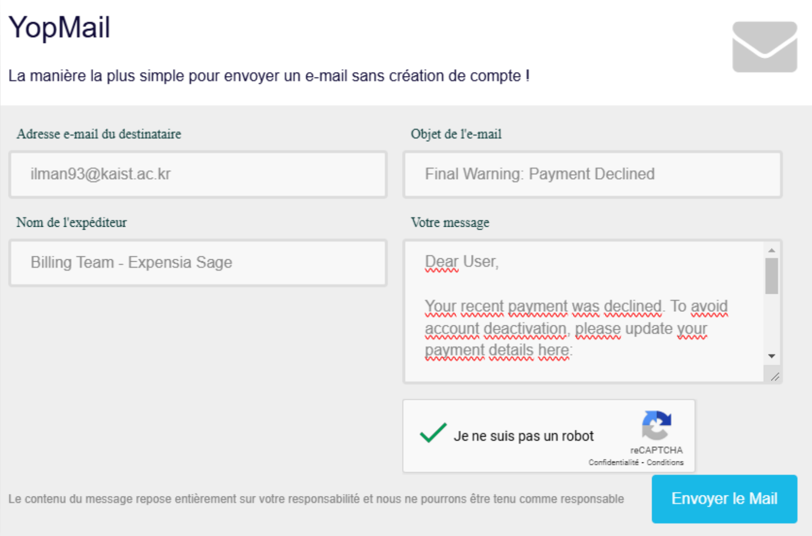


URL Status Verification using DMARC Tool

Results Summary

Original URL:	http://7iwfna.blu.livefilestore.com/y1pXdX3kwzhBa8xhXv8tdHbjHn7Tj4VT91YQg5_Hs9yuDwmU5wOteqBO-KnULiisB2QJJlug_bNfnrNH0YoSw/index.html
Redirected URL:	http://7iwfna.blu.livefilestore.com/y1pXdX3kwzhBa8xhXv8tdHbjHn7Tj4VT91YQg5_Hs9yuDwmU5wOteqBO-KnULiisB2QJJlug_bNfnrNH0YoSw/index.html
URL Status:	Suspicious

Sent email from YopMail
(not DMARC registered)



YopMail

La manière la plus simple pour envoyer un e-mail sans création de compte !

Adresse e-mail du destinataire: ilman93@kaist.ac.kr

Objet de l'e-mail: Final Warning: Payment Declined

Nom de l'expéditeur: Billing Team - Expensia Sage

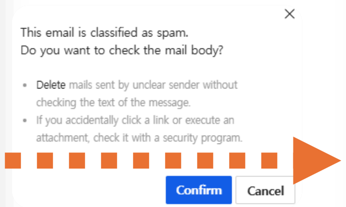
Votre message:
Dear User,

Your recent payment was declined. To avoid account deactivation, please update your payment details here:

☑ Je ne suis pas un robot

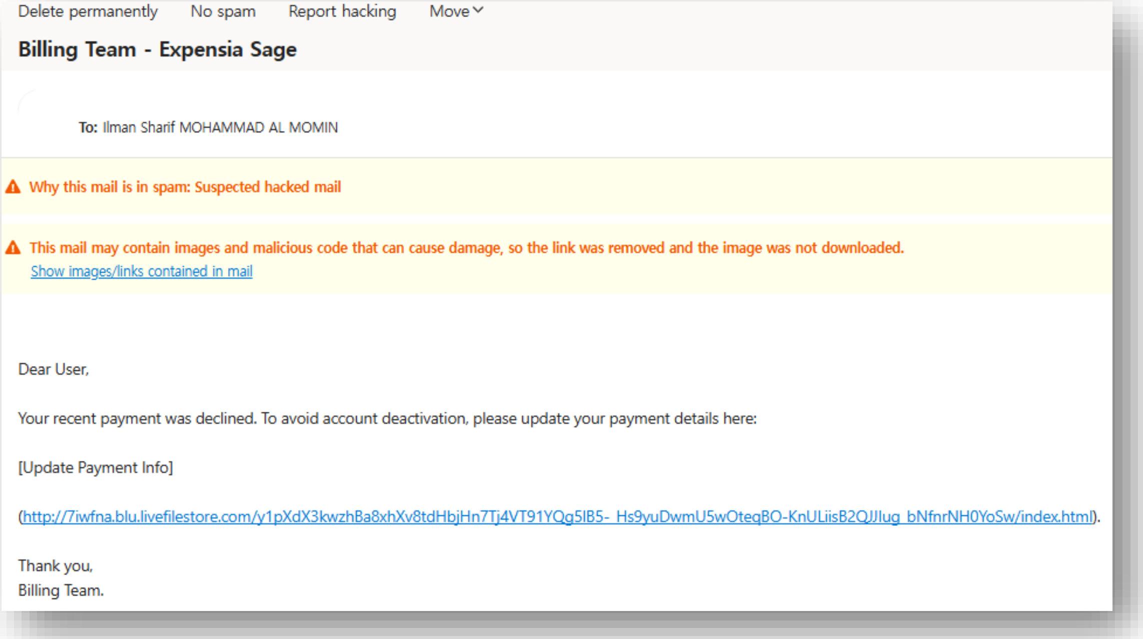
Le contenu du message repose entièrement sur votre responsabilité et nous ne pourrons être tenu comme responsable

Spam Notification on Dooray web app



This email is classified as spam.
Do you want to check the mail body?

- **Delete** mails sent by unclear sender without checking the text of the message.
- If you accidentally click a link or execute an attachment, check it with a security program.



Billing Team - Expensia Sage

To: Ilman Sharif MOHAMMAD AL MOMIN

⚠ Why this mail is in spam: Suspected hacked mail

⚠ This mail may contain images and malicious code that can cause damage, so the link was removed and the image was not downloaded.
Show images/links contained in mail

Dear User,

Your recent payment was declined. To avoid account deactivation, please update your payment details here:

[Update Payment Info]

(http://7iwfna.blu.livefilestore.com/y1pXdX3kwzhBa8xhXv8tdHbjHn7Tj4VT91YQg5IB5-_Hs9yuDwmU5wOteqBO-KnULiisB2QJJlug_bNfnrNH0YoSw/index.html).

Thank you,
Billing Team.

Email Reception on Spam Mailbox (Dooray)

Phishing Email Test: YopMail → Dooray (Detected)

YopMail
Dooray (Detected a

Contribution of our Research Work (Part. 2)

- *Machine Learning Based Phishing Detection Tools*
  - *First Tool: Phishing Mail Detection*
  - *Second Tool: Phishing URL Detection*

→ *Evaluation of both models using an External Dataset (CEAS_08.csv)*

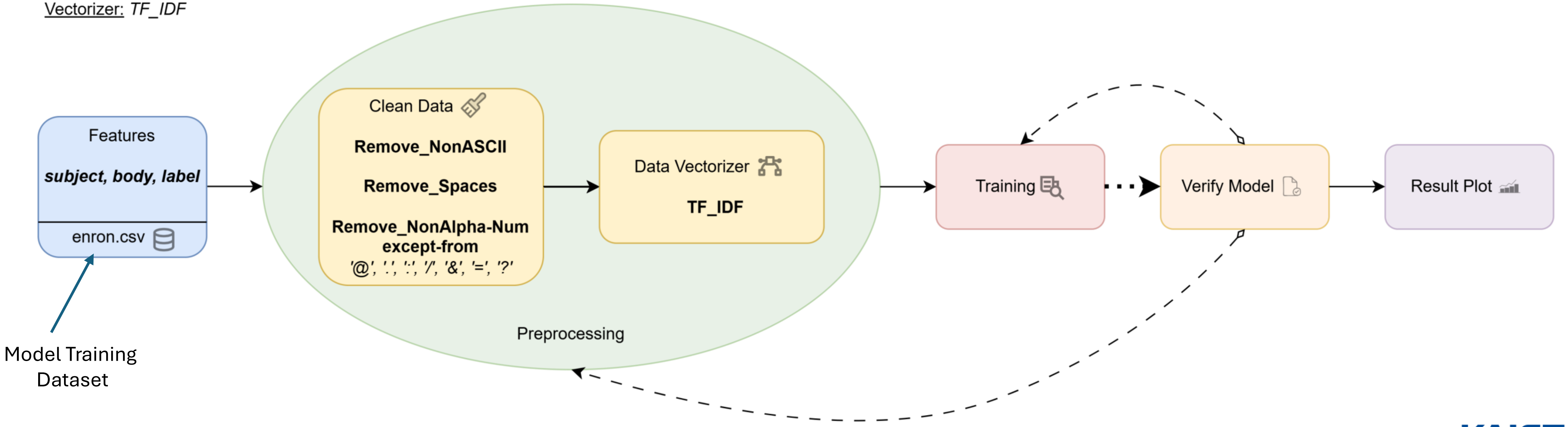
Methodology

Mail Model In Detail

Mail Model

Based on *Logistic Regression*

Vectorizer: *TF_IDF*



Features

subject, body, label

enron.csv

Clean Data

Remove_NonASCII

Remove_Spaces

Remove_NonAlpha-Num except-from

'@', '.', ':', '/', '&', '=', '?'

Data Vectorizer

TF_IDF

Preprocessing

Training

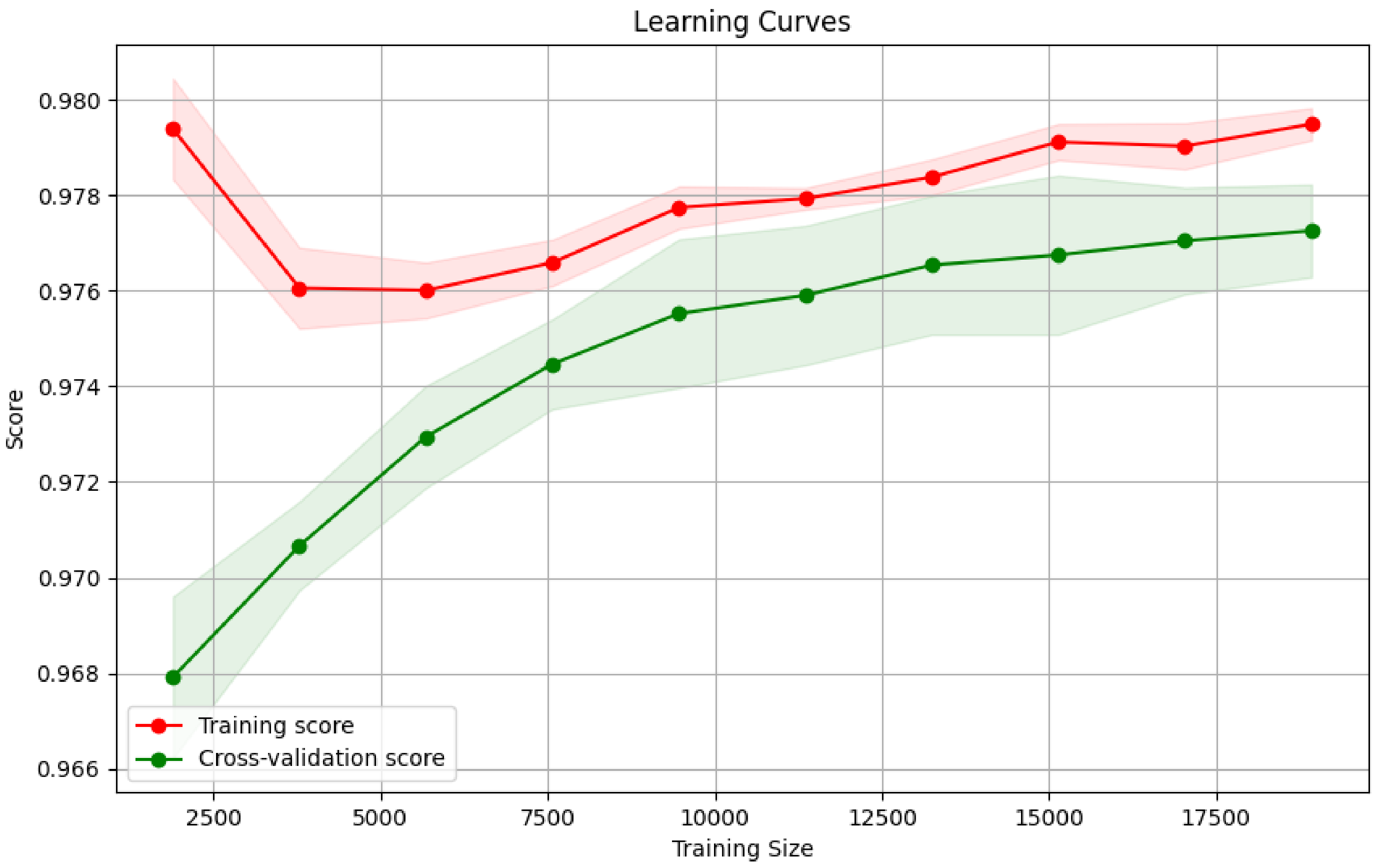
Verify Model

Result Plot

Model Training Dataset

Results

Learning Curves for Mail Model using Logistic Regression

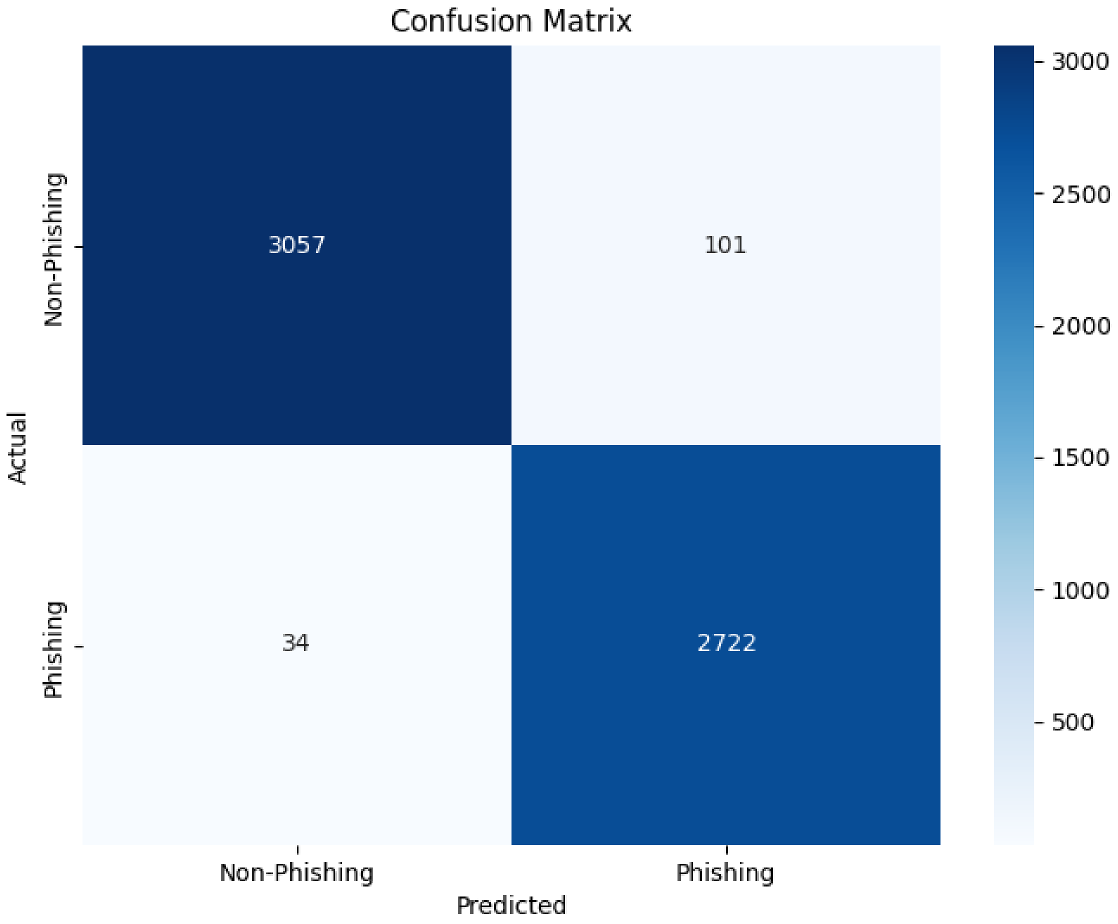


Comment:
This graph shows us that
our model is not Over / Under Fitting
using the enron.csv dataset

Checking Learning Curves
ensure us that the Model is
capable to replicate the result on
external dataset

Results

Confusion Matrix for Mail Model using Logistic Regression



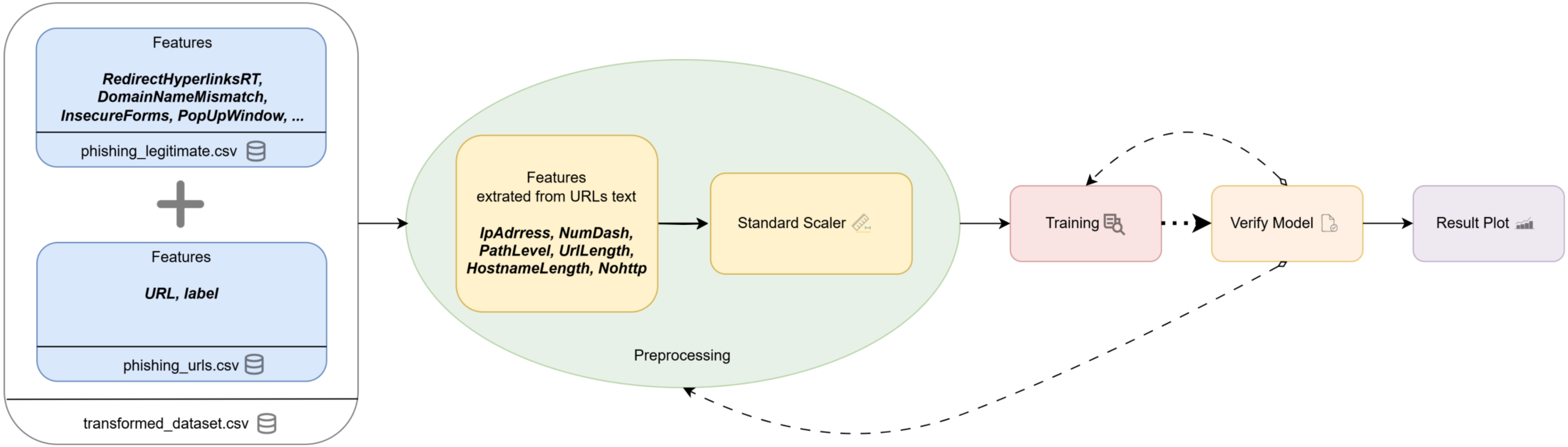
Comment **:**
This Confusion Matrix shows us that the Model successfully identified most phishing and non-phishing emails, with 101 false positives and 34 false negatives, indicating areas for potential improvement.

Methodology

URL Model In Detail

URL Model

Based on *Boosting Trees (XGBoost)*



Features

RedirectHyperlinksRT, DomainNameMismatch, InsecureForms, PopUpWindow, ...

phishing_legitimate.csv

+

Features

URL, label

phishing_urls.csv

transformed_dataset.csv

Features extrated from URLs text

IpAdrress, NumDash, PathLevel, UrlLength, HostnameLength, Nohttp

Standard Scaler

Preprocessing

Training

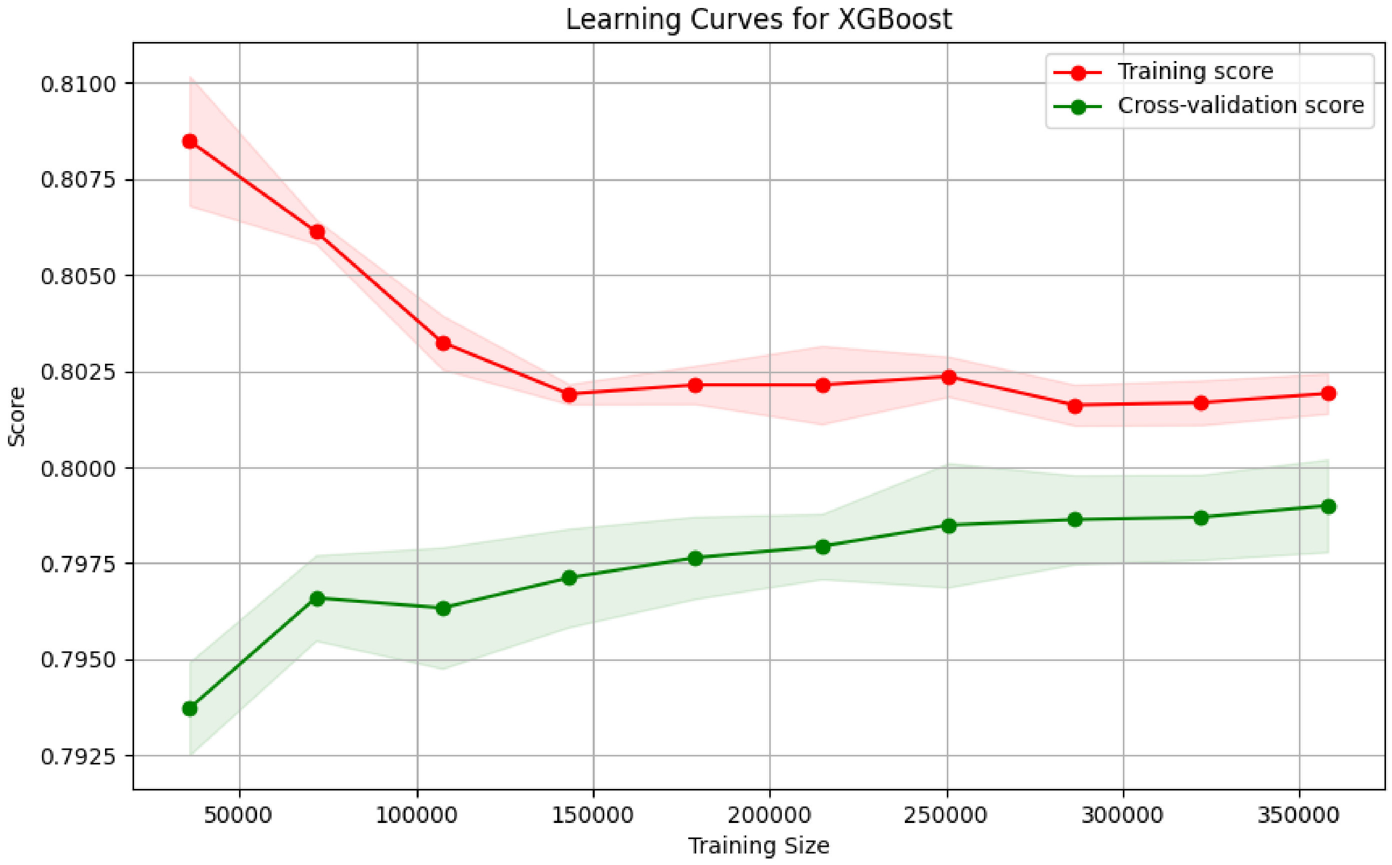
Verify Model

Result Plot

Model Training
Combined Datasets

Results

Learning Curves for URL Model using Boosting Trees (XGBoost)

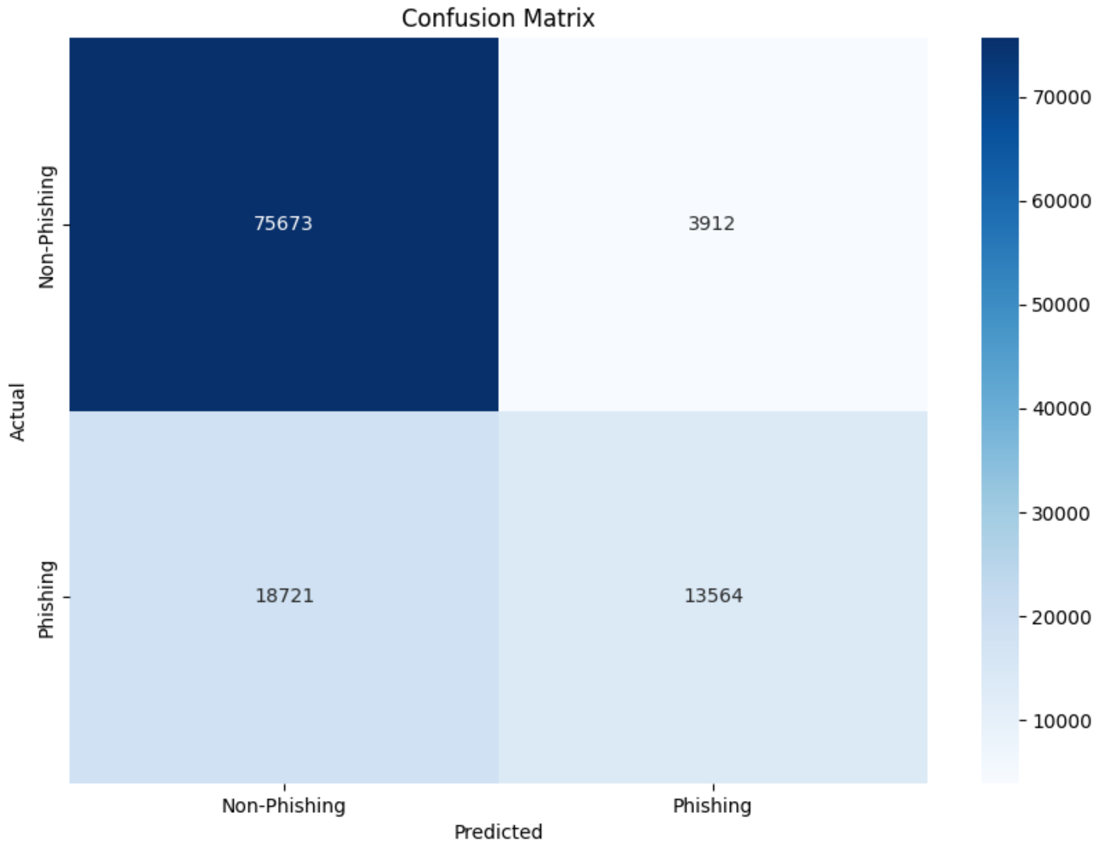


Comment:
This graph shows us that
our model is not Over / Under Fitting
using the enron.csv dataset

Checking Learning Curves
ensure us that the Model is
capable to replicate the result on
external dataset

Results

Confusion Matrix for URL Model using Boosting Trees (XGBoost)



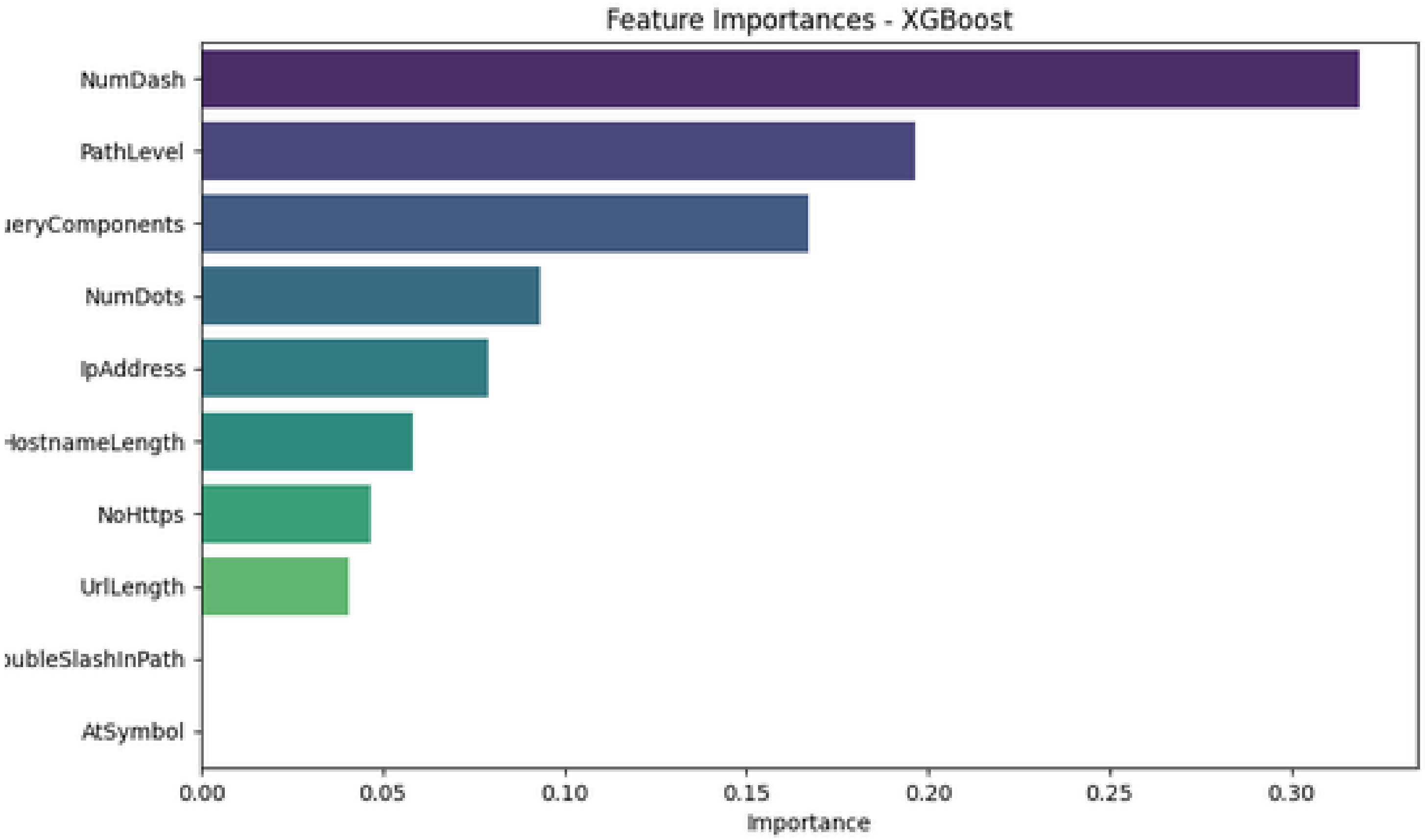
Comment :
The model performs well in detecting non-phishing URLs but performs poorly on detecting phishing emails, indicating a need for improved sensitivity. However, we used the ability of this model to detect non-phishing emails for the rest of our work.

Features Exploitation

Extracted URL Features

classified by Importance

phishing_legitimate.csv



Features Extraction used to train our XGBoost model

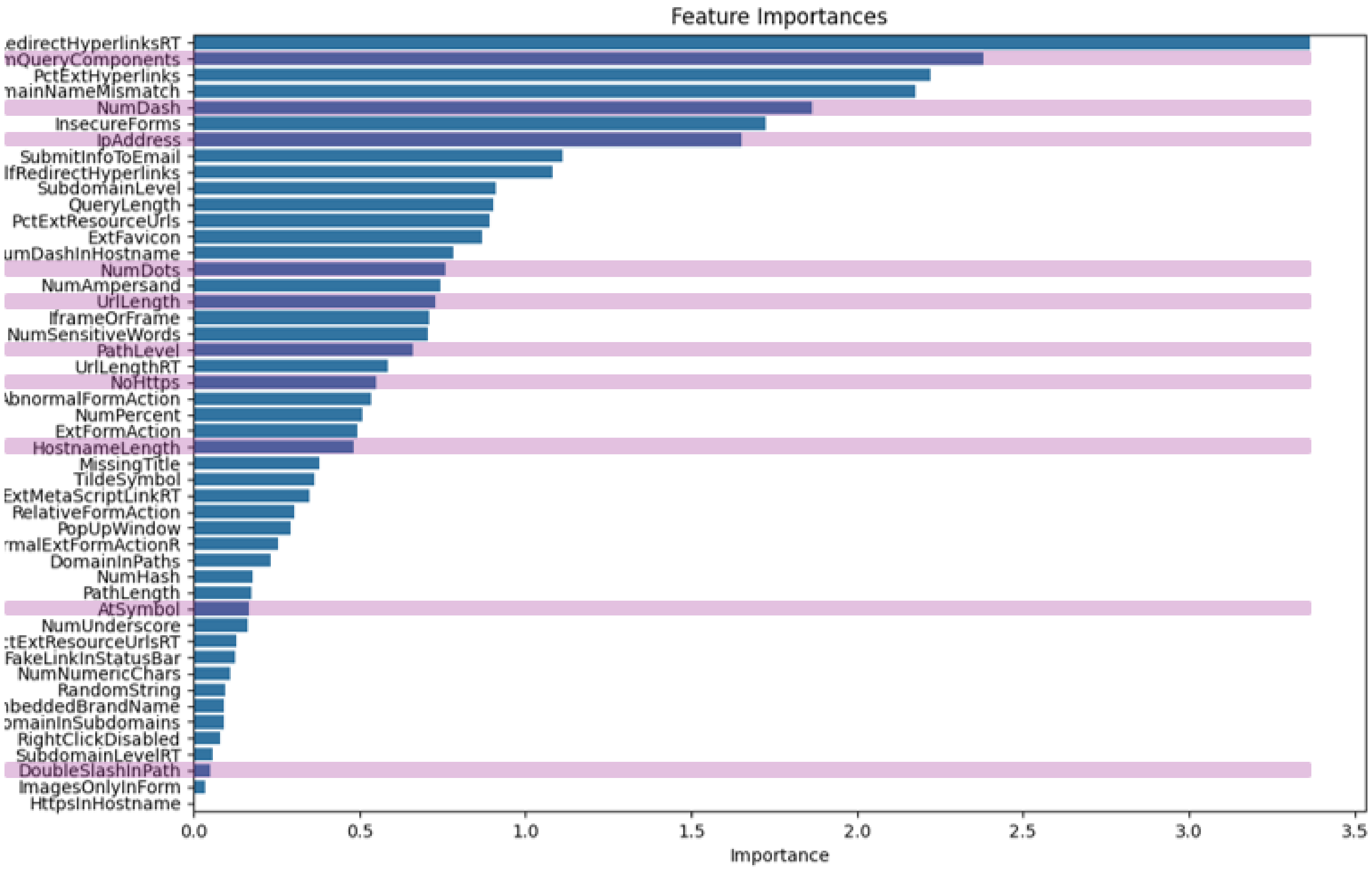
Comment :
This plot show the features used for training our model in order to classify the emails.

Features Exploitation

Extracted URL Features

classified by Importance

phishing_legitimate.csv



The **48 features** contained in the dataset vs the **10 features** we used in training our model

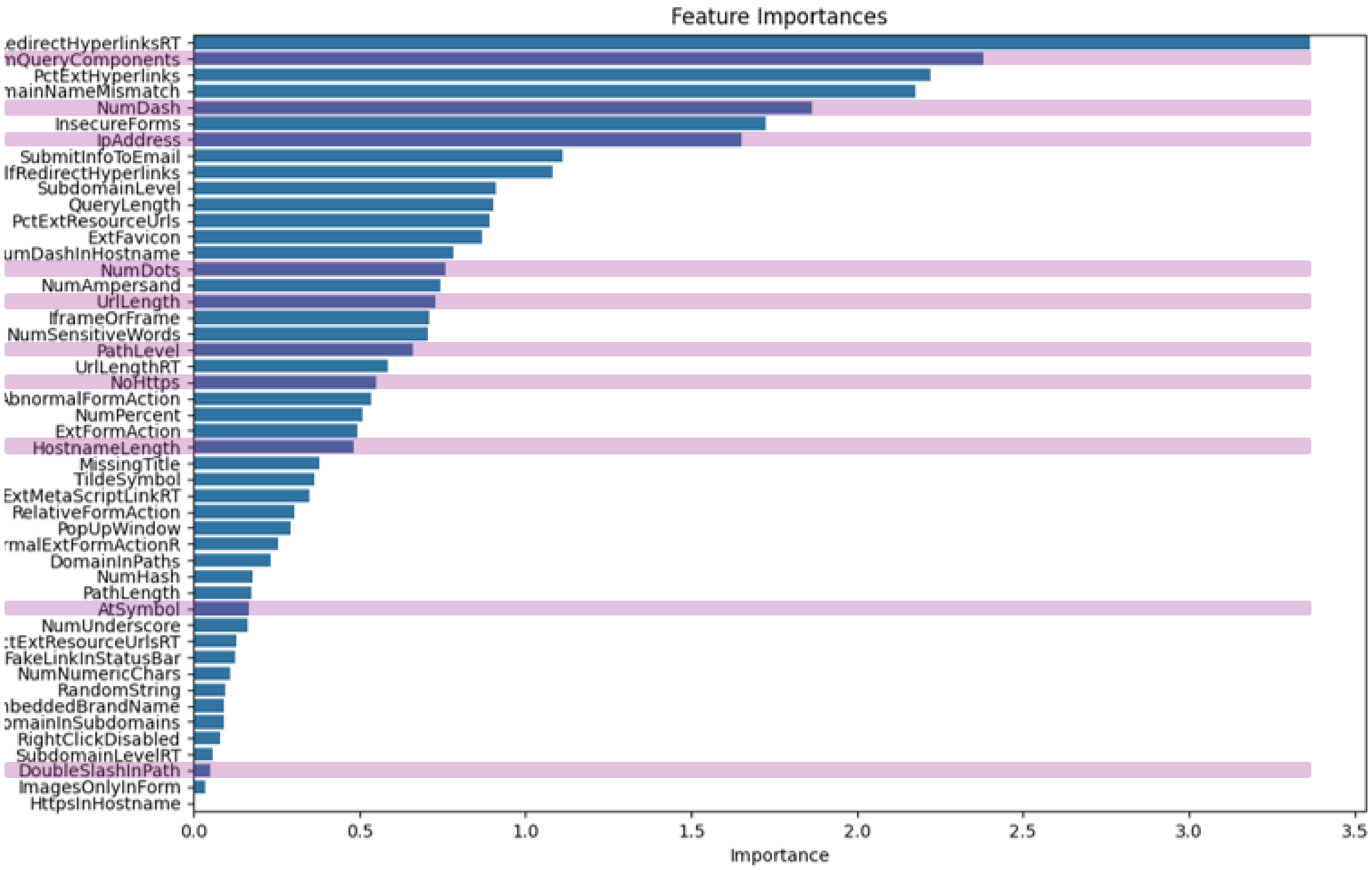
Comment :
The dataset used *Selenium Web Driver ToolKit* to extract the features from each URL.

Features Exploitation

Extracted URL Features

classified by Importance

phishing_legitimate.csv



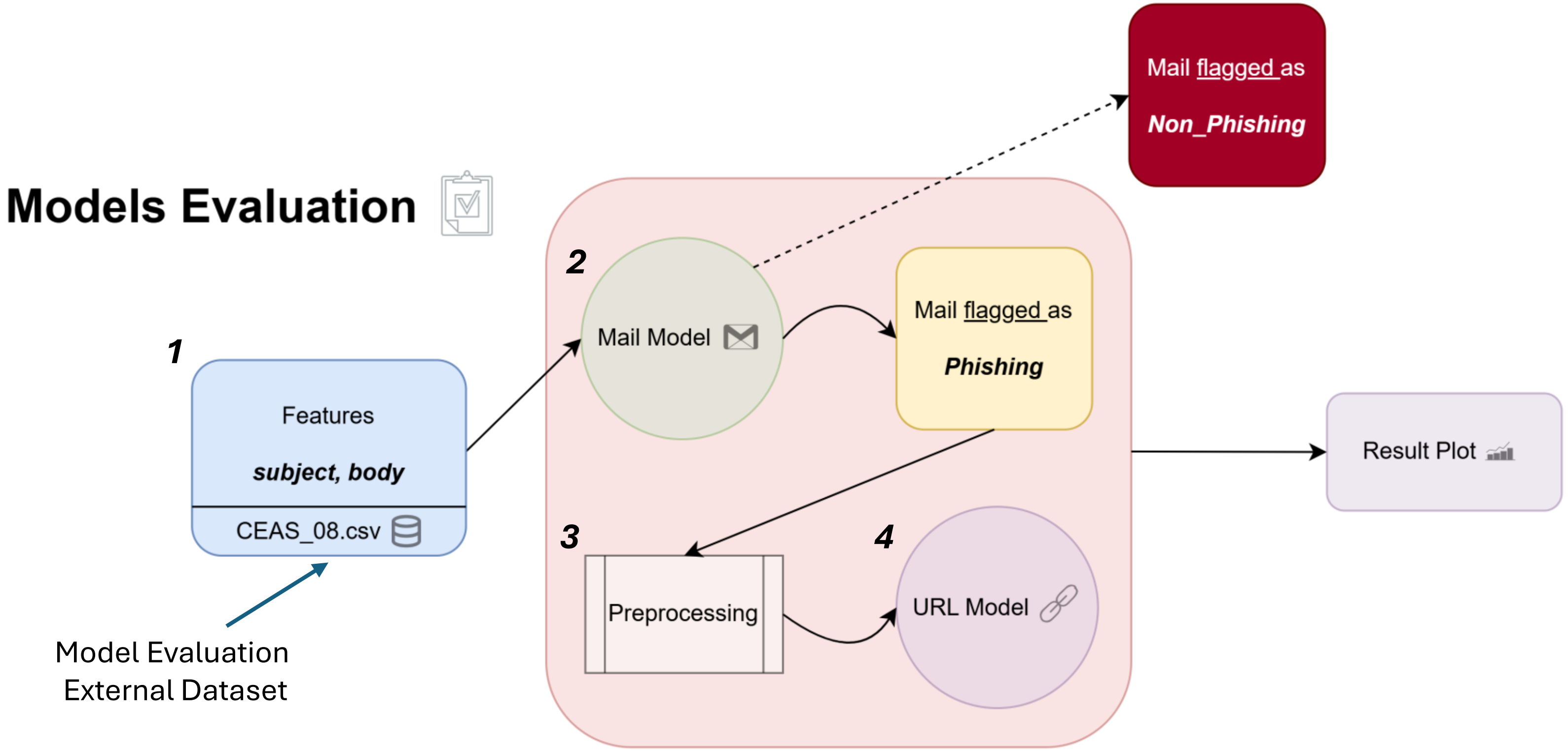
Comment :

We didn’t use the 48 features of the dataset because when testing our model, most of the websites from the URLs were down as the mails were old.

→ *We focused only on the « persistent » features.*

Methodology

Models Evaluation In Detail



Model Evaluation
External Dataset

Comment:

1 - We use an external dataset to test our framework.

2 - We use the Mail Model to flag mails as ***Phishing*** or ***Non-Phishing***.

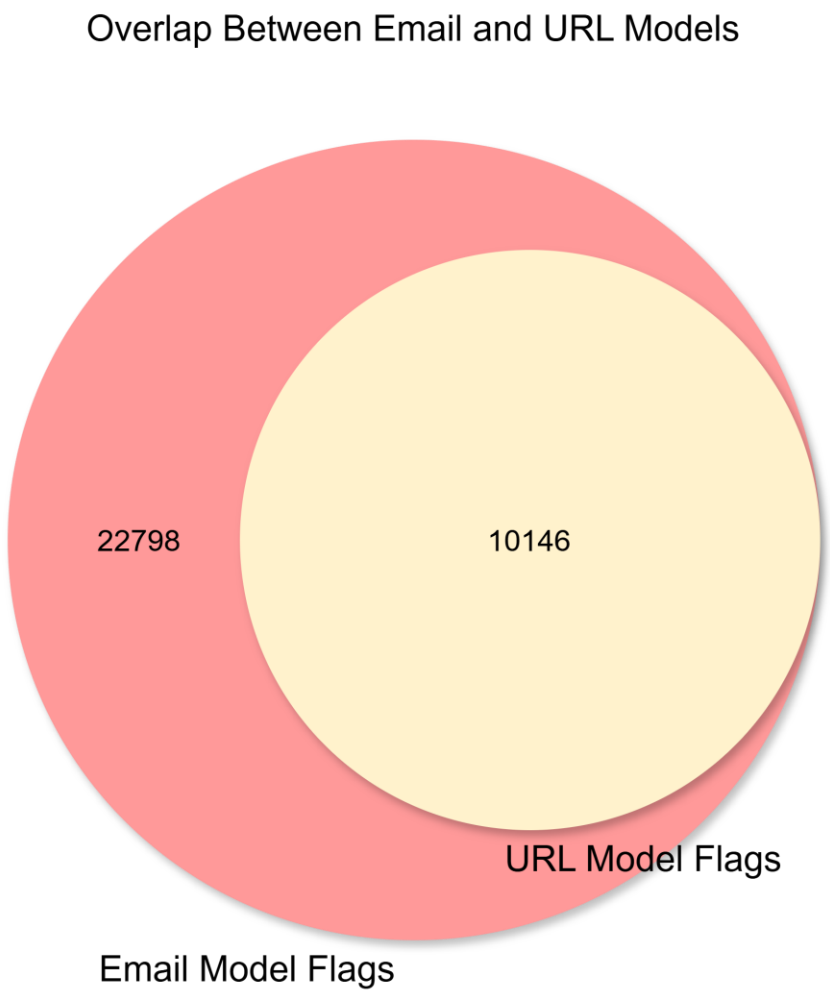
3 - We scrap all the URLs from the mail that are flagged as Phishing (Preprocessing)

4 - We use the URL Model to flag those URLs as Phishing / Non-Phishing.

Evaluation of Models

Venn Diagram

for Comparative Results



Comment :

This diagram shows the result of the evalution of our framework on the CEAS_08 dataset:

*→ The first Mail Model flags 22798 emails as **phishing***

- We extract the URLs from all these emails,

*(if they have **URLs**, otherwise they are labelled as **non-phishing**)*

*- We preprocess & transfer them into the second URL model, we separate **non-phishing** from **phishing** URLs*

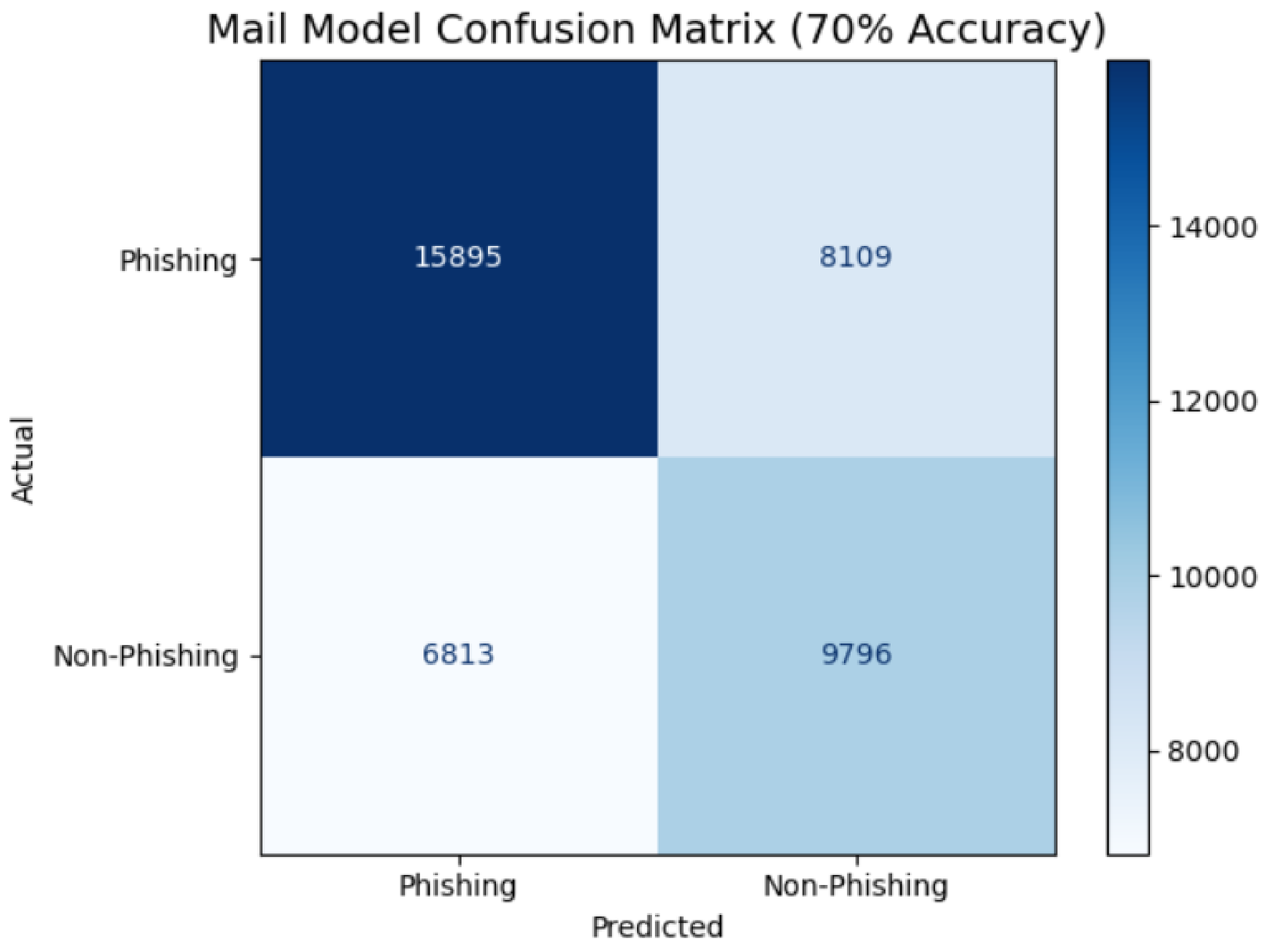
(the model has a high accuracy for detecting non-phishing URLs)

*→ We find 10146 emails flagged as **phishing**.*

Evaluation of Models

Confusion Matrix for Mail Model

using Boosting Trees (XGBoost) on CEAS_08 Dataset



Comment **:**
Evaluation the Mail Model using CEAS_08 gave us an accuracy of 70%.

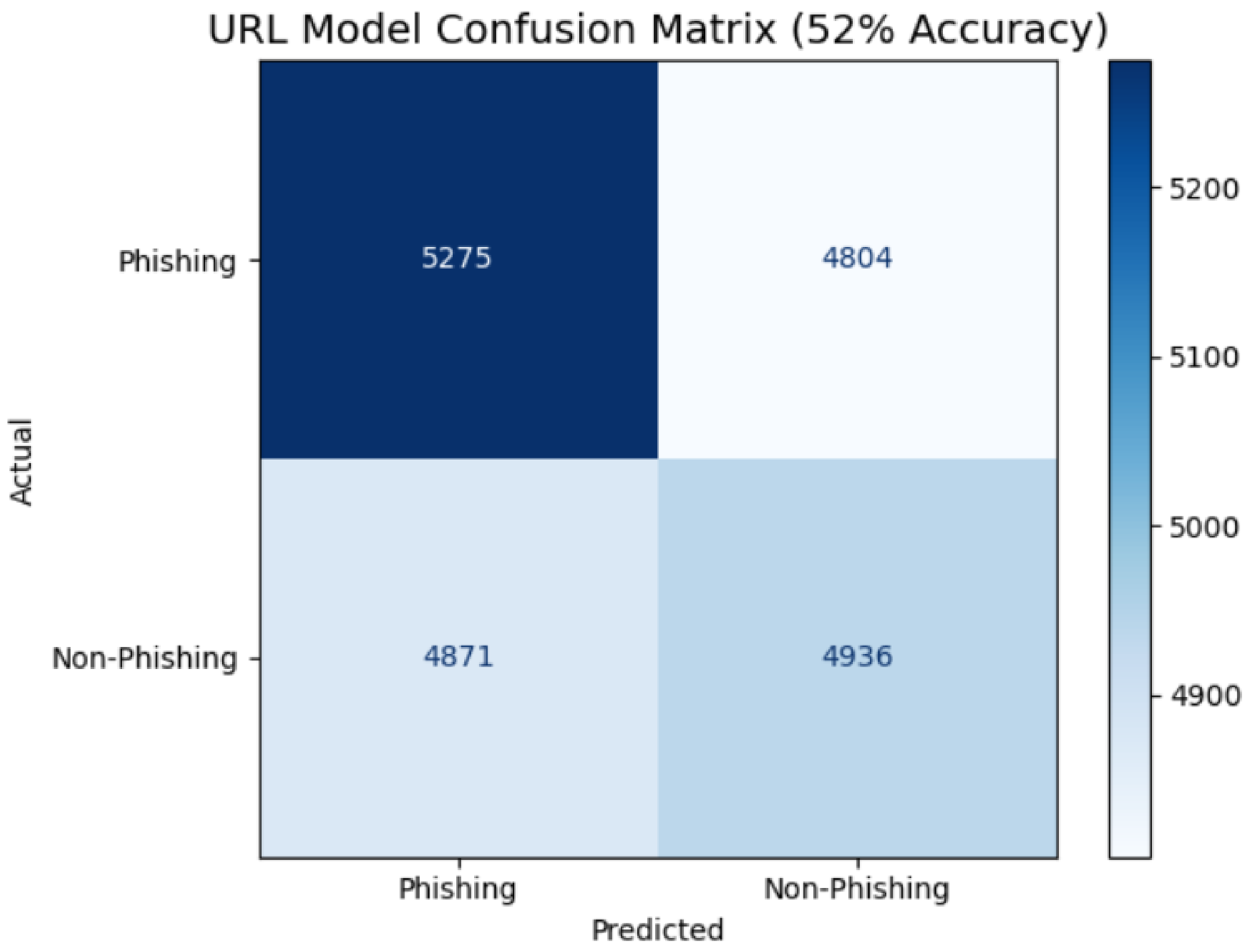
The mail model shows a moderate performance with a clear distinction between true positives and true negatives, but a noticeable number of false positives and false negatives reduces its reliability.

KAIST

Evaluation of Models

Confusion Matrix for URL Model

using Boosting Trees (XGBoost) on CEAS_08 Dataset



URL Model Confusion Matrix (52% Accuracy)

Actual \ Predicted	Phishing	Non-Phishing
Phishing	5275	4804
Non-Phishing	4871	4936

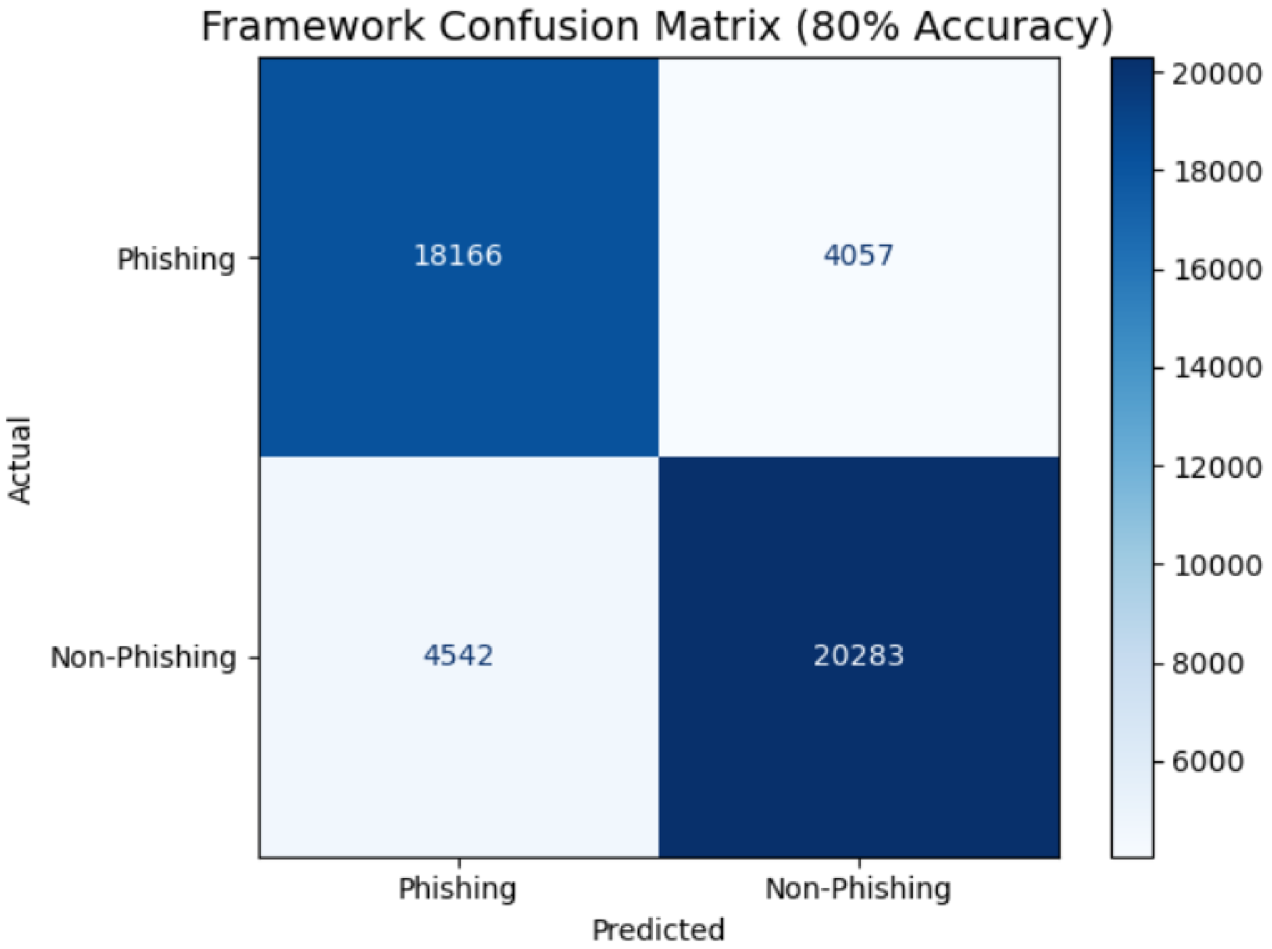
Comment :
Evaluation the URL Model using CEAS_08 gave us an accuracy of 52%.

The URL model exhibits lower accuracy, indicating significant challenges in correctly predicting phishing URLs (feature scrapping issue), with a high count of both false positives and false negatives.

Evaluation of Models

Confusion Matrix for the Double Model Framework

using Boosting Trees (XGBoost) on CEAS_08 Dataset



Comment :
The overall accuracy increased significantly, demonstrating better performance in detecting phishing URLs.

The combined framework demonstrates improved accuracy, effectively reducing false negatives and false positives, showing the benefit of integrating both models.

Overall Technical Challenges

○ *Selection & Data Prep*

❖ Finding the most exploitable dataset

→ enron.csv, phishing_legitimate.csv, CEAS_08.csv

❖ Missing & Mismatched Data

→ Mixing datasets : phishing_legitimate.csv + phishing_urls.csv & Standardization

Technical Challenges

○ *for Mail Model*

❖ Model Training

→ Choosing the Learning Method (Logistic Regression, Boosting Trees, Random Forest)

❖ Over / Underfitting Issues

→ Adjusting Hyperparameters & Optimizing Learning Curves

Technical Challenges

○ *for URL Model*

❖ URLs and features extraction

→ Variety of URL formats (http, https, IPs, ...)
→ Adapting the Extraction Function

❖ Model Training

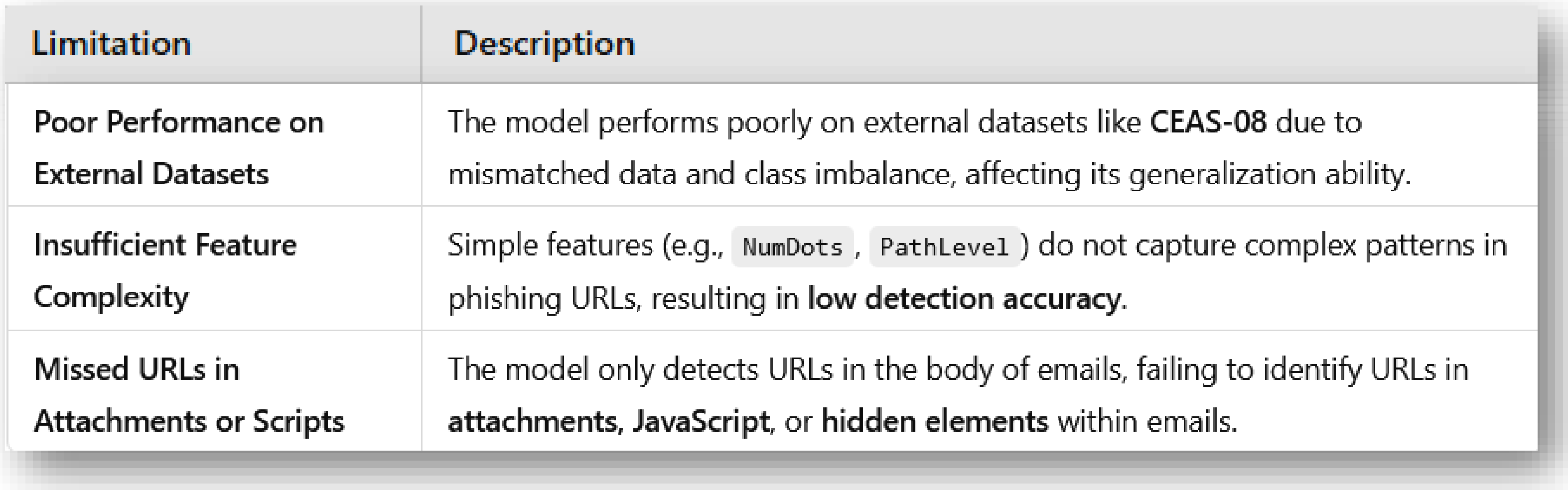
→ Choosing the Learning Method (Logistic Regression, Boosting Trees, Random Forest)

❖ Datasets

→ Lack of diversity in the dataset for the training
→ Limited features exploitability

Limitations of our Methodology

- *Dependency on standard installations & real-world Variances*

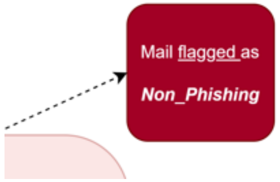


Limitation	Description
Poor Performance on External Datasets	The model performs poorly on external datasets like **CEAS-08** due to mismatched data and class imbalance, affecting its generalization ability.
Insufficient Feature Complexity	Simple features (e.g., `NumDots`, `PathLevel`) do not capture complex patterns in phishing URLs, resulting in **low detection accuracy**.
Missed URLs in Attachments or Scripts	The model only detects URLs in the body of emails, failing to identify URLs in **attachments, JavaScript**, or **hidden elements** within emails.

Future Work

- **Fine Tune Double-Evaluation Models**

  → Extend Research to Non-Phishing Flagged Mail
  → Enhance Models accuracy
  → Detection of Phishing Emails with Images URLs and Tracking artifacts



- **Browser Automation Kit**

  → Usage of a Web Driver Tool Kit like Selenium could be effective to scrap URL content
  → Result **-> More Features could be exploited for Model Training**

- **Integration with Dooray API**

  → Do real-time phishing detection

Conclusion

- **Research on Mailing Protocols**
  → DMARC, DKIM, SPF, SMTP

- **Analyzed Dooray's Security Mechanism**
  → Zphisher & Several Mailboxes

- **Tool Framework**
  → ML-based Phishing Detection Tools
  → Evaluation on public Dataset (CEAS_08.csv)

THANK
YOU!

Discussion