PHISHING DETECTION & AWARENESS REPORT

Prepared by : **Aditya Mehta**

CIN ID: **FIT/JAN26/CS5511**

Date : **16 February 2026**

1. Introduction :

- Phishing is a type of cyber attack where attackers impersonate trusted entities to trick users into providing sensitive information such as login credentials, banking details or personal data. These attacks are commonly performed through fraudulent emails, messages or websites.
- Phishing is a type of cyber attack where attackers impersonate trusted entities to trick users into providing sensitive information such as login credentials, banking details or personal data. These attacks are commonly performed through fraudulent emails, messages or websites.

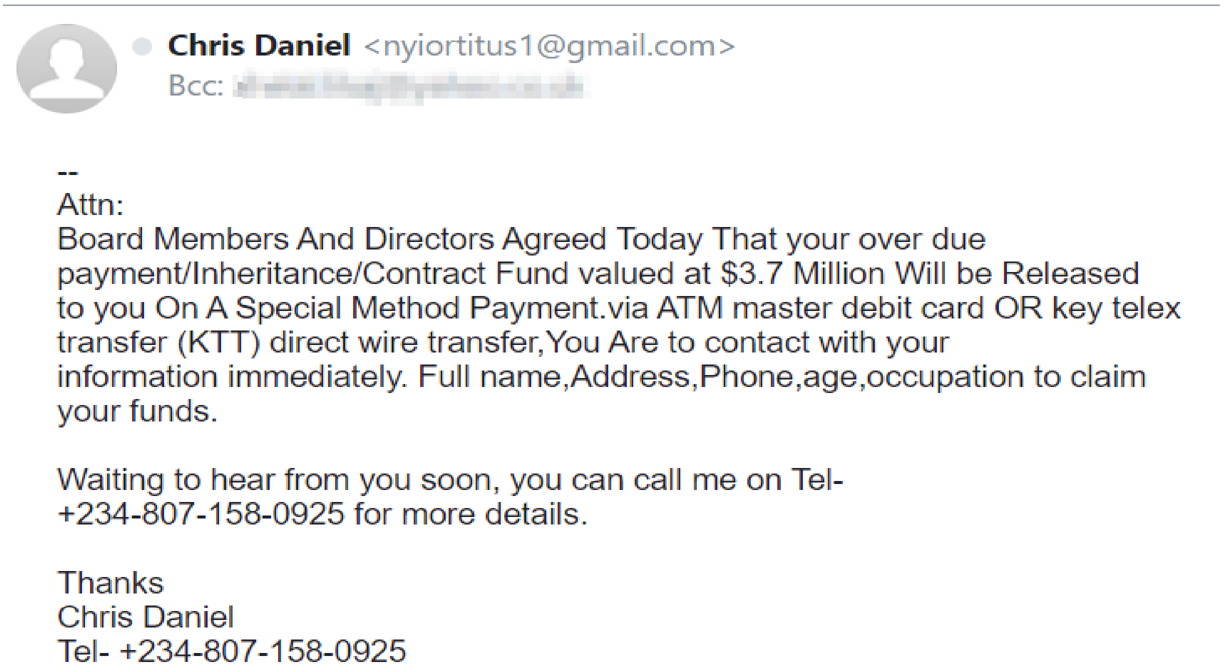
2. Objectives :

- To analyze phishing email samples.
- To analyze phishing email samples.
- To identify phishing indicators.
- To perform email header analysis.
- To classify phishing risk level.
- To recommend prevention techniques.
- To contribute towards society.

3. Tool Used :

Tool Name	Purpose
MXToolbox	Email Header Analysis
Gmail Web Client	Extract Email Header
GitHub	Repository Management
MS Word	Documentation

4. Phishing Email Sample Analysis :



Chris Daniel <nyiortitus1@gmail.com>
Bcc: [redacted]

--
Attn:
Board Members And Directors Agreed Today That your over due payment/Inheritance/Contract Fund valued at $3.7 Million Will be Released to you On A Special Method Payment.via ATM master debit card OR key telex transfer (KTT) direct wire transfer,You Are to contact with your information immediately. Full name,Address,Phone,age,occupation to claim your funds.

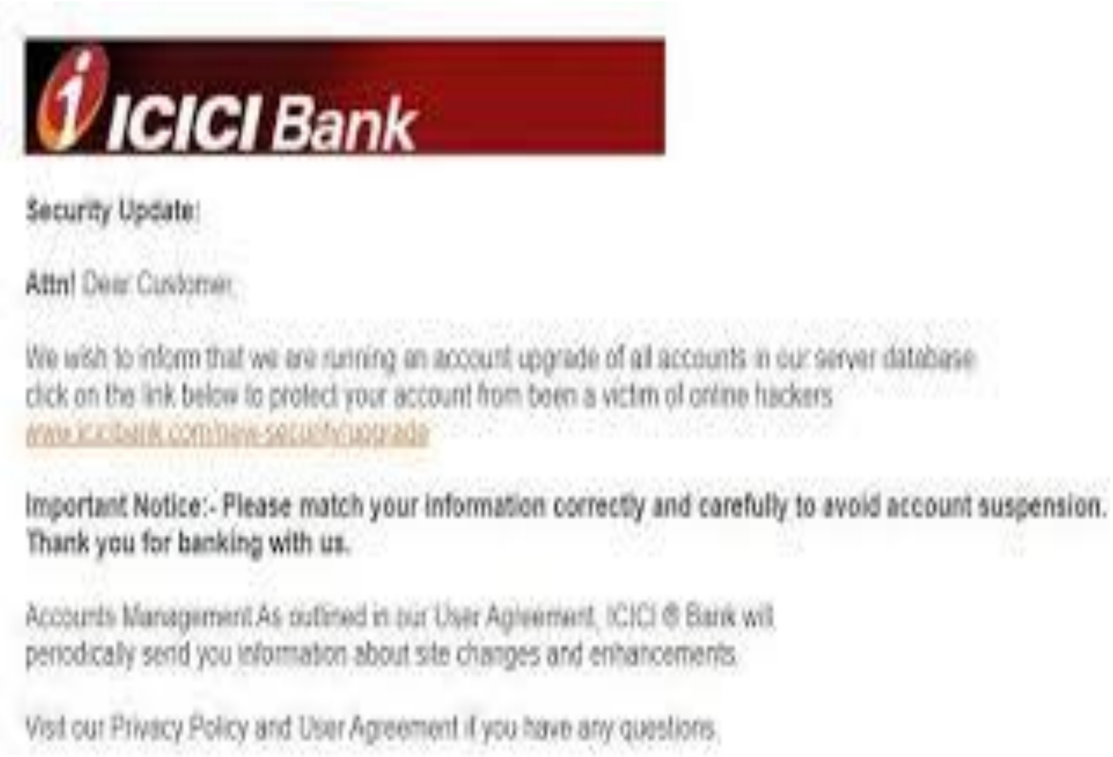
Waiting to hear from you soon, you can call me on Tel- +234-807-158-0925 for more details.

Thanks
Chris Daniel
Tel- +234-807-158-0925

— Indicators Found :

- Suspicious sender email address.
- Urgent request for personal information.
- Use of financial bait ($3.7 Million).
- Grammatical mistakes.
- Unknown contact number.
- No official organization mentioned.

5. Email Sample 2 (Fake ICICI Security Update) :



ICICI Bank

Security Update!

Attn! Dear Customer

We wish to inform that we are running an account upgrade of all accounts in our server database
click on the link below to protect your account from been a victim of online hackers
www.icicibank.com/new-security/upgrade

**Important Notice:- Please match your information correctly and carefully to avoid account suspension.
Thank you for banking with us.**

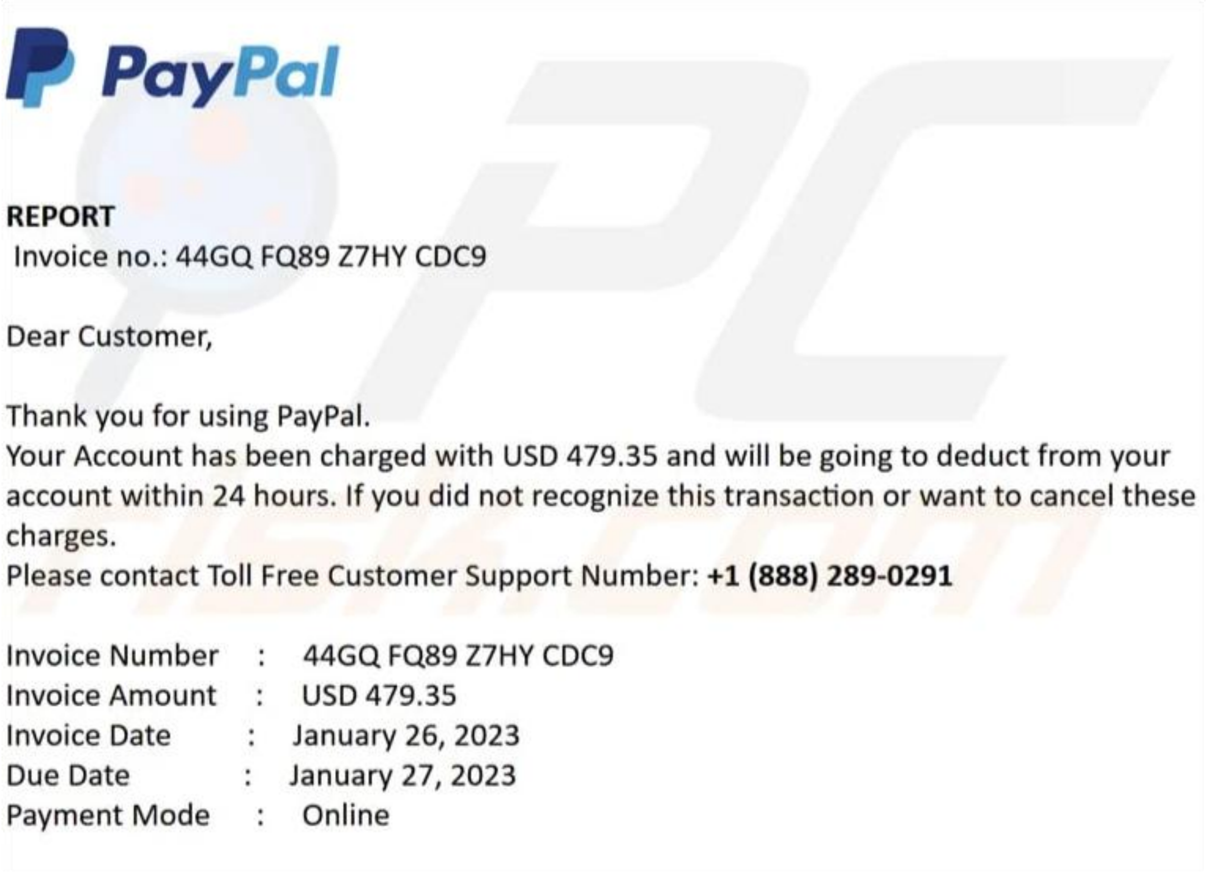
Accounts Management As outlined in our User Agreement, ICICI ® Bank will
periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.

— Indicators Found :

- Generic greeting (Dear Customer).
- Fake urgency.
- Suspicious hyperlink.
- Mismatch between sender and domain.
- Threat of account suspension.

6. Email Sample 3 (Fake Paypal Invoice) :



PayPal

REPORT
Invoice no.: 44GQ FQ89 Z7HY CDC9

Dear Customer,

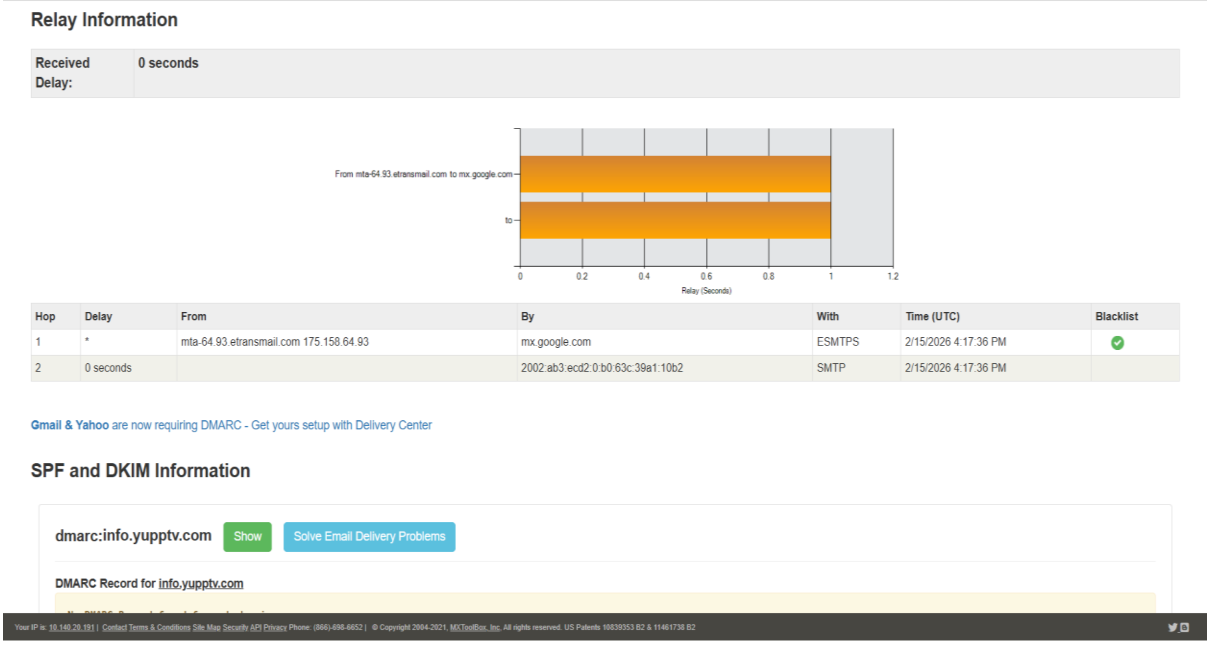
Thank you for using PayPal.
Your Account has been charged with USD 479.35 and will be going to deduct from your account within 24 hours. If you did not recognize this transaction or want to cancel these charges.
Please contact Toll Free Customer Support Number: **+1 (888) 289-0291**

Invoice Number	:	44GQ FQ89 Z7HY CDC9
Invoice Amount	:	USD 479.35
Invoice Date	:	January 26, 2023
Due Date	:	January 27, 2023
Payment Mode	:	Online

— Indicators Found :

- Fake transaction alert.
- Unknown invoice number.
- Suspicious toll-free number.
- Urgency to cancel transaction.
- No official paypal domain used.

7. Email Header Analysis :



Relay Information

Received Delay:	0 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mta-64.93.etransmail.com 175.158.64.93	mx.google.com	ESMTPS	2/15/2026 4:17:36 PM	✓
2	0 seconds		2002:ab3:ecd2:0:b0:63c:39a1:10b2	SMTP	2/15/2026 4:17:36 PM	

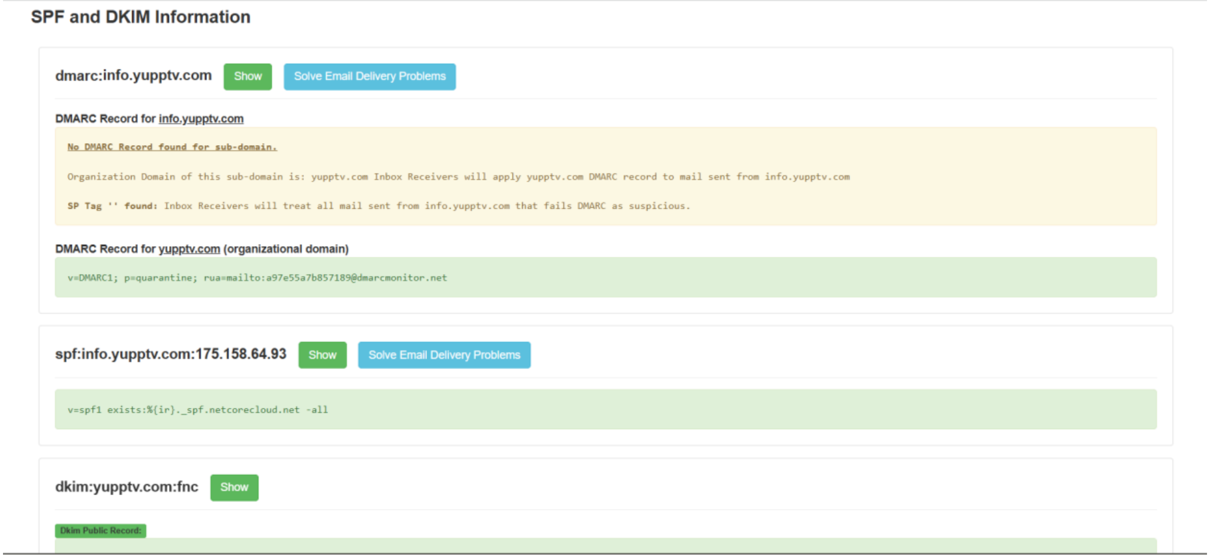
Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

dmarc:info.yupptv.com Show Solve Email Delivery Problems

DMARC Record for info.yupptv.com

Your IP is: 10.140.20.191 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2



SPF and DKIM Information

dmarc:info.yupptv.com Show Solve Email Delivery Problems

DMARC Record for info.yupptv.com

```
No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: yupptv.com Inbox Receivers will apply yupptv.com DMARC record to mail sent from info.yupptv.com

SP Tag '' found: Inbox Receivers will treat all mail sent from info.yupptv.com that fails DMARC as suspicious.
```

DMARC Record for yupptv.com (organizational domain)

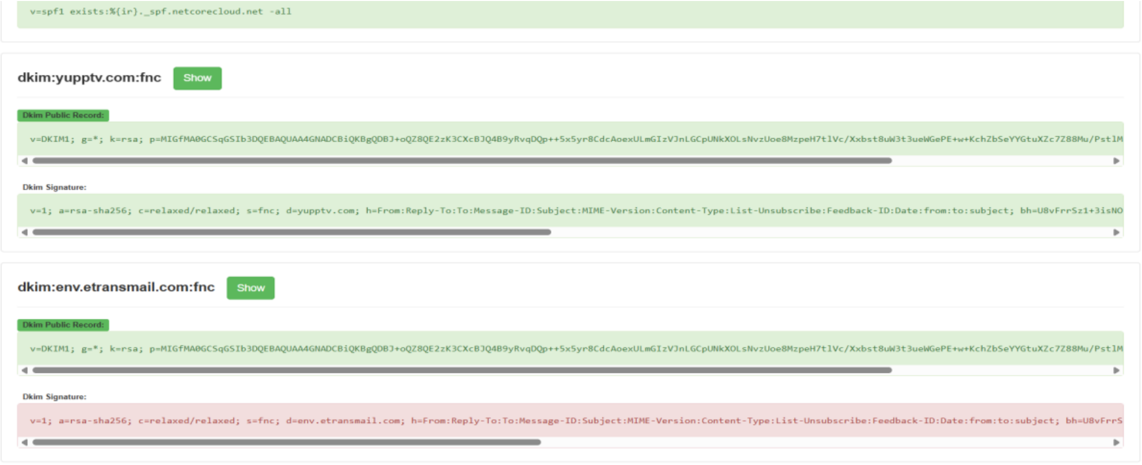
```
v=DMARC1; p=quarantine; rua=mailto:a97e55a7b857189@dmarcmonitor.net
```

spf:info.yupptv.com:175.158.64.93 Show Solve Email Delivery Problems

```
v=spf1 exists:%{ir}._spf.netcorecloud.net -all
```

dkim:yupptv.com:fnc Show

Dkim Public Record:



```
v=spf1 exists:%{ir}._spf.netcorecloud.net -all
```

dkim:yupptv.com:fnc Show

Dkim Public Record:

```
v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDBJ+oQZ8QE2zK3CXcBJQ4B9yRvqDQp++5x5yr8CdcAoexULmGIzVJnLGCpUNkXOLsNvzUoe8MzpeH7tlVc/Xxbst8uW3t3ueWGePE+w+KchZbSeYYGtuXZc7Z88Mu/PstlM
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; s=fnc; d=yupptv.com; h=From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe:Feedback-ID:Date:from:to:subject; bh=U8vFrrSz1+3isNO
```

dkim:env.etransmail.com:fnc Show

Dkim Public Record:

```
v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDBJ+oQZ8QE2zK3CXcBJQ4B9yRvqDQp++5x5yr8CdcAoexULmGIzVJnLGCpUNkXOLsNvzUoe8MzpeH7tlVc/Xxbst8uW3t3ueWGePE+w+KchZbSeYYGtuXZc7Z88Mu/PstlM
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; s=fnc; d=env.etransmail.com; h=From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe:Feedback-ID:Date:from:to:subject; bh=U8vFrrS
```

- The email header was analyzed using MXToolbox.
- The analysis revealed SPF and DKIM authentication failures indicating that the sender domain was not authorized to send emails on behalf of the claimed organization.
- This confirms that the email was spoofed and potentially malicious.

8. Risk Calculation Table :

Indicator	Present (Yes/No)	Risk Score
Suspicious Sender Address	Yes	2
Urgent Language Used	Yes	1
Unknown Hyperlink	Yes	2
Financial Temptation	Yes	2
Grammar Mistakes	Yes	1
Header Authentication Failure	Yes	2
Total Risk Score		**10**

9. Risk Classification :

- Based on the above calculation, the analyzed phishing emails fall under **High Risk Category**.
- Below is the risk classification table is given to classify the risk using risk score range and risk level.

Risk Score Range	**Risk Level**
0 – 3	Low Risk
4 – 6	Medium Risk
7 – 10	High Risk

10. Prevention Guidelines :

- Avoid clicking on unknown links.
- Verify sender email address.
- Check domain authenticity.
- Do not share personal information.
- Enable spam filters.
- Report phishing emails.

11. Conclusion :

- Phishing attacks continue to pose significant threats to individuals and organizations.
- Through this analysis, various phishing indicators and header authentication failures were identified confirming the malicious nature of the emails.
- Proper awareness and technical verification can significantly reduce the risk of phishing attacks.

GITHUB REPOSITORY LINK : **iamadityamehta/FUTURE_CS_02: Showcasing the work of the 2nd task of cybersecurity I've done during the internship at future interns.**