PHISHING EMAIL DETECTION

Click to add text

Samardeep Gurudatta
Data Modelling and Optimization

Mahadevan Iyer
Data Engineering and Extraction

Rohan Shukla
Data Preprocessing, Feature Engineering

Meghana Boinpally
Data Preprocessing, Feature Engineering

The Boston Globe Sign In | SUBSCRIBE

The town of Tewksbury loses $102,000 in email phishing scam

By **Charlie McKenna** Globe Correspondent,
Updated February 23, 2022, 1:35 p.m.

The town of Tewksbury lost more than $100,000 due to a fraudulent wire payment after a town employee fell victim to a phishing scam late last year, officials said.

The employee received an email in late December from a regular vendor inquiring about invoices and asking for payment to be

Cloning

THE VERGE

TECH SCIENCE MORE

POLICY TECH CYBERSECURITY

$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users

Two hundred and fifty-four tokens were stolen over roughly three hours

Russell Brandom | Feb 20, 2022, 9:37am EST

SHARE

Spear Phishing

Tewksbury loses $102,000 to phishing scam

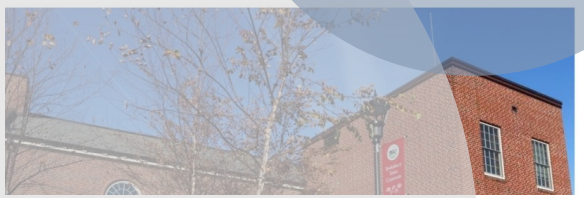
a Lavery

BLISHED: February 23, 2022 at 12:50 p.m. |

DATED: February 23, 2022 at 6:

ne and Public Safety, Latest Headlines, Local

vs, News



Attacks/Breaches 5 MIN READ ARTICLE

More Orgs Suffered Successful Phishing Attacks in 2021 Than in 2020

Threat actors maintained their relentless attacks on enterprise end users for yet another year, new study shows.

February 22, 2022

Jai Vijayan

17 FEB 2022 NEWS

Phishing Top Threat to US Healthcare

Sarah Coble

Home › News ›

Report: Phishing Attacks Grew 28% Across 2021

In December 2021, enterprises averaged around 68 attacks per month on social media alone.

Adam Rowe

February 23rd 2022 | 9:32 am

Email Phishing

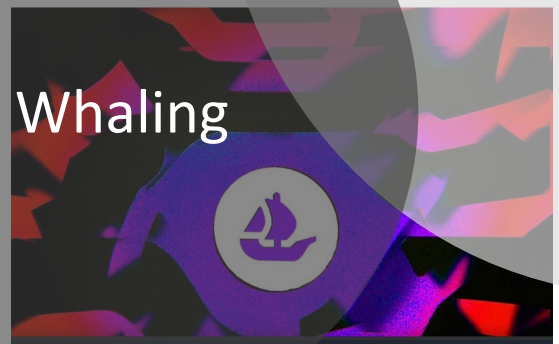
WCNC CHARLOTTE

58°

Charlotte, NC »

Scam Alert: Phishing techniques impacting taxpayers this tax season

Whaling



PHISHERDANT

DATA COLLECTION

Enron corpus

Nazario corpus

Parsed it to csv

Few Shot Learning

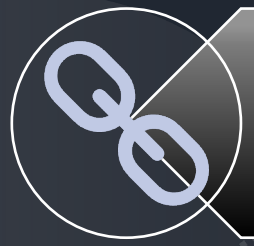
PHISHERDANT

DATA WRANGLING

- Identified and Restructured metadata
- Text Cleaning
- Text Mapping and Generalization
- Handled Class Imbalance

PHISHERDANT

We protect the end user from



Malicious URLs

Link and Domain analysis

Business Email Compromise

Content analysis

Brand Imposters

Meta data analysis

PHISHERDANT

DOMAIN ANALYSIS

FRAUDULENT DOMAIN

FROM: **no-reply@ebuy.com**

Links:
- http://pages.ebay.com
- https://sign-in.eby.com

MALICIOUS URL

FROM: **w-confirm@ebay.com**

Links:
- https://images.ebay.com
- http://251.120.83.1
- http://login-member.rcmail.eu

WHITELISTING URLS

FROM: **sender**@domain.com

Links:
- **https://mobile.msn.com**
- **http://teams.microsoft.com**

FROM: sender@domain.com

Links:
- **https://microsoft.jindo.com**

PHISHERDANT

CONTENT ANALYSIS

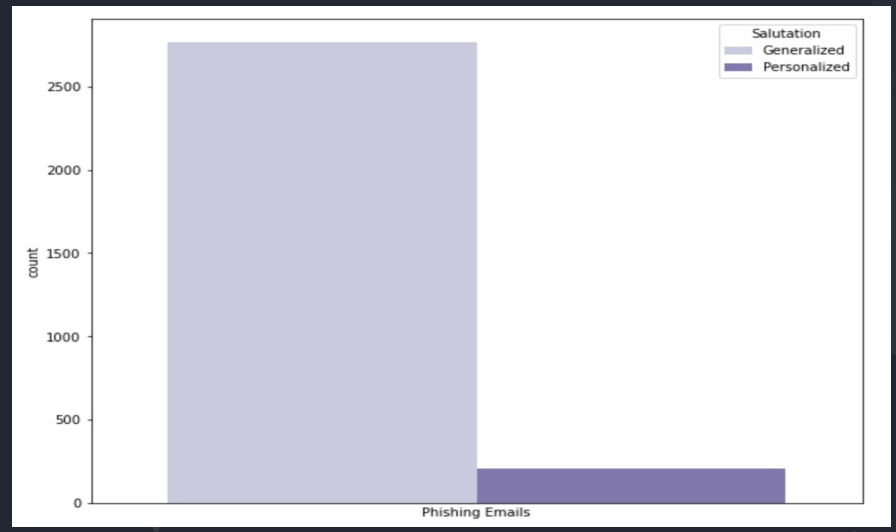
From BM paypl.secure.org

[EXT] Immediate Action: Account locked due to suspicious activity.

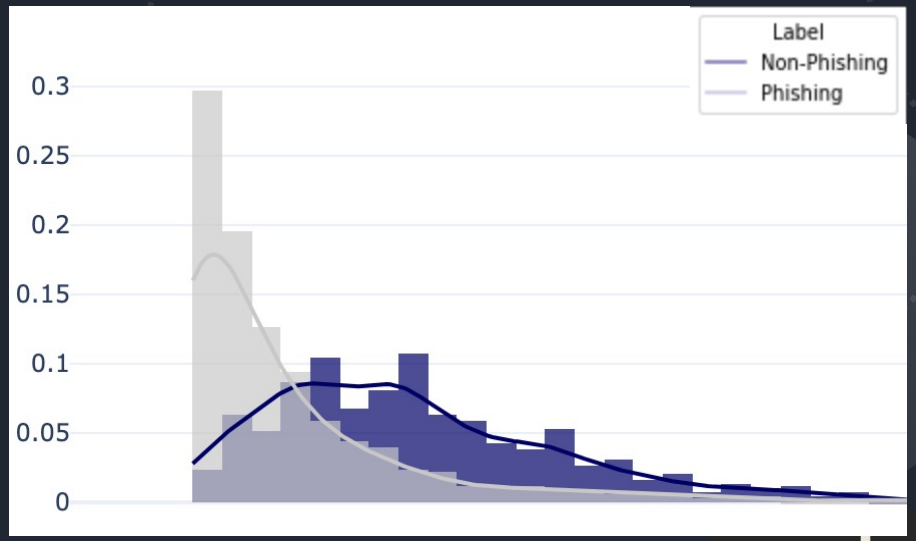
Dear Valued Customer.
We have received notice that you have recently attempted to withdraw the following amount, from your paypal account, while in another country : $500. As a safety measure, please visit our website via the link below to verify and update your personal information. Click here
www.paypal.com/account/security
www.paypal.com/log
Cmd+Click to follow link
http://www.paypl.com/

Thanks.
Paypal Team

Generalized Salutation



Call For Action



METADATA ANALYSIS

From BM paypl.secure.org

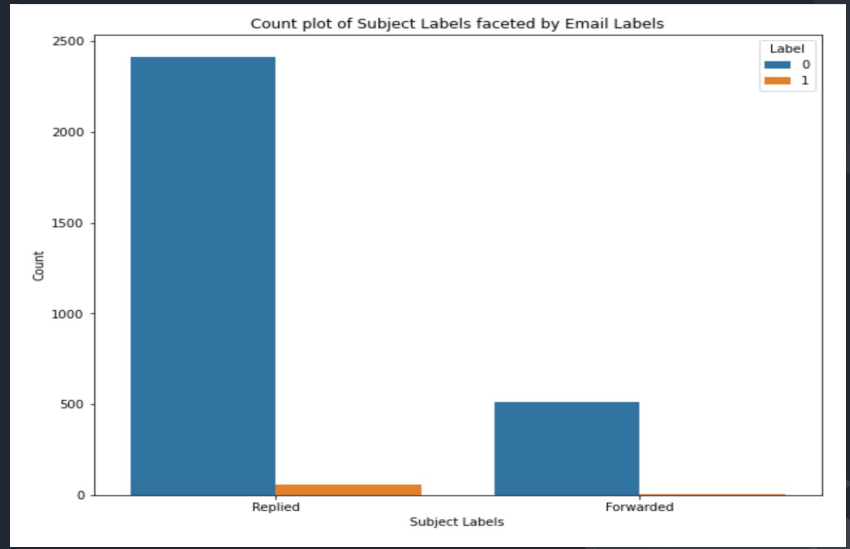
[EXT] Immediate Action: Account locked due to suspicious activity.

Dear Valued Customer.
We have received notice that you have recently attempted to withdraw the following amount, from your paypal account, while in another country : $500. As a safety measure, please visit our website via the link below to verify and update your personal information. Click here
www.paypal.com/account/security
www.paypal.com/loc
Cmd+Click to follow link
http://www.paypl.com/

Thanks.
Paypal Team

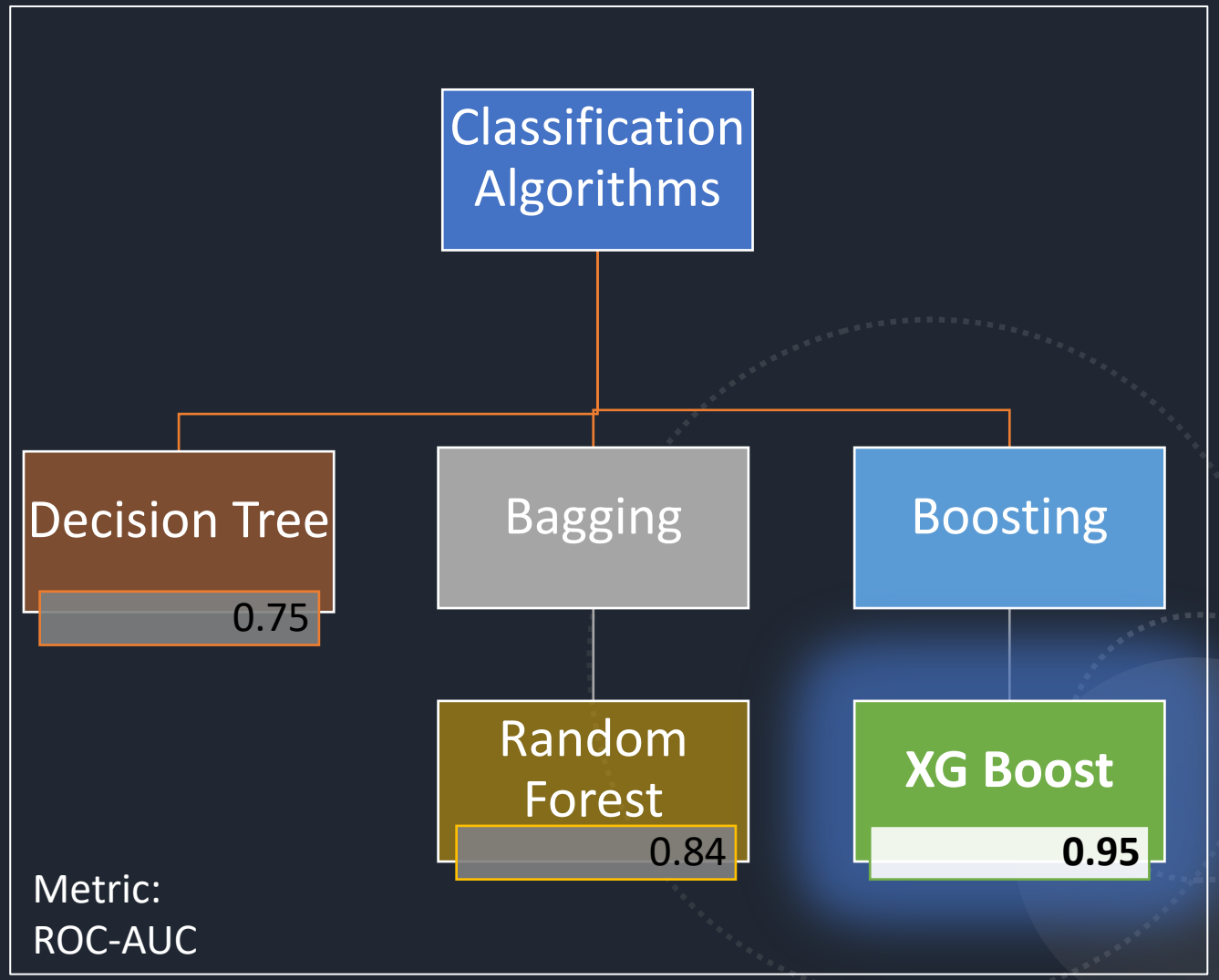
Email Subject Abbreviations

Subject Urgency



PHISHERDANT

ALGORITHMS IMPLEMENTED



PHISHERDANT

FUTURE SCOPE

- Learn and update the best predictor for future data at every step using Online learning
- Expanding the scope against phishing attacks to include social media and instant messaging
- Customizable filter rules so that administrators can define their own policies for blocking
  - Spam Emails
  - Bulk Campaigns
  - Unsolicited Marketing materials

THANK YOU

PHISHERDANT