Phishing – Attack, Detection and Prevention

Presenters : **Bharath Srinivasan, Karthi Balasundaram, Mukilan A.R.**
Advisor : **Dr. Phu H. Phung**, Department of Computer Science

University of Dayton

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account bh*****@gmail.com.

Sign-in details

Country/region: Turkey

IP address: 88.241.50.170

Date: 3/16/2019 2:49 PM (IST)

Platform: Windows

Browser: Chrome

Please go to your recent activity page to let us know whether or not this was you. If this wasn't you, we'll help you secure your account. If this was you, we'll trust similar activity in the future.

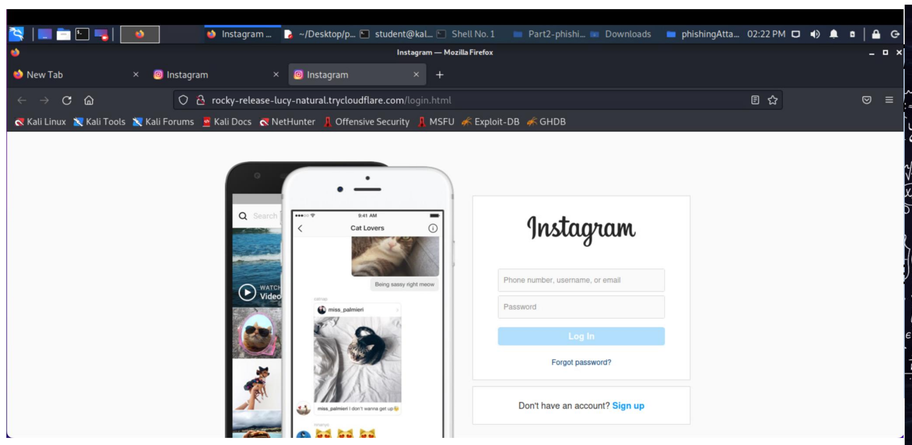
OBJECTIVE

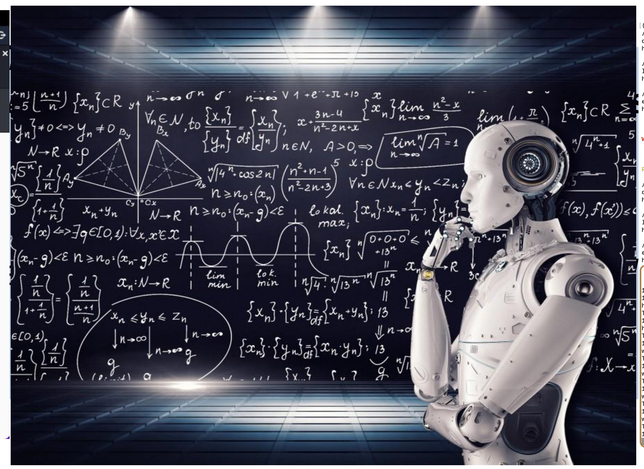
- To understand Phishing and Social Engineering.
- Email Phishing and how the hacker tricks the victim.
- Implement Phishing attack on a system.
- Machine Learning techniques on how to detect malicious URLs.
- Techniques on how to prevent Phishing attacks.
- To create awareness among common netizens.

Dear AWS Customer,

We believe that someone obtained your account and/or financial information elsewhere and used it to access your Amazon Web Services (AWS) account. If the activity was authorized, please let us know by following Step 3, below. Your account will remain open for five (5) days, so you can follow the steps below to secure your account. Failure to contact AWS within five (5) days may result in the suspension of your account and disruption of your AWS service in order to protect you from unauthorized usage and charges.

Although it appears someone did access your AWS account, they would not have been able to view your full credit card number since they are never displayed on our site. However, it is possible your credit card information may have been compromised at the time your other personal information was obtained. We suggest you carefully review recent credit card statements to check for any unusual activity or unauthorized charges.





```
(base) karthibalasundaram@Karthis-MacBook-Pro htmlWeb % python3 phishing.py
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator CountVectorizer from version 0.24.2 when using version 1.1.1. This might lea
d to breaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator LogisticRegression from version 0.24.2 when using version 1.1.1. This might
lead to breaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator Pipeline from version 0.24.2 when using version 1.1.1. This might lead to br
eaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
 * Serving Flask app 'phishing'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://10.64.229.21:5000
Press CTRL+C to quit
 * Restarting with stat
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator CountVectorizer from version 0.24.2 when using version 1.1.1. This might lea
d to breaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator LogisticRegression from version 0.24.2 when using version 1.1.1. This might
lead to breaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
/Users/karthibalasundaram/miniforge3/lib/python3.9/site-packages/sklearn/base.py:329: UserWarning: Trying to unpickle estimator Pipeline from version 0.24.2 when using version 1.1.1. This might lead to br
eaking code or invalid results. Use at your own risk. For more info please refer to:
https://scikit-learn.org/stable/model_persistence.html#security-maintainability-limitations
  warnings.warn(
 * Debugger is active!
 * Debugger PIN: 122-458-698
127.0.0.1 - - [08/Dec/2022 10:53:10] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [08/Dec/2022 10:53:10] "GET /favicon.ico HTTP/1.1" 404 -
https://isidore.udayton.edu/ is given as input by the user
The label predicted is good
127.0.0.1 - - [08/Dec/2022 10:53:28] "POST /predict HTTP/1.1" 200 -
https://isidore.udayton.edu/portal/site/fdc5c7d7-2da6-4ed7-9b1e-02112e64c87d/tool/627164e1-ef67-46d4-930d-a9fe6daccd56 is given as input by the user
The label predicted is bad
127.0.0.1 - - [08/Dec/2022 10:53:39] "POST /predict HTTP/1.1" 200 -
www.paypal.com is given as input by the user
The label predicted is bad
127.0.0.1 - - [08/Dec/2022 10:54:00] "POST /predict HTTP/1.1" 200 -
www.google.com is given as input by the user
The label predicted is good
127.0.0.1 - - [08/Dec/2022 10:54:21] "POST /predict HTTP/1.1" 200 -
www.alibaba.com is given as input by the user
The label predicted is bad
127.0.0.1 - - [08/Dec/2022 10:54:29] "POST /predict HTTP/1.1" 200 -
www.tamilgun.com is given as input by the user
The label predicted is good
127.0.0.1 - - [08/Dec/2022 10:54:47] "POST /predict HTTP/1.1" 200 -
```