SECURITY AUTOMATION

PHISHING DETECTION

The Development of the UISO’s Automated Phishing Detection Bot

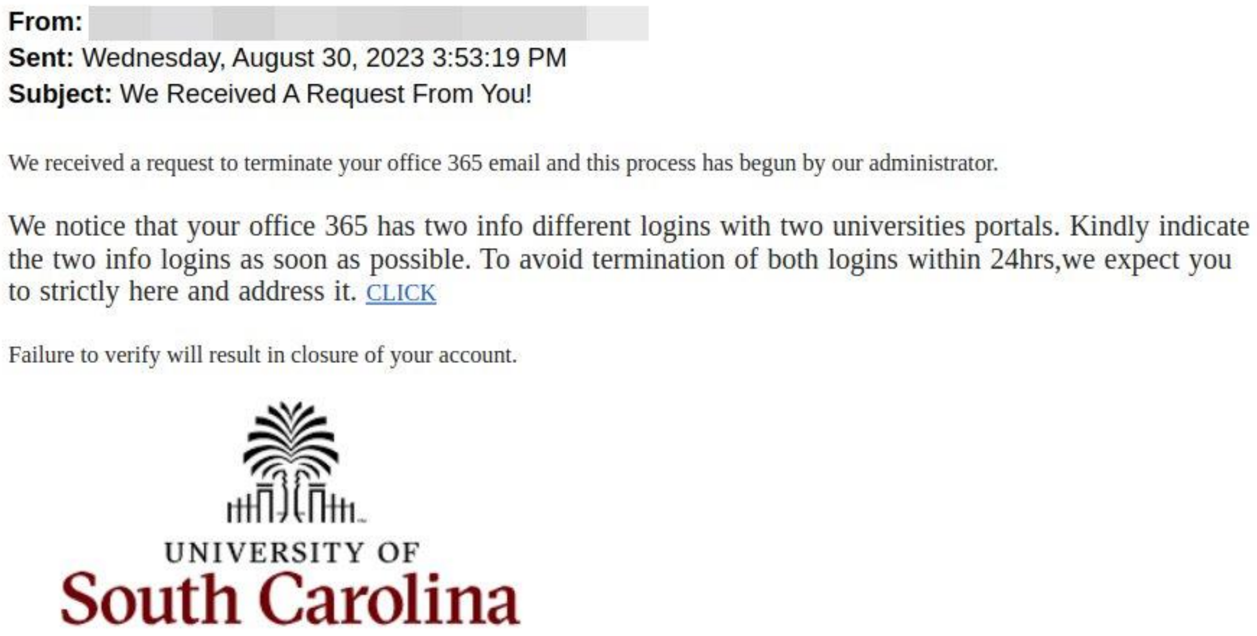
Spring 2025

UNIVERSITY OF
South Carolina

Division of Information Technology

WHAT IS PHISHING?

- A manipulation tactic used to gain sensitive information from users
- Commonly seen in:
  - Emails
  - Text messages
  - Phone calls
  - QR Codes



From: [redacted]
Sent: Wednesday, August 30, 2023 3:53:19 PM
Subject: We Received A Request From You!

We received a request to terminate your office 365 email and this process has begun by our administrator.

We notice that your office 365 has two info different logins with two universities portals. Kindly indicate the two info logins as soon as possible. To avoid termination of both logins within 24hrs,we expect you to strictly here and address it. CLICK

Failure to verify will result in closure of your account.

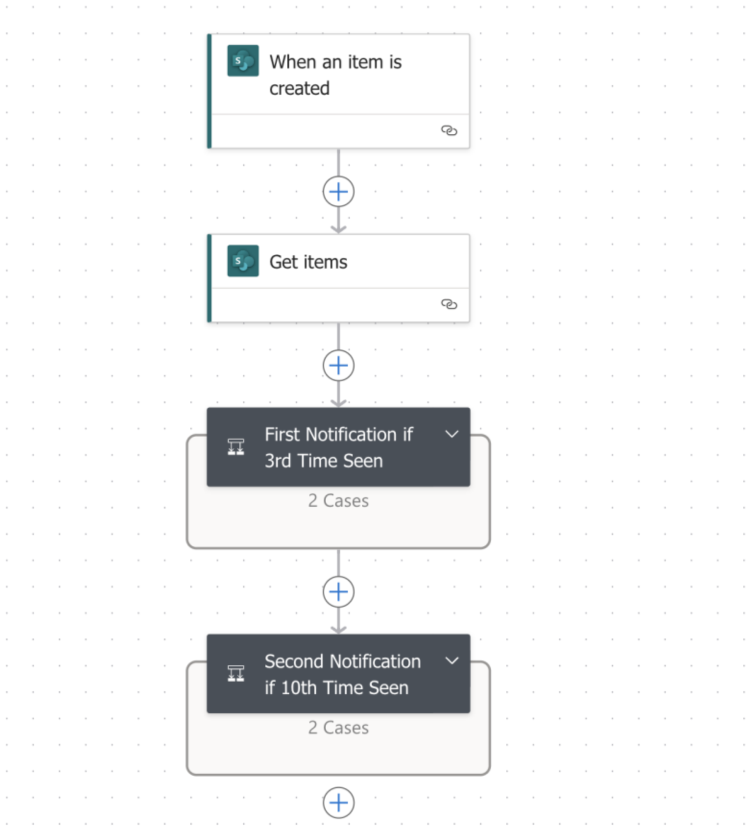
UNIVERSITY OF
South Carolina

HOW DOES THE UISO HANDLE PHISHING?

THE OLD PROCESS

- *phishing@mailbox.sc.edu*
  - Phishing reports were forwarded to this inbox
  - Emails reported through “report as phishing” were unchecked
  - Unmonitored
- Basic automation
  - Filtering based on subject line
  - Most information was found manually

POWER AUTOMATE



When an item is created

Get items

First Notification if 3rd Time Seen

2 Cases

Second Notification if 10th Time Seen

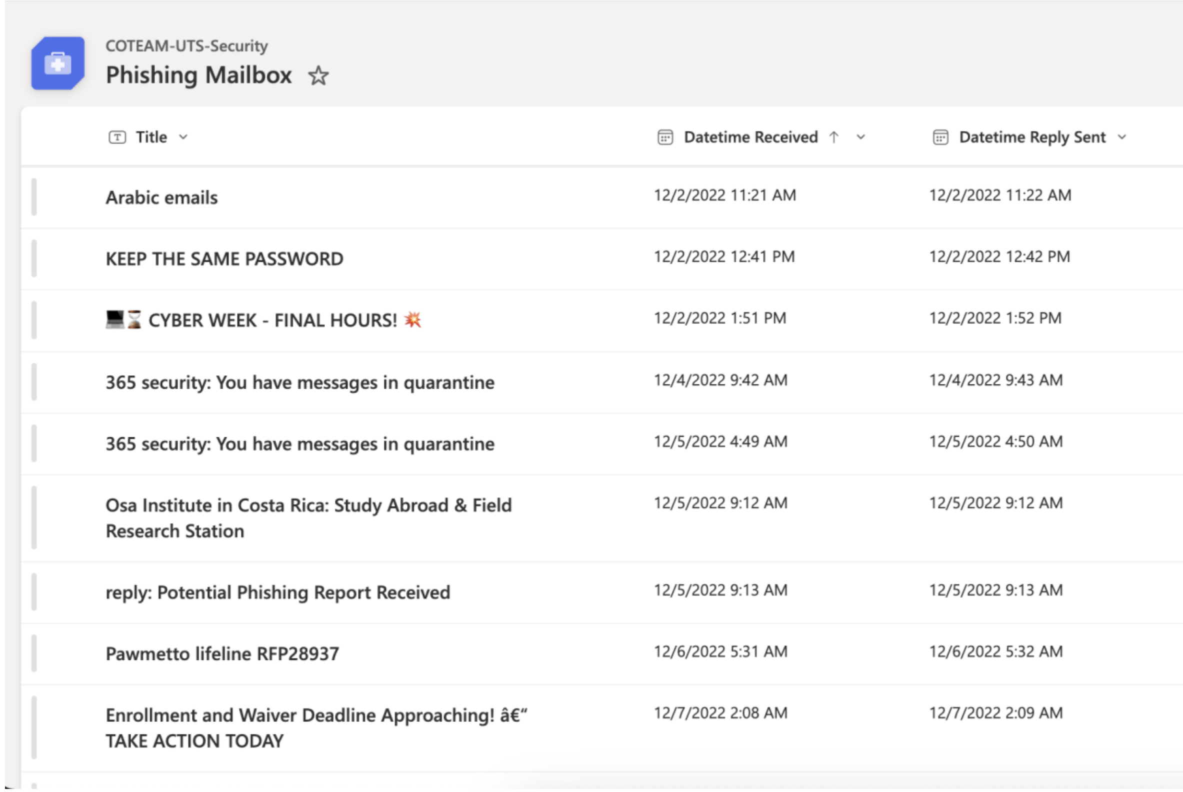
2 Cases

- "Low code" automation solution
- Easy M365 integrations
- Included in current M365 license
  - No extra cost

GETTING STARTED

- Re-organized phishing mailbox
- Started to include emails logged by Defender for Endpoint
- New automated flow
  - Rebuilt from previous iteration

PHISHING BOT 2.0

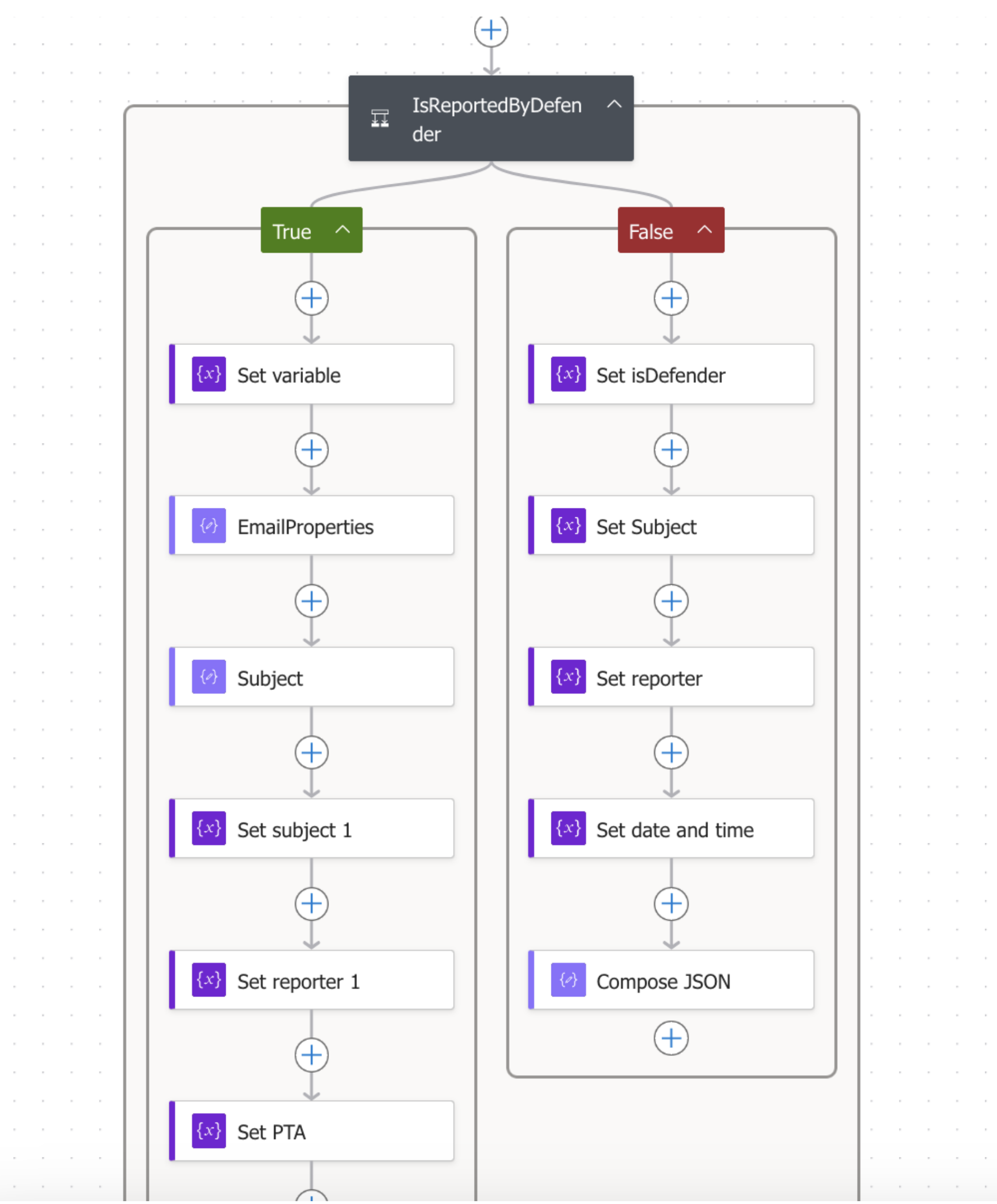


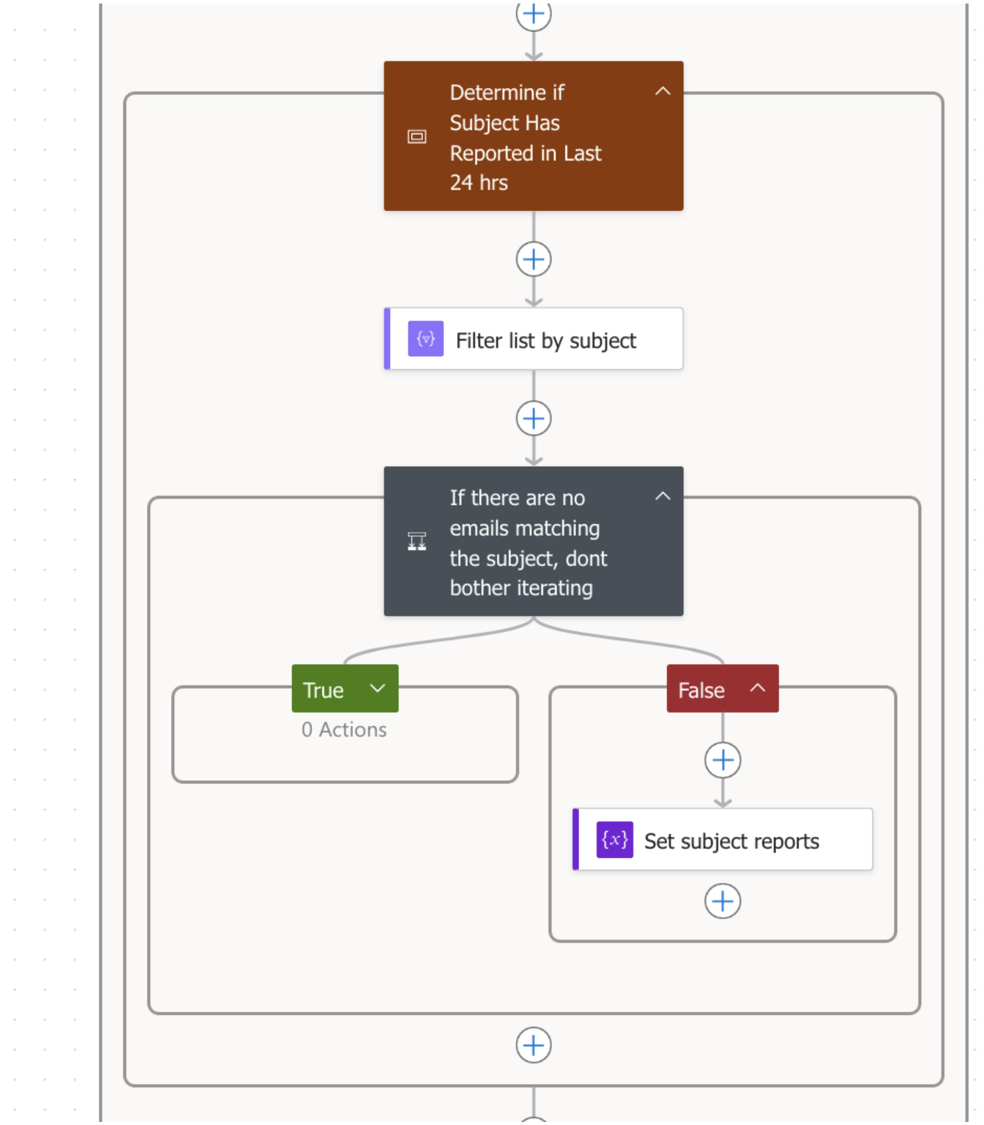
COTEAM-UTS-Security

Phishing Mailbox ☆

Title	Datetime Received ↑	Datetime Reply Sent
Arabic emails	12/2/2022 11:21 AM	12/2/2022 11:22 AM
KEEP THE SAME PASSWORD	12/2/2022 12:41 PM	12/2/2022 12:42 PM
💻⌛ CYBER WEEK - FINAL HOURS! 💥	12/2/2022 1:51 PM	12/2/2022 1:52 PM
365 security: You have messages in quarantine	12/4/2022 9:42 AM	12/4/2022 9:43 AM
365 security: You have messages in quarantine	12/5/2022 4:49 AM	12/5/2022 4:50 AM
Osa Institute in Costa Rica: Study Abroad & Field Research Station	12/5/2022 9:12 AM	12/5/2022 9:12 AM
reply: Potential Phishing Report Received	12/5/2022 9:13 AM	12/5/2022 9:13 AM
Pawmetto lifeline RFP28937	12/6/2022 5:31 AM	12/6/2022 5:32 AM
Enrollment and Waiver Deadline Approaching! â€“ TAKE ACTION TODAY	12/7/2022 2:08 AM	12/7/2022 2:09 AM

- Simple flow in Power Automate
- Processed an email every time one came in
- Stored report data in a Microsoft SharePoint list
- Current email was compared to the list
- If reported too many times, a Teams message is sent to SOC analysts


IsReportedByDefender
True
False
Set variable
EmailProperties
Subject
Set subject 1
Set reporter 1
Set PTA
Set isDefender
Set Subject
Set reporter
Set date and time
Compose JSON


Determine if Subject Has Reported in Last 24 hrs
Filter list by subject
If there are no emails matching the subject, dont bother iterating
True
0 Actions
False
Set subject reports

Accomplishments

- Visibility
- More information available to analysts
- Significantly improved response time

Challenges

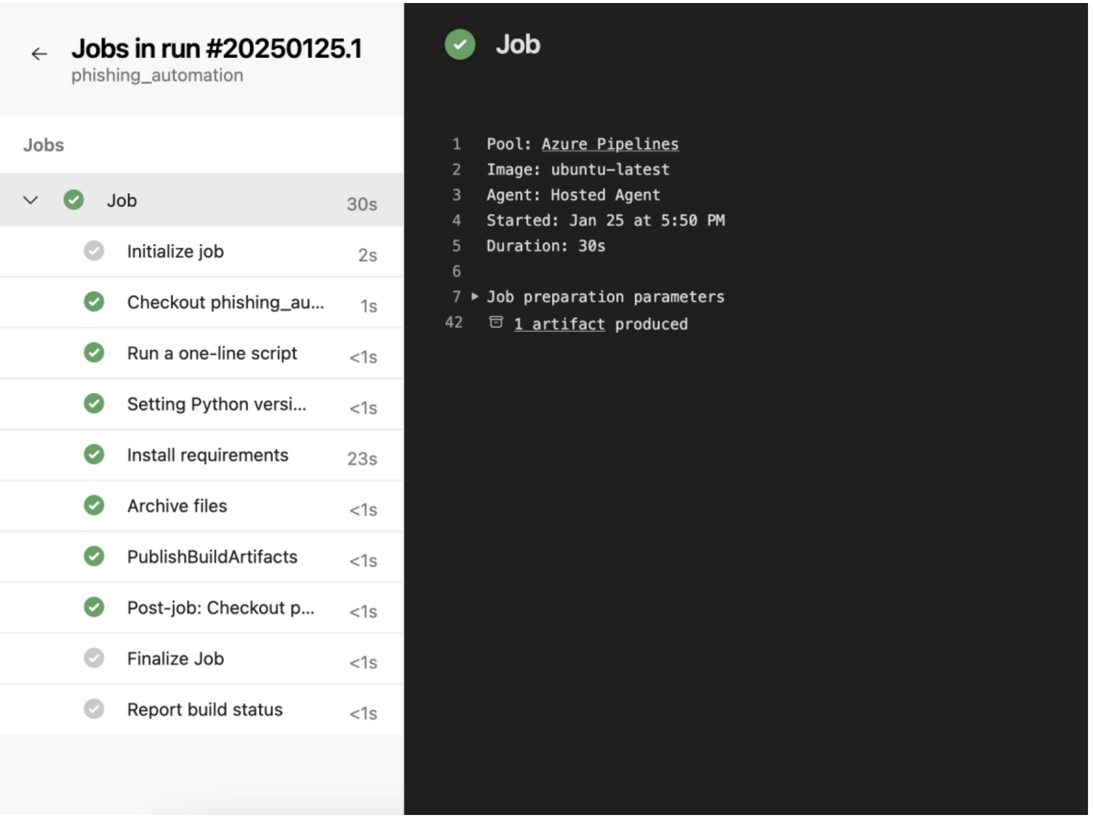
- One email at a time
- Only reported on email count
- Defender vs Manual reports
- Power Automate limitations
- Inaccurately high report volume

CURRENT ITERATION: PHISHING BOT 3.0

- Power Automate front end
  - Takes parsed data and sends it to Teams
- Python backend
  - Parses email data
  - Sends to our in-house workflow tool
- Azure Architecture
  - Storage
  - Serverless Compute (Lambda)
  - DevOps

CI/CD PIPELINE

- Continuous Integration/Continuous Delivery
- Permission Management
- Automated tests



← **Jobs in run #20250125.1**
phishing_automation

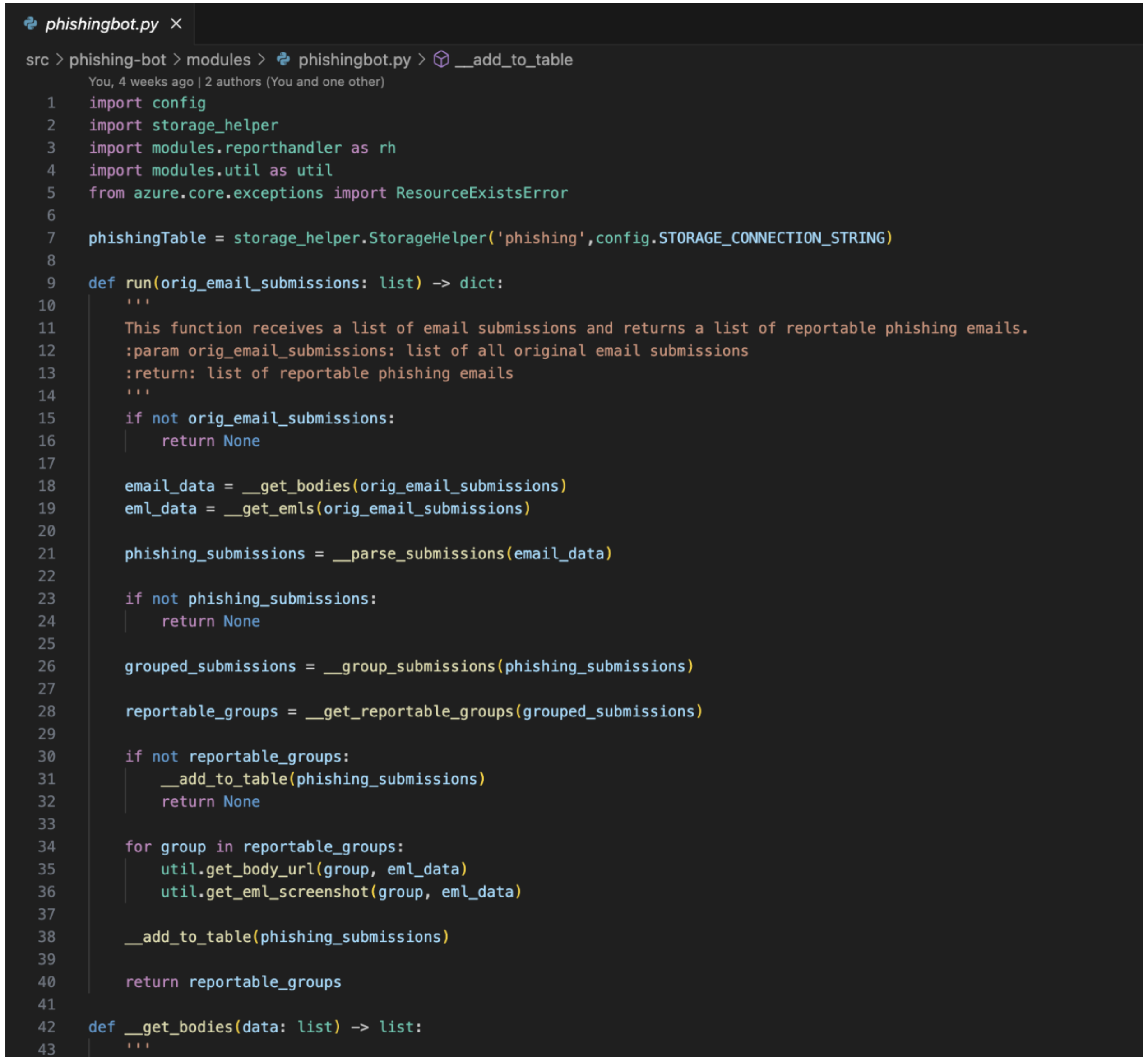
Jobs

✓ Job	30s
Initialize job	2s
✓ Checkout phishing_au...	1s
✓ Run a one-line script	<1s
✓ Setting Python versi...	<1s
✓ Install requirements	23s
✓ Archive files	<1s
✓ PublishBuildArtifacts	<1s
✓ Post-job: Checkout p...	<1s
Finalize Job	<1s
Report build status	<1s

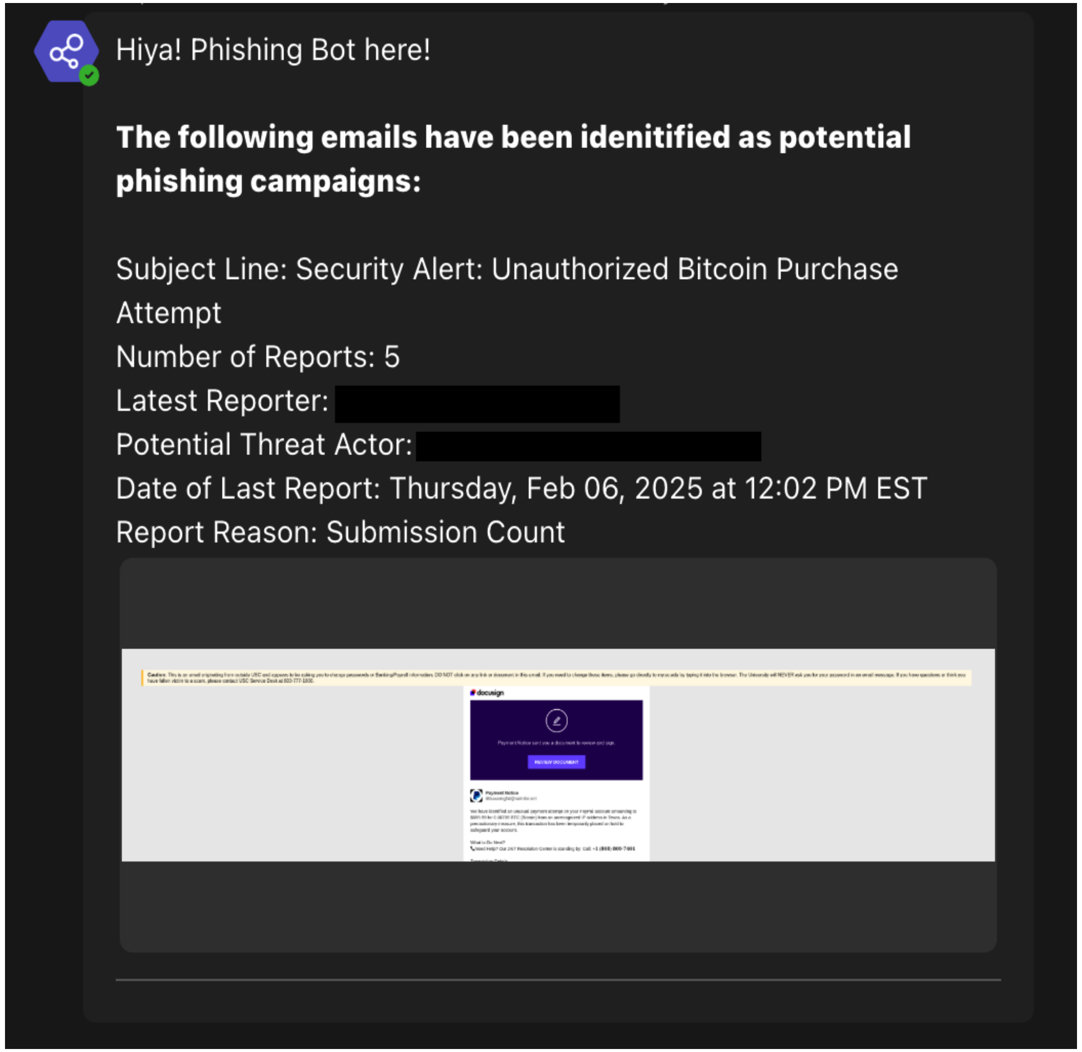
✓ **Job**

```
Pool: Azure Pipelines
Image: ubuntu-latest
Agent: Hosted Agent
Started: Jan 25 at 5:50 PM
Duration: 30s

▸ Job preparation parameters
  1 artifact produced
```

Information Technology
UNIVERSITY OF SOUTH CAROLINA


phishingbot.py ×
src > phishing-bot > modules > phishingbot.py > __add_to_table
You, 4 weeks ago | 2 authors (You and one other)

```python
import config
import storage_helper
import modules.reporthandler as rh
import modules.util as util
from azure.core.exceptions import ResourceExistsError

phishingTable = storage_helper.StorageHelper('phishing',config.STORAGE_CONNECTION_STRING)

def run(orig_email_submissions: list) -> dict:
    '''
    This function receives a list of email submissions and returns a list of reportable phishing emails.
    :param orig_email_submissions: list of all original email submissions
    :return: list of reportable phishing emails
    '''
    if not orig_email_submissions:
        return None

    email_data = __get_bodies(orig_email_submissions)
    eml_data = __get_emls(orig_email_submissions)

    phishing_submissions = __parse_submissions(email_data)

    if not phishing_submissions:
        return None

    grouped_submissions = __group_submissions(phishing_submissions)

    reportable_groups = __get_reportable_groups(grouped_submissions)

    if not reportable_groups:
        __add_to_table(phishing_submissions)
        return None

    for group in reportable_groups:
        util.get_body_url(group, eml_data)
        util.get_eml_screenshot(group, eml_data)

    __add_to_table(phishing_submissions)

    return reportable_groups

def __get_bodies(data: list) -> list:
    '''
```



Hiya! Phishing Bot here!

The following emails have been idenitified as potential phishing campaigns:

Subject Line: Security Alert: Unauthorized Bitcoin Purchase Attempt
Number of Reports: 5
Latest Reporter: [redacted]
Potential Threat Actor: [redacted]
Date of Last Report: Thursday, Feb 06, 2025 at 12:02 PM EST
Report Reason: Submission Count

Information Technology
UNIVERSITY OF SOUTH CAROLINA

NEXT STEPS

- Continued optimization
- Automated Unit Testing
- Additional detection criteria

THANKS!

Bongiors@mailbox.sc.edu

Information Technology
UNIVERSITY OF SOUTH CAROLINA