Task Write-Up: Identifying Phishing Characteristics in a Suspicious Email Sample

Objective

The primary goal of this task is to identify and analyze the characteristics of phishing in a suspicious email sample. Phishing is a malicious attempt to obtain sensitive information, such as usernames, passwords, or credit card details, by disguising as a trustworthy entity in electronic communication. By recognizing the signs of phishing, individuals can protect themselves from potential scams and data breaches.

Tools Required

1. Email Client or Saved Email File: This will be the source of the suspicious email that we will analyze. It can be accessed through any standard email client (like Gmail, Outlook, etc.) or as a saved text file.
2. Free Online Header Analyzer: This tool will help us examine the email header, which contains crucial information about the sender, the path the email took, and any potential red flags that indicate phishing.

Sample Email:

https://github.com/CnRagnor/Elevate_Labs/blob/main/Phishing%20Email/sample_email.eml

Source(https://github.com/rf-peixoto/phishing_pot)

Practical Example

Details:

To: phishing@pot

From: tomaskicrom@physicaltherapyahwatukee.com

Subject: USA Mechanics, Dream Tools or More? Peek Inside!

Date Received: 04/10/2023 17:44

URL Count: 16

Attachment Count: 0

Sender IP: fe80::478e:3ef6:f13a:25d0

Geolocation: IP not found in GeoLocation database

Sender IP Blacklist Check Status: Error

Analysis Date: 27/05/2025 08:08

Reason: Forbidden

Links Found in the Email:

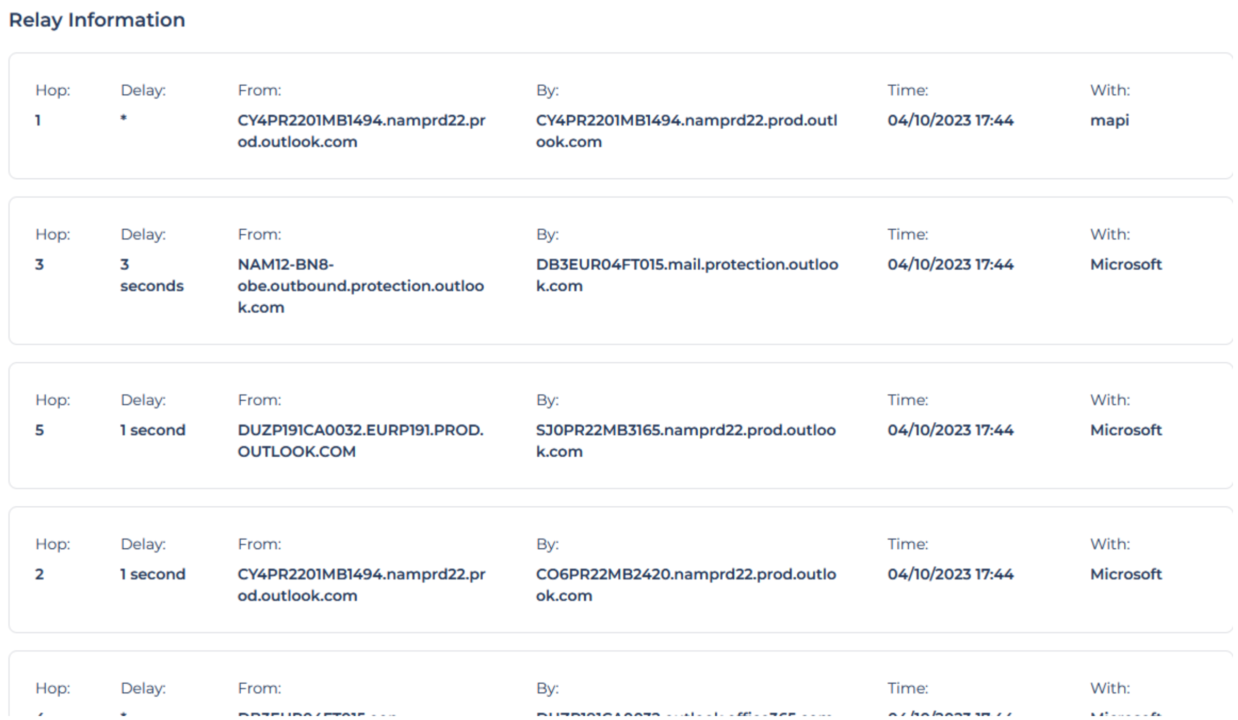
1. https://genofood.com/bhs/DyS5VzqpGzGA0j.php?email=rodrigo-f-p@hotmail.com - Undetected
2. https://info.mrc.org/e/752103/m-campaign-ws-utm-content-head/3nrk9s/1606649565?h=4CVUIvbiO2Z9HZ5Xy87aCRGeE4ubu_EuVEs-FEXzl1A - Undetected
3. https://info.mrc.org/e/752103/newsletter-preferences/3nrk9w/1606649565?h=4CVUIvbiO2Z9HZ5Xy87aCRGeE4ubu_EuVEs-FEXzl1A - Undetected

4. https://info.mrc.org/e/752103/mrcsocial/47c451/1606649565?h=4CVUIvbiO2Z9HZ5Xy87aCRGeE4ubu_EuVEs-FEXzl1A - Undetected
5. https://info.mrc.org/e/752103/Jnck7Hl9uic/3nrk8s/1606649565?h=4CVUIvbiO2Z9HZ5Xy87aCRGeE4ubu_EuVEs-FEXzl1A - Undetected

Findings:

1. Obtain the Suspicious Email: Start by selecting the email provided above, which raises suspicion due to its unusual sender and subject line.
2. Analyze the Email Header:
   - Use the free online header analyzer to input the email header information. This will provide insights into the sender's email address, the originating IP address, and the servers that processed the email.
   - Look for discrepancies in the sender's address, such as misspellings or unusual domains that do not match the organization's official domain.
3. Examine the Email Content:
   - Sender Information: The email is from a public domain, which raises a red flag. The sender's address, tomaskicrom@physicaltherapyahwatukee.com, should be verified against the official domain of the organization.
   - Language and Tone: The subject line, "USA Mechanics, Dream Tools or More? Peek Inside!" is vague and enticing, which is a common tactic used in phishing emails.
   - Links and Attachments: There are 16 URLs included in the email, which is unusually high. Hover over the links to check if the URLs match the displayed text. The presence of multiple undetected links is concerning.
4. Identify Security Threats:
   - Email does not request personal information directly, but the vague subject and numerous links suggest a potential phishing attempt.
   - The sender's IP address is not found in the GeoLocation database, which could indicate a lack of legitimacy.

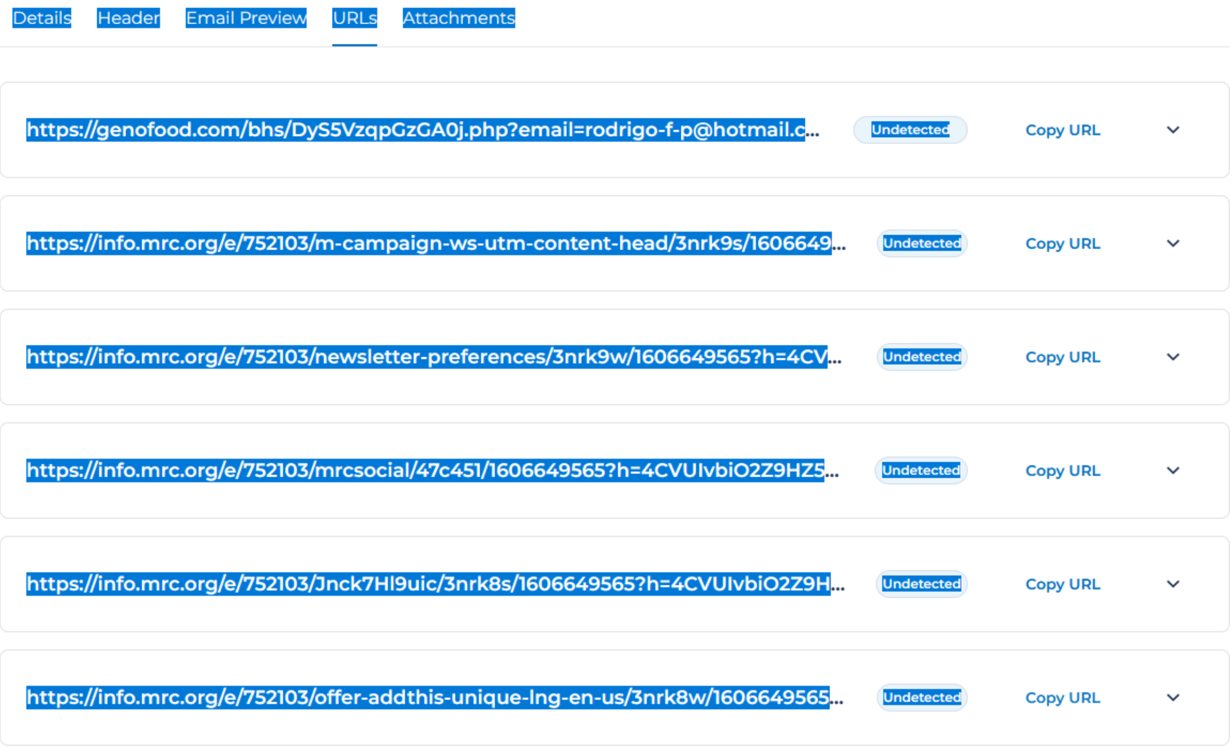
Relay Information



Relay Information

Hop:	Delay:	From:	By:	Time:	With:
1	*	CY4PR2201MB1494.namprd22.prod.outlook.com	CY4PR2201MB1494.namprd22.prod.outlook.com	04/10/2023 17:44	mapi
3	3 seconds	NAM12-BN8-obe.outbound.protection.outlook.com	DB3EUR04FT015.mail.protection.outlook.com	04/10/2023 17:44	Microsoft
5	1 second	DUZP191CA0032.EURP191.PROD.OUTLOOK.COM	SJ0PR22MB3165.namprd22.prod.outlook.com	04/10/2023 17:44	Microsoft
2	1 second	CY4PR2201MB1494.namprd22.prod.outlook.com	CO6PR22MB2420.namprd22.prod.outlook.com	04/10/2023 17:44	Microsoft
4	*	DB3EUR04FT015.eop	DUZP191CA0032.outlook.office365.com	04/10/2023 17:44	Microsoft

URLS:



https://genofood.com/bhs/DyS5VzqpGzGA0j.php?email=rodrigo-f-p@hotmail.c... Undetected Copy URL

https://info.mrc.org/e/752103/m-campaign-ws-utm-content-head/3nrk9s/1606649... Undetected Copy URL

https://info.mrc.org/e/752103/newsletter-preferences/3nrk9w/1606649565?h=4CV... Undetected Copy URL

https://info.mrc.org/e/752103/mrcsocial/47c451/1606649565?h=4CVUIvbiO2Z9HZ5... Undetected Copy URL

https://info.mrc.org/e/752103/Jnck7Hl9uic/3nrk8s/1606649565?h=4CVUIvbiO2Z9H... Undetected Copy URL

https://info.mrc.org/e/752103/offer-addthis-unique-lng-en-us/3nrk8w/1606649565... Undetected Copy URL

Phishing Email Alert: How to Spot a Scam Fast

Wondering if that email in your inbox is trying to trick you? If you answer "yes" to any of these signs, be cautious—it could be a scam.

Check Who Sent It

- Is the sender’s address from a generic provider like Gmail but claiming to be a company?
- Is the website domain just a little off or misspelled (like amaz0n instead of amazon)?
- Does the sender’s email look different from what you usually get from that company?

Read the Message Carefully

- Are there typos or awkward grammar mistakes?
- Does it pressure you to act immediately, with phrases like “Urgent” or “Your account will be suspended”?

- Does the tone feel unusual or not like the normal communication style you’re familiar with?

Inspect Links and Attachments

- Does the link’s URL not match the clickable text?
- Did they include attachments you weren’t expecting?
- Are the buttons or links vague, saying things like “Click here” or “Verify now”?

Watch Out for Pressure Tactics

- Are they asking for sensitive details like passwords or personal info?
- Do they urge you to ignore normal company procedures?
- Do they threaten consequences if you don’t respond quickly?

If any of these rings are true, don’t click or download anything. Instead, get in touch with the company directly using a verified contact source before taking any action.

Stay safe and always double-check suspicious emails!

Conclusion

By following these steps and using the specified tools, individuals can effectively identify phishing characteristics in suspicious emails. This enhances personal information protection and contributes to cybersecurity awareness.

Always remember to verify any suspicious communications through trusted channels before taking any action.