README: Phishing Email Analysis Report

Task Overview

Task 2: Analyze a Phishing Email Sample
This task involves examining a suspicious email file to identify key phishing indicators. The objective is to develop awareness of phishing tactics and enhance threat analysis skills.

Objective

To investigate and analyze a potentially malicious email message and generate a detailed report listing the phishing characteristics found within the content and metadata of the message.

Tools Used

- .eml file email viewer
- Manual header analysis
- Online email header analyzers (e.g., MXToolbox, Google Admin Toolbox)
- Text parsing tools (optional)

Email Sample Details

Subject: Microsoft account unusual signin activity
From: no-reply@access-accsecurity.com
Reply-To: sotrecognizd@gmail.com
To: phishing@pot
Date: Fri, 08 Sep 2023 05:47:04 +0000
Claimed Sign-In IP: 103.225.77.255 (Russia)

Phishing Indicators Identified

1. Spoofed Sender Address:
   - Claims to be Microsoft, but sender domain is access-accsecurity.com (not legitimate).

README: Phishing Email Analysis Report

2. Suspicious Reply-To:

   - Points to a Gmail address (sotrecognizd@gmail.com), not affiliated with Microsoft.

3. Authentication Failures:

   - SPF: None
   - DKIM: None
   - DMARC: Permanent error

4. Urgent Language:

   - Phrases designed to induce fear and fast action.

5. Deceptive Hyperlinks:

   - Uses mailto links to direct the user to email the attacker.

6. Tracking Pixel:

   - Hidden image used for tracking the email opening.

7. Impersonation of Branding:

   - Mimics Microsoft UI but uses a fake domain.

8. Lack of Personalization:

   - Generic greeting, no user-specific information.

9. Fake Unsubscribe Link:

   - Also routes to a suspicious email address.

Conclusion

This email is a confirmed phishing attempt.

It includes:

- Spoofed identity

README: Phishing Email Analysis Report

- Urgent call to action
- Failed email authentication
- Malicious contact links

Recommendation:

Do not respond or click on any links. Report and delete the email immediately.

Deliverables

- Email_Sample.eml (raw email file)
- README.pdf (this document)
- Phishing Analysis Report (contained in this README)