# PHISHING EMAIL ANALYSIS REPORT

**Prepared By:**

**Spandana S**

Future Interns Project

Cybersecurity Task

# ABSTRACT

Phishing attacks remain one of the most common and effective cyber threats, exploiting human behavior rather than technical vulnerabilities to gain unauthorized access to sensitive information. This report focuses on the analysis of phishing emails to identify key indicators that distinguish malicious messages from legitimate communication. Using reconstructed and publicly available phishing email examples, the study examines sender details, email content, embedded links, and header-level authentication mechanisms such as SPF, DKIM, and DMARC. The analysis highlights common social engineering techniques, including urgency, brand impersonation, and deceptive links, used to manipulate users into disclosing credentials. Additionally, the report provides practical prevention and awareness guidelines aimed at helping users and organizations recognize and respond to phishing attempts effectively. The findings emphasize the importance of email inspection and user awareness as critical components of cybersecurity defense.

# INTRODUCTION

Phishing is a type of cyber attack in which attackers attempt to deceive users into revealing sensitive information such as login credentials, personal data, or financial details by impersonating trusted organizations. These attacks are commonly carried out through emails that appear legitimate and often exploit human emotions such as fear, urgency, or curiosity.

Attackers use various techniques in phishing emails, including spoofed sender domains, misleading links, fake notifications, and social engineering tactics to trick recipients into taking immediate action. Even users with basic technical knowledge can fall victim to well-crafted phishing messages, making email-based attacks a significant risk for individuals and organizations alike. A single successful phishing attempt can lead to data breaches, financial loss, and unauthorized access to systems.

This report focuses on analyzing phishing emails to identify key indicators that help distinguish malicious emails from legitimate ones. By examining email content, sender details, embedded links, and header authentication mechanisms, the study aims to demonstrate how phishing attempts can be detected effectively. In addition, the report emphasizes the importance of user awareness and preventive measures as essential components of a strong cybersecurity defense.

# OBJECTIVES

The objectives of this study are:

- To understand the concept of phishing and its role as a major cybersecurity threat.
- To analyze phishing emails and identify common indicators that distinguish them from legitimate emails.
- To examine sender details, email content, and embedded links to detect signs of phishing.
- To understand the role of email header authentication mechanisms such as SPF, DKIM, and DMARC in phishing detection.
- To classify analyzed emails based on their risk level (Phishing / Suspicious / Safe).
- To promote user awareness by outlining preventive measures to reduce the risk of phishing attacks.

# METHODOLOGY

- Phishing email samples were selected using reconstructed examples and publicly available phishing repositories.
- Email content was analyzed to identify social engineering techniques such as urgency, impersonation, and generic messaging.
- Sender domains were inspected to detect spoofing and look-alike domain techniques.
- Embedded links were examined without clicking to identify suspicious or misleading URLs.
- Email header analysis was performed conceptually using tools such as MXToolbox and Google Admin Toolbox to understand authentication indicators like SPF, DKIM, and DMARC.
- Based on identified indicators, each email was classified according to its risk level.

# PHISHING EMAIL ANALYSIS

## Phishing Email Sample 1 – Microsoft Account Alert

This email claims to be from Microsoft Security and alerts the user about unusual sign-in activity. The message urges immediate action by requesting account verification, which is a common tactic used in credential stealing phishing attacks.

**Email Content (Sample)**

From: Microsoft Support <security-alert@micros0ft-support.com>

To: user@example.com

Subject: Urgent Action Required – Unusual Sign-in Activity Detected

Dear User,

We detected unusual sign-in activity on your Microsoft account from an unknown device.

To prevent account suspension, please verify your identity immediately by clicking the link below:

https://micros0ft-support[.]com/verify-account

Failure to verify your account within 24 hours will result in temporary suspension.

Thank you,

Microsoft Security Team

### 1) Sender Domain Inspection

**Findings:** The sender email address uses the domain micros0ft-support.com, which closely resembles a legitimate Microsoft domain but replaces the letter "o" with the number "0". This technique, known as typosquatting, is commonly used in phishing attacks to impersonate trusted brands. Example of similar typosquatting techniques: rnicrosoft.com (using ‘rn’ instead of ‘m’).

**Conclusions:** The sender domain is spoofed and does not belong to Microsoft.

### 2) Email Header Analysis

**Approach:** Email header analysis was performed conceptually using tools such as MXToolbox and Google Admin Toolbox to understand sender authentication and routing information.

**Indicators Observed:**

- SPF, DKIM, and DMARC authentication checks would likely fail or show misalignment due to the spoofed sender domain.
- The email is unlikely to originate from an authorized Microsoft mail server.

**Conclusion:** Header-level authentication indicators suggest that the email is not legitimate.

### 3) Link Inspection

**Finding:** The verification link directs to micros0ft-support[.]com, which is not an official Microsoft domain. Although the link uses HTTPS, the domain itself impersonates a trusted brand and is likely designed to capture user credentials.

**Conclusion:** The embedded link is suspicious and unsafe.

### 4) Phishing Indicators Identified

The following phishing indicators were identified in this email:

- Spoofed sender domain using look-alike characters.
- Urgent and threatening language to create fear.
- Generic greeting without personalization.
- Suspicious verification link.

## 5) Risk Classification

**Final Classification:** Phishing Email

**Risk Level:** High

**Reason:** The email attempts to harvest user credentials through brand impersonation, urgency-based messaging, and a deceptive verification link.

## 6) Summary

- The email impersonates Microsoft using a spoofed domain.
- Header authentication mechanisms indicate sender illegitimacy.
- The embedded link is designed for credential harvesting.
- Multiple phishing indicators confirm malicious intent.

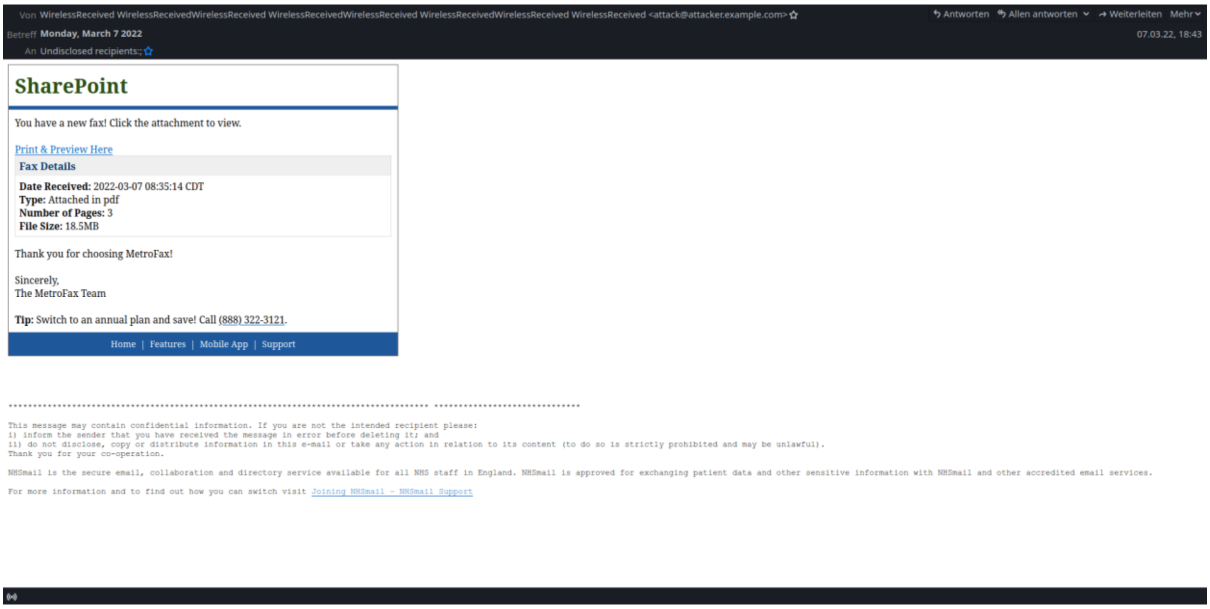
## 7) Prevention and Awareness Guidelines

- Do not click on links in unexpected security emails.
- Verify sender domains carefully for spelling variations.
- Access accounts by typing official website URLs manually.
- Report suspected phishing emails to the security team.

## Phishing Email Sample 2 – New Fax Message

The phishing email sample was obtained from a public GitHub repository in .eml format, which includes both the header and body. The header fields were examined to identify authentication indicators such as SPF and DKIM.

**FIGURE 1: SharePoint themed phishing email example.**



Von WirelessReceived WirelessReceivedWirelessReceived WirelessReceivedWirelessReceived WirelessReceivedWirelessReceived WirelessReceived <attack@attacker.example.com>

Betreff **Monday, March 7 2022**

An Undisclosed recipients:;

07.03.22, 18:43

**SharePoint**

You have a new fax! Click the attachment to view.

Print & Preview Here

**Fax Details**

**Date Received:** 2022-03-07 08:35:14 CDT
**Type:** Attached in pdf
**Number of Pages:** 3
**File Size:** 18.5MB

Thank you for choosing MetroFax!

Sincerely,
The MetroFax Team

**Tip:** Switch to an annual plan and save! Call (888) 322-3121.

```
************************************************************************************ ******************************

This message may contain confidential information. If you are not the intended recipient please:
i) inform the sender that you have received the message in error before deleting it; and
ii) do not disclose, copy or distribute information in this e-mail or take any action in relation to its content (to do so is strictly prohibited and may be unlawful).
Thank you for your co-operation.

NHSmail is the secure email, collaboration and directory service available for all NHS staff in England. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other accredited email services.

For more information and to find out how you can switch visit Joining NHSmail – NHSmail Support
```

This image shows a SharePoint-themed phishing email/webpage. Attackers commonly impersonate Microsoft SharePoint because many organizations use it for file sharing.

The email or page claims that:

A document or message is waiting. The user must click a link to view it.

This is a real-world, very common phishing technique.

### 1) Sender Domain Inspection

**Finding:** The sender email address does not belong to a legitimate fax service provider and appears unrelated to any known organization offering fax services.

**Conclusion:** The sender domain is suspicious and does not match the claimed service.

### 2) Email Header Analysis

**Approach:** Conceptual header analysis was performed using tools such as MXToolbox and Google Admin Toolbox to evaluate sender authentication and legitimacy.

**Indicators Observed:** SPF, DKIM, and DMARC authentication would likely fail or show misalignment. The sending mail server is unlikely to be associated with a legitimate fax service provider.

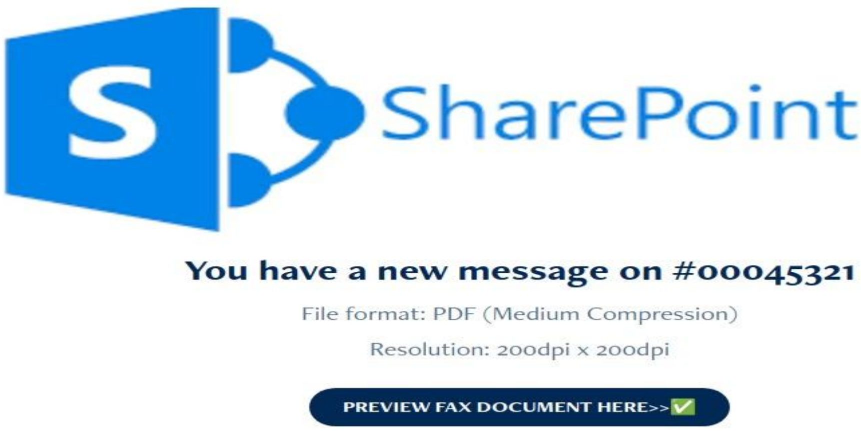
**Conclusion:** Header authentication indicators suggest the email is spoofed.

### 3) Image and Link Inspection

**Finding:** The email relies on an embedded image instead of clear text content. The image acts as a clickable element redirecting users to an external webpage. Image-based links are commonly used to bypass spam filters and hide malicious URLs.

**Conclusion:** The embedded image is suspicious and likely redirects users to a credential-harvesting or malicious site.

**FIGURE 2: Example of image based phishing redirection.**



You have a new message on #00045321

File format: PDF (Medium Compression)

Resolution: 200dpi x 200dpi

This image represents the webpage users are typically redirected to after interacting with the phishing email.

### 4) Phishing Indicators Identified

The following phishing indicators were identified:

- Unexpected fax notification.
- Lack of sender identity or personalization.
- Image-based call to action.
- Suspicious sender domain.
- No contextual information about the fax content.

### 5) Risk Classification

**Final Classification:** Phishing Email.

**Risk Level:** High.

**Reason:** The email uses an unexpected fax alert and an image-based link to trick users into clicking a potentially malicious resource.

### 6) Findings Summary

- The email impersonates a fax notification without legitimate sender verification.
- Header authentication mechanisms indicate sender illegitimacy.
- The image-based redirection is a common phishing technique.
- Multiple phishing indicators confirm malicious intent.

### 7) Prevention and Awareness Guidelines

- Users should be cautious of unexpected fax or document notifications.
- Avoid clicking images or buttons in unsolicited emails.
- Verify fax notifications through official internal systems or trusted providers.
- Report suspicious emails to the organization’s security team.

## Conclusion

The analysis of two distinct phishing email samples highlights how attackers use different techniques, such as text-based deception and image-based impersonation, to exploit users. Despite variations in format, both emails share common phishing indicators that can be effectively identified through careful inspection.