**Phishing Email Threat Analysis Report**

**Objective**

Analyze the provided phishing email samples, identify their common characteristics, and summarize observed phishing tactics to build awareness and demonstrate email threat analysis skills.

**Sample Phishing Emails Reviewed**

Example 1: Account Suspension Notice (PayPal themed)

***From:****PayPaI Support <*[*support@paypa1-services.com*](mailto:support@paypa1-services.com)*>****Subject:****URGENT: Your PayPal Account Will Be Suspended!*

*Dear Customer,*

*We noticed unusual activity in your account. For your protection, your account will be suspended unless you verify your information immediately.*

***Please click the link below to verify your account:***[*https://paypa1-secure-login.com*](https://paypa1-secure-login.com/)

*Failure to respond will result in permanent suspension.*

*Thank you,  
PayPal Security Team*

Example 2: Tax Refund Notification (IRS themed)

***From:****IRS Support <*[*irs-taxrefund@secure-mail.net*](mailto:irs-taxrefund@secure-mail.net)*>****Subject:****You Are Eligible for a Tax Refund!*

*Dear Taxpayer,*

*After annual calculations of your fiscal activity, we have determined that you are eligible for a $1,250 tax refund.*

***Access your refund form here:***[*Open refund form*](http://refund-irs-gov.com/secure)

*Please submit the completed form within 24 hours.*

*Regards,  
Internal Revenue Service*

Example 3: Delivery Problem Notification (FedEx themed)

***From:****FEDEX Express <*[*delivery@fedex-parcels.co*](mailto:delivery@fedex-parcels.co)*>****Subject:****Package Delivery Issue – Action Required*

*Hello,*

*We attempted to deliver your package today but were unsuccessful due to incomplete address information.*

*Please open the attached document and provide the correct address to reschedule delivery.*

***Attachment:****FedEx-Delivery-Details.zip*

*Sincerely,  
FedEx Delivery Team*

Example 4: Unusual Sign-in Attempt (Microsoft themed)

***From:****Microsoft Account Team <*[*security@micros0ft-accounts.com*](mailto:security@micros0ft-accounts.com)*>****Subject:****Unusual sign-in attempt detected*

*Dear user,*

*We detected an unusual sign-in attempt to your Microsoft account from IP: 159.123.45.6, location: Russia.*

*If this was not you, please secure your account immediately by resetting your password:*[*Secure My Account*](http://micros0ft-support.com/)

*Thank you for helping us protect you.  
Microsoft Security Team*

Example 5: Winner Notification (Amazon themed)

***From:****Amazon Rewards <*[*winner@amaz0n-giveaway.com*](mailto:winner@amaz0n-giveaway.com)*>****Subject:****Congratulations! You’ve Won a $500 Amazon Gift Card*

*Dear Valued Customer,*

*You have been selected as the winner of the Amazon Gift Card Promotion! To claim, simply fill out your delivery information:*

[*Claim your prize*](http://amazon-prize-center.com/)

*Congratulations once again!  
Amazon Rewards Team*

1. Sender’s Email Address (Spoofing & Mismatching)

Spoofed Domains: All samples use sender addresses that closely resemble, but do not match, official domains. For instance, support@paypa1-services.com versus legitimate @paypal.com, and security@micros0ft-accounts.com versus @microsoft.com.

Misspelling/Substitution: Use of visually similar characters (“1” for “l”, “0” for “o”) and non-standard domains (amaz0n-giveaway.com).

Suspicious Generic Emails: Some use general public domain emails (e.g., free mail accounts or non-corporate-sounding domains).

2. Email Headers & Technical Discrepancies

Discrepant Return Path: The address shown doesn’t match the real sender—visible in header analysis using online tools.

Irregular Sending Servers: Analysis may reveal emails sent via non-affiliated infrastructure, not the genuine brand servers.

3. Suspicious Links and Attachments

Hyperlinks Masked as Legitimate: Hovering over links exposes the real destination, which often subtly differs from the official domain (e.g., paypa1-secure-login.com or refund-irs-gov.com/secure).

Dangerous Attachments: Attachments (like FedEx-Delivery-Details.zip) commonly contain malware or further phishing prompts.

Warning: Clicking these could compromise security.

4. Urgent or Threatening Language

Pressure to Act: Frequent use of phrases like “Your account will be suspended immediately,” or “submit the completed form within 24 hours.”

Threat of Loss: Suggest negative consequences for inaction: account suspension, loss of funds, missed prize, etc.

Reward/Lure: “You’ve won a $500 gift card”—exploiting recipient excitement to provoke unthinking responses.

5. Mismatched URLs

URL/Visible Text Disparity: Link text says one thing, but the underlying URL goes somewhere unexpected. For example, “Secure My Account” links to micros0ft-support.com, not microsoft.com. Always hover to check.

6. Spelling & Grammar Errors

Frequent Mistakes: Noted errors such as “Your acount are about to be colsed” point to non-professional origins.

Odd Phrasing: Unnatural language that native speakers would not use; misspellings abound throughout samples.

7. Generic Greetings

No Personalization: Greetings like “Dear Customer” or “Dear User” suggest a bulk email, rather than a legitimate business outreach, which would typically use your actual name.

8. Request for Sensitive Data

Unusual Requests: Asking for passwords, credit card numbers, or other confidential data via email is a hallmark of phishing.

Submission of Personal Info: Links or forms ask for sensitive input under the guise of security or claim processes.

9. Other Phishing Red Flags

Unexpected Attachments: Files sent without prior context, especially zipped folders or macro-enabled documents.

Strange Formatting: Odd colors, disproportionately large logos, or inconsistent font usage.

**Summary Table of Phishing Characteristics**

|  |  |
| --- | --- |
| Phishing Trait | How It Appears in the Samples |
| Spoofed/misspelled sender | support@paypa1-services.com, security@micros0ft-accounts.com |
| Header/server mismatch | Return path or sender’s domain doesn't match display name |
| Urgency/threats | “Your account will be suspended…”, “Act now…” |
| Suspicious link/attachment | Links to faked domains, attached .zip files |
| Mismatched URLs | Link text is safe but true URL is suspicious |
| Grammar/spelling problems | “Your acount are about…”, “Congratulattions!” |
| Generic greeting | “Dear customer,” or no greeting |
| Sensitive data request | “Please confirm your password/credit card number” |

**Conclusion & Awareness**

The above phishing samples demonstrate the classic warning signs organizations and individuals should watch for when evaluating suspicious emails. Spotting these traits is essential for cyber hygiene and prevents falling victim to common email-based attacks.

**Key takeaways include:**

* Inspect sender address and email header details.
* Never open unexpected attachments or click suspicious links.
* Verify URLs, especially when prompted to log in or provide details.
* Question urgent or threatening language.
* Look for improper grammar, odd formatting, and generic greetings.
* If any of these red flags are present, report the email to IT/security teams and do not interact further.

: 50+ Phishing Email Examples - Hook Security

: 19 Phishing Email Examples - Terranova Security

: 10 Real Phishing Email Examples - Norton