July 22, 2025

**Project: Analyzing a Phishing Email**

Written by: Joshua Lopez

Simi Valley, California, USA

[jlopez082905@gmail.com](mailto:ty.01ww@gmail.com)

**Step 1 - Spin up a Virtual Machine to Conduct Analysis**A screenshot of a computer

AI-generated content may be incorrect.

It is best practice to use a sandboxed environment when engaging in any type of cybersecurity analysis. So, make sure you have a VM spun ready to use.

**Step 2 - Find or Generate a Test Phishing Email** A screenshot of a computer

AI-generated content may be incorrect.

Other Resources: <https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-114.eml>

Case study: Phishing attempt from Adversary posing as OpenSea Sale Confirmation Email

Tools used:

* Mozilla Thunderbird
* Text Editor(VIM)
* Sandboxed kali Linux VM using the VirtualBox VM manager
* VirusTotal
* MXToolbox
* Spf-record.com
* WHOis
* IPVoid

**Introduction**

**Step 3 - Understanding the Goal**

**The Goal of a malicious attacker:**

Make the email look as legitimate as possible to increase the chances of the victims to:

* ***Open links included in the email***
  + ***Enter credentials or give away sensitive information***
* ***Open a malicious file***

**Step 4 - Understanding Email Structure**

**Email Structure:**

* ***Header***: Contains technical details of the email, including the sender, recipient, and routing information.
* ***Body***: The main content of the email, including text, images, and links.

**Step 5 - Analyze the Body of the Email**

**Spot The Red Flags in the Email Body:**

Go through the email systematically and provide comments on whether you identified any red flags for each bullet point.

* **Unfamiliar sender or email address:** The email is from someone you don't recognize, or the domain is slightly misspelt (e.g., "[*support@paypa1.com*](mailto:support@paypa1.com)" instead of "[*support@paypal.com*](mailto:support@paypal.com)"). Sender [noreply@notify.thinkific.com](mailto:noreply@notify.thinkific.com) is unfamiliar.
* **Urgent or alarming language:** The email pressures you to act immediately, often threatening consequences if you don’t. No urgency to act immediately.
* **Suspicious attachments or links:** Unexpected attachments or links that request sensitive information or lead to unfamiliar websites. Unexpected link(View Item(Button)) to unfamiliar domain.

<https://email.notify.thinkific.com/c/eJwdjUuOwyAQRE9jdkS43abDgsVscg2LTxOjkOAxRM7x4xmpNqVXesV21PqKQFqhiNaFBA5EtnoigDRPTDTjQpMPwZECTaOa_YCq5ciP_CtLPSQZf0VDBo38JBPL5elyEauFQGmEwISYmFxKWgMZF1B5jgq9KHbtfWvD9DPA7UyuG78au3a4UrhfQn2K3e417vleZZLbebzW_qf_Z9223Hk5uJyNl-1cvkPP9fUFJI9D8g>

Additionally, according to VirusTotal, this link is flagged as malicious and phishing by 2/97 security vendors.A screenshot of a computer

AI-generated content may be incorrect.

* **Generic greetings:** Using broad salutations like "Dear Customer" instead of addressing you by name. There isn’t a salutation to a party. Only generic congratulations.
* **Spelling and grammar mistakes:** Phishing emails often contain poor grammar, awkward language, or spelling errors. No noted grammar or spelling errors.
* **Request for personal or financial information:** Asking for passwords, credit card numbers, or other sensitive information. No request for sensitive information. Just a link to view recent activity.
* **Mismatch between display name and email address:** The name shown in the email may not match the actual email address. Mismatch between display name “OpenSea NFT’s” and email noreply@notify.thinkific.com
* **Inconsistent or suspicious URLs:** Hover over links without clicking to check if the destination URL matches the claimed website. All links in the body including, facebook, twitter, linkedin all point to the same unfamiliar domain email.notify.thinkific.com. Also noted that options to unsubscribe, do not have a hyperlink for the click HERE option.
* **Unexpected request for payment:** An email asking for payment for a service you don't recognize or weren't expecting. No payment for a service requested.
* **Too good to be true offers:** Promises of large rewards, cash prizes, or free gifts that seem unrealistic. No unrealistic offers.
* **Unfamiliar or odd attachments:** Unexpected file attachments, especially if they have unusual extensions like .exe, .zip, or .rar. No attachments noted.
* **Lack of company branding:** Legitimate companies typically include professional logos, branding, and consistent formatting. OpenSeas logo is in the body of the email.
* **Unusual sender’s email domain:** The email might come from a suspicious or untrusted domain, rather than an official company email (e.g., "[info@gmail.com](mailto:info@gmail.com)" instead of "[support@company.com](mailto:support@company.com)"). Unusual sender domain noreply@notify.thinkific.com
* **No signature or contact information:** Legitimate companies usually include proper signatures and contact details at the end of their emails. No sender or contact information provided.

**Step 6 - Analyze the Body of the Email**

**Analyzing the Email Header:**

Go through the email systematically and provide comments on whether or not you identified any red flags for each bullet point.

* **"From" Address**
  + **Check the sender's email address** for inconsistencies or slight misspellings that mimic legitimate domains (e.g., "[support@paypa1.com](mailto:support@paypa1.com)" instead of "[support@paypal.com](mailto:support@paypal.com)").

Verify if the domain matches the supposed sender's official domain. On OpenSeas website, noted domain is <https://opensea.io/> which does not match senders official domain notify.thinkific.com

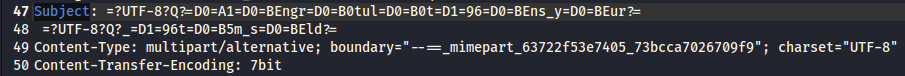
* **"Reply-To" Address**
  + Inspect the **"Reply-To"** field.Phishing emails often use a different reply address than the "From" address, redirecting replies to the scammer. Reply-To contact email is [contacto@pixostudio.com](mailto:contacto@pixostudio.com) different from the FROM address noreply@notify.thinkific.com
* **"Received" Fields**
  + Check the **"Received"** headers to trace the path of the email. Compare the IP addresses and domains to ensure they originate from a legitimate source.
  + If the email claims to be from a well-known service but the IP belongs to an unrelated provider, this is suspicious. IP Received: from rs186.mailgun.us (209.61.151.186) belongs to an unrelated provider.
* **IP Address and Domain Reputation**
  + Analyze the **IP addresses** in the"Received" fields. Use tools like **MXToolbox** or **IPVoid** to check if the IP is associated with phishing or spam. IP Address 209.61.151.186 in the received section is not blacklisted.
  + Look up the sending domain for any blacklists or warnings using domain reputation tools like **Whois** or **MXToolbox.** According to MXToolbox, sending domain rs186.mailgun.us is not blacklisted.
* **External Links and Attachments**
  + Hover over any links to inspect their true destination. Ensure they match the expected domain (e.g., "[delivero[.]com](http://deliveroo.com)"). Use tools like **VirusTotal** or **PhishTank** to scan URLs for malware or phishing attempts. According to VirusTotal, sending domain rs186.mailgun.us, which is a designated and permitted sender for the FROM domain notify.thinkific.com, is flagged malicious by security vendor Webroot.

A screenshot of a computer

AI-generated content may be incorrect.

* + Do not download or open any attachments unless you are certain of their legitimacy. Suspicious attachments should be scanned using antivirus software or online services like VirusTotal to check for malware.
* **DKIM Signature (DomainKeys Identified Mail)** A computer screen with white text

  AI-generated content may be incorrect.
  + **DKIM** verifies if the email was sent by the legitimate domain. Check if the DKIM signature in the header is valid and aligned with the domain of the email sender. DKIM from legitimate domain and aligned with domain of the email sender.
* **SPF Record (Sender Policy Framework)** A computer screen with white text

  AI-generated content may be incorrect.
  + Look for an **SPF** record result in the header, indicating if the email passed or failed SPF authentication. A **pass** means the email came from an authorized server for that domain. Email came from an authorized server for that domain.
  + If it **fails**, it's a sign the email may be **forged**.
* **DMARC Authentication** 
  + **DMARC** (Domain-based Message Authentication, Reporting & Conformance) ensures the email’s authenticity. Look for **pass** or **fail** results, which indicate whether the message aligns with SPF and DKIM policies. DMARC = pass, message aligns with SPF and DKIM policies.
* **Message-ID** 
  + Every legitimate email has a unique **Message-ID**. Check for strange patterns in this field, such as missing, repeated, or generic message IDs, which can indicate spoofing. No strange patterns noted.
* **Subject Encoding and Language** 
  + Review the **subject line** for suspicious characters, encoding issues, or misspellings. Malicious actors often use strange encoding or poorly constructed subjects to bypass filters. No strange patterns noted.
* **MIME-Version** A screenshot of a computer program

  AI-generated content may be incorrect.
  + Check the **MIME-Version** field to see how the email’s format is structured. Irregular MIME types or missing headers may indicate an mpt to manipulate the format for malicious purposes. Noted a different url https://iopenseaswallet.com for the link “VIEW ITEM.” Right-clicking the VIEW ITEM button on the email and copying link location points to domain <https://email.notify.thinkific.com>. Not sure if that is a redirection. That url does not have a DNS Record, according to MXToolbox.

**Step 7 - Summary**

* Phishing likelihood: High. Unfamiliar sender email address, suspicious link in body of email flagged for malicious and phishing activity. Mismatch between display name and email address, all links in email pointing to domain flagged malicious. No sender contact information, Reply-To email address different from the FROM email address, sender IP belongs to an unrelated provider. All signs of malicious phishing activity.