**TITLE :**

**Phishing Email Analysis:**

How to Identify, Analyse, and Understand Malicious Emails

**How to Identify a Fake Email (Phishing):**

>> Check the Sender’s Address

Looks similar to a real one but slightly altered (e.g., admin@paypa1.com instead of paypal.com).

>> Look for Urgent or Threatening Language

“Your account will be suspended!” or “Action required immediately!”

>> Suspicious Links

Hover over links without clicking – they often lead to fake websites or malicious domains.

>> Unexpected Attachments

Especially ZIP, EXE, DOCX, or PDF files from unknown senders.

>> Generic Greeting

“Dear Customer” instead of your real name.

>> Poor Grammar or Spelling Errors

Many phishing emails contain mistakes or odd phrasing.

>> Request for Personal Information

Legit companies never ask for passwords, OTPs, or credit card numbers over email.

>> Inconsistent Branding

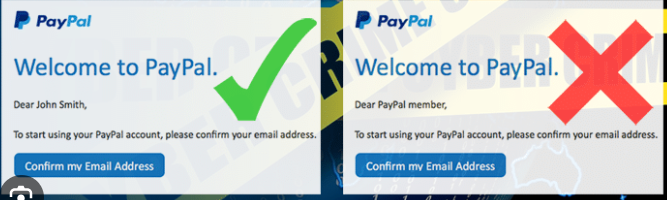
Logos, colors, or email formatting may look off or low quality.

>> Mismatch Between Sender & Reply-To

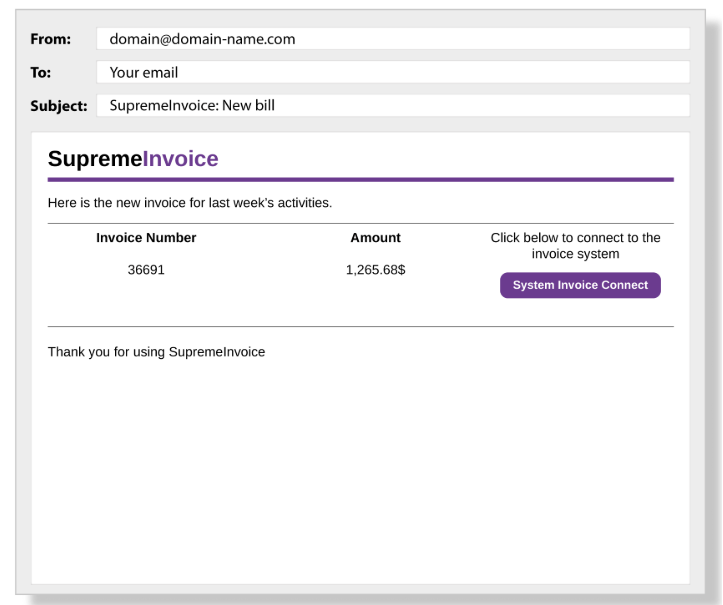
If you reply, your response goes to a completely different address.

>> Too Good to Be True Offers

“You’ve won a gift card” or “Click to claim your prize” are classic traps.



EXAMPLE :



**Phishing Email Analysis: Invoice Scam Example**

**Email Sample:**

**Subject:** SupremeInvoice: New bill  
**From:** domain@domain-name.com  
**To:** Your email

"Here is the new invoice for last week’s activities..."  
**Invoice Number:** 36691  
**Amount:** 1,265.68$  
 **[System Invoice Connect]** (button link)

**Red Flags – Why This Email Looks Suspicious:**

1. **Suspicious Sender Email**
   * The sender uses a generic and fake-looking domain: domain@domain-name.com.
   * Legitimate companies usually use official domains (e.g., billing@supremeinvoice.com).
2. **Psychological Pressure (Urgency + Money)**
   * Invoice attached with a large amount ($1,265.68) can cause panic or confusion.
   * The goal is to make you click the button without thinking.
3. **Malicious Link Button**
   * “System Invoice Connect” button likely redirects to a phishing site or malware.
   * Hovering over the link (without clicking) can reveal a suspicious URL.
4. **Poor Formatting / Language**
   * Grammar is okay, but small details are off:
     + Dollar sign placed incorrectly (1,265.68$ instead of $1,265.68).
     + Vague phrase: “last week's activities” — no reference or company name.
5. **No Contact Info / Company Branding**
   * Legitimate invoices always include:
     + A business address
     + Phone number
     + Customer service email
     + Detailed invoice context

**Red Flags Identified:**

|  |  |
| --- | --- |
| **Indicator** | **Description** |
| **Spoofed Sender Address** | The domain domain-name.com is generic and suspicious. Likely forged using spoofing techniques. |
| **Urgency with Financial Threat** | Social engineering tactic — creates pressure by showing a large invoice. |
| **Misleading Button Link** | Button may redirect to a malicious login page or malware dropper. |
| **Unusual Formatting** | Currency format is incorrect (1,265.68$ instead of $1,265.68). |
| **No Personalization** | No recipient name or real invoice details, which real businesses usually include. |

**Header Analysis (What to Check):**

If available, analyze the original email header for:

* **Return-Path:** Does it match the "From" address?
* **SPF (Sender Policy Framework):** Pass/Fail?
* **DKIM (DomainKeys Identified Mail):** Signed correctly?
* **DMARC:** Enforced by domain owner?
* **Received:** Look for suspicious or mismatched mail servers.

**Social Engineering Techniques Used:**

|  |  |
| --- | --- |
| **Technique** | **How it's applied** |
| **Fear of Financial Consequence** | Suggests you owe money urgently. |
| **Impersonation of Authority** | Uses a pseudo-corporate identity (fake “SupremeInvoice”). |
| **Implied Urgency** | Pushes user to “connect” without time to validate. |
| **Trust Hijacking** | Mimics structure of real invoice emails. |

**Threat Detection Tips:**

1. **Use email gateways** that filter based on SPF, DKIM, and DMARC.
2. **Implement sandboxing** to test suspicious links or attachments safely.
3. **Train staff** on phishing red flags — frequent awareness campaigns help.
4. **Inspect headers manually** or with tools like:
   * Google’s “Show Original”
   * MXToolbox Email Header Analyzer
5. **Block lookalike domains** (e.g., supremelnvoice.com vs. supremeinvoice.com)

**What You Should Do:**

* **Do not click** any links or buttons.
* **Report** the email to your IT/security team.
* **Mark it as phishing** in your email client.
* If unsure, **contact the real company** via official website, not links in the email.

**Tips to Avoid Getting Fooled:**

* Always **hover over links** to preview the actual URL.
* Verify the sender’s email domain.
* Look for **authentic invoice references**, contact numbers, and email footers.
* When in doubt, search the company name + “invoice scam” online.