**Phishing Email Analysis Report**

Sample Email Summary

* Subject: SupremeInvoice: New bill
* From: domain@domain-name.com
* Claimed Brand: SupremeInvoice
* Attachment/Link: System Invoice Connect button

**Analysis: -**

1. Sender's Email Address  
The email is sent from a suspicious domain (domain@domain-name.com).  
Legitimate businesses use official domains (e.g., @supremeinvoice.com).

2. Header Check  
Headers not shown here, but often indicate:

* Missing SPF/DKIM/DMARC
* No secure digital signature  
  Recommended tool: MxToolbox Email Header Analyzer

3. Suspicious Link or Attachment  
The “System Invoice Connect” button is likely malicious.  
Hovering may reveal a misleading or non-official domain.

4. Urgent or Manipulative Language

* Urgent tone, implies unrecognized amount (USD 1,265.68)
* No contact method, only click action

5. Mismatched or Fake Branding

* “SupremeInvoice” not a recognized or verifiable brand
* Missing contact info, legal footer, or support links

6. Grammar and Formatting Issues

* Incorrect amount format: "1,265.68USD" instead of "USD 1,265.68"
* Vague statement: “last week's activities”

Summary of Phishing Traits

* Fake sender domain
* No personalization
* Suspicious CTA button
* Urgency and billing panic tactic
* Branding inconsistencies

Purpose

This phishing example shows how invoice scams can trick users into clicking malicious links using impersonation and urgency.

Tools Used

* CanIPhish Phishing Simulation
* MxToolbox Header Analyzer
* VirusTotal URL Scanner