1. Introduction

In recent years, cyber attacks have increased significantly across industries, targeting organizations of all sizes. Among various cyber threats, email phishing has emerged as one of the most common and dangerous attack methods. Attackers use deceptive emails to trick employees into revealing sensitive information such as login credentials, financial details, and confidential business data.

Organizations face serious challenges due to phishing attacks, including financial losses, data breaches, reputational damage, and operational disruption. Since email remains a primary communication channel in businesses, even a single successful phishing attempt can compromise critical systems and sensitive information. Therefore, identifying phishing emails and strengthening user awareness has become an essential component of organizational cybersecurity strategy.

2. Objective

The primary objective of this task is to analyze email samples to identify potential phishing indicators and classify them based on risk level (Safe, Suspicious, or Phishing).

This report aims to:

- Detect common phishing characteristics such as spoofed sender addresses, fake domains, malicious links, and urgent language.
- Evaluate the potential risk associated with each email.
- Explain the identified threats in clear, business-friendly language.
- Provide practical prevention and awareness guidelines to reduce phishing risks within organizations.

3.What is Phishing?

Phishing is a cyber attack in which criminals send fake emails to trick people into sharing sensitive information. These emails are designed to look real and often appear to come from trusted organizations such as banks, payment services, or company departments.

In many phishing attacks, the sender address is spoofed. This means the attacker makes the email look like it is coming from a legitimate source, even though it is fake. For example, the email may look like it is from “support@paypal.com,” but the actual domain is slightly changed to deceive the recipient.

Phishing emails often contain links that redirect users to fake login pages. These fake websites are carefully designed to look identical to official websites. When users enter their usernames and passwords on these pages, the information is captured by the attacker.

The main objective of phishing is credential stealing. Once attackers obtain login credentials, they can access accounts, steal financial data, misuse company systems, or perform further cyberattacks. Because phishing relies on human trust and urgency, it remains one of the most successful and dangerous cyber threats faced by organizations today.

4. Types of Phishing Attacks

Phishing attacks can take different forms depending on the target and communication method. The most common types are:

1 Email Phishing

This is the most common type of phishing attack. Attackers send bulk fake emails to many users, pretending to be from trusted organizations such as banks or online services. These emails usually contain malicious links or attachments designed to steal login credentials or financial information.

2 Spear Phishing

Spear phishing is a targeted attack aimed at a specific individual or organization. Unlike general email phishing, the attacker personalizes the message using the victim's name, job role, or company details to make it more convincing and harder to detect.

3 Whaling

Whaling is a specialized form of spear phishing that targets high-level executives such as CEOs, CFOs, or senior managers. These attacks often attempt to steal large financial transactions or confidential corporate data.

4 Smishing

Smishing refers to phishing attacks conducted through SMS (text messages). Victims receive fake messages containing malicious links or urgent requests, such as prize claims or account verification alerts.

5️⃣ Vishing

Vishing (voice phishing) involves attackers making fraudulent phone calls while pretending to be bank officials, IT support, or government representatives. The goal is to convince the victim to share sensitive information over the phone.

5. Tools Used

The following tools were used to Analyze and classify suspicious URLs for phishing detection.

1️⃣ Google Safe Browsing (Transparency Report)

Google Safe Browsing was used to check whether a website is currently flagged as unsafe. It helped identify whether the site contains harmful content or attempts to trick users into sharing personal information.

2️⃣ Virus Total

Virus Total was used to scan suspicious URLs against multiple cybersecurity engines. The detection ratio (e.g., 16/94 flagged) helped classify links into High, Medium, and Low risk categories based on vendor analysis.

3️⃣ Google Docs / MS Word

Google Docs / MS Word was used to structure the report professionally, organize findings, insert screenshots, and prepare the final PDF submission.

6. Email Analysis Methodology

1️⃣ Check Sender Email Address

The sender email shown is:

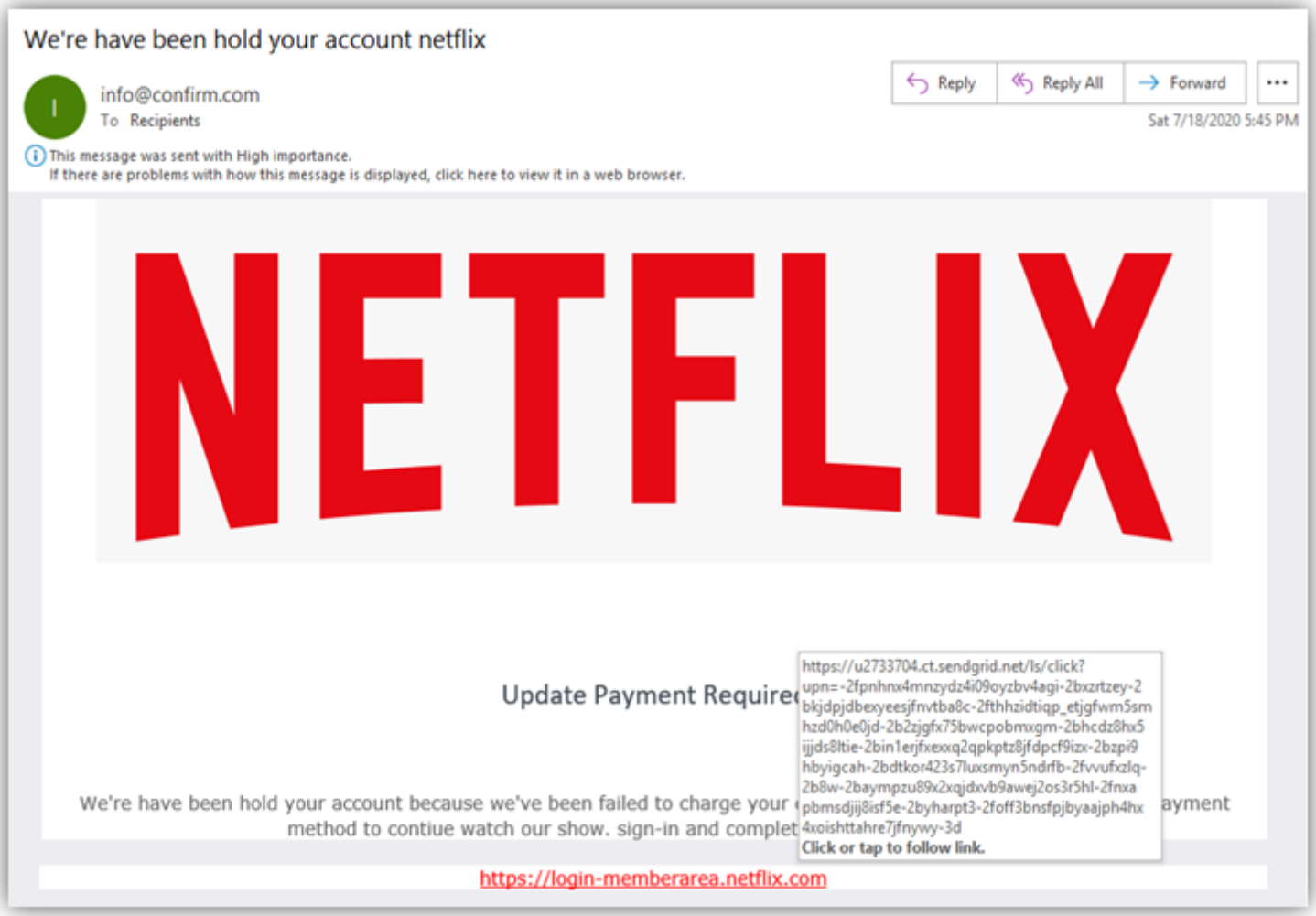
info@confirm.com

🔎 **Analysis:**

- Official Netflix emails are sent from domains like:
  - @netflix.com
- The sender domain **confirm.com** is unrelated to Netflix.

- This is a classic example of **brand impersonation using domain mismatch**.

⚠ **Red Flag Identified:** Sender domain does not match official company domain.



2 Verify Domain Legitimacy

The email contains a visible link:

https://login-memberarea.netflix.com

🔎 **Analysis:**

- Official Netflix login domain is:
  - https://www.netflix.com
- The domain shown:
  - login-memberarea.netflix.com
- While it appears similar, it is a **subdomain trick** used in phishing.

Additionally, when hovering over the button, the preview shows:

u273704.ct.sendgrid.net/...

This indicates redirection via third-party tracking or malicious routing.

⚠ **Red Flag Identified:** Domain spoofing and redirect-based phishing.

3 Check Email Header (Technical Inspection)

Although the full header is not shown in the screenshot, visible indicators include:

- "This message was sent with High importance."
- Suspicious sender infrastructure.
- Use of external email distribution service (SendGrid redirect).

🔎 **Professional Observation:**

Phishing emails often:

- Use compromised SMTP servers
- Spoof sender display name
- Use bulk mailing services

⚠ **Red Flag Identified:** Email routing inconsistency with legitimate Netflix infrastructure.

4 Inspect Embedded Links

The call-to-action button says:

"Update Payment Requirement"

Hover preview shows:

`u273704.ct.sendgrid.net/...`

🔎 **Analysis:**

- Link does not directly go to `netflix.com`
- It redirects via tracking domain
- Final visible link: `login-memberarea.netflix.com`

This technique is called:

🎣 **Credential Harvesting via Redirected Phishing Link**

⚠ **Red Flag Identified:** Suspicious redirection chain.

5️⃣ Look for Urgency Language

The email states:

"We've have been hold your account because we've been failed to charge your payment method."

🔎 **Analysis:**

- Claims account suspension
- Mentions payment failure
- Pushes user to act immediately

Phishing psychology tactic used:

⚡ **Fear + Urgency Manipulation**

This pressures victims into clicking without verifying.

⚠ **Red Flag Identified:** Artificial urgency to bypass rational thinking.

6️⃣ Check Grammar and Language Errors

Examples from the email:

- We've have been hold your account
- Incorrect verb usage
- Awkward sentence structure

🔎 **Professional Assessment:**

Legitimate corporate emails undergo:

- Legal review
- Brand consistency checks
- Grammar verification

Such errors strongly indicate fraudulent origin.

⚠ **Red Flag Identified:** Poor grammar inconsistent with professional brand communication.

📌 Final Assessment

Based on:

- Sender domain mismatch
- Suspicious redirection links
- Urgency-based manipulation
- Grammar mistakes
- Infrastructure inconsistencies

✅ This email is clearly identified as a **Phishing Attack Attempt** targeting user credentials and payment information.

2. 1 Check Sender Email Address

Sender shown:

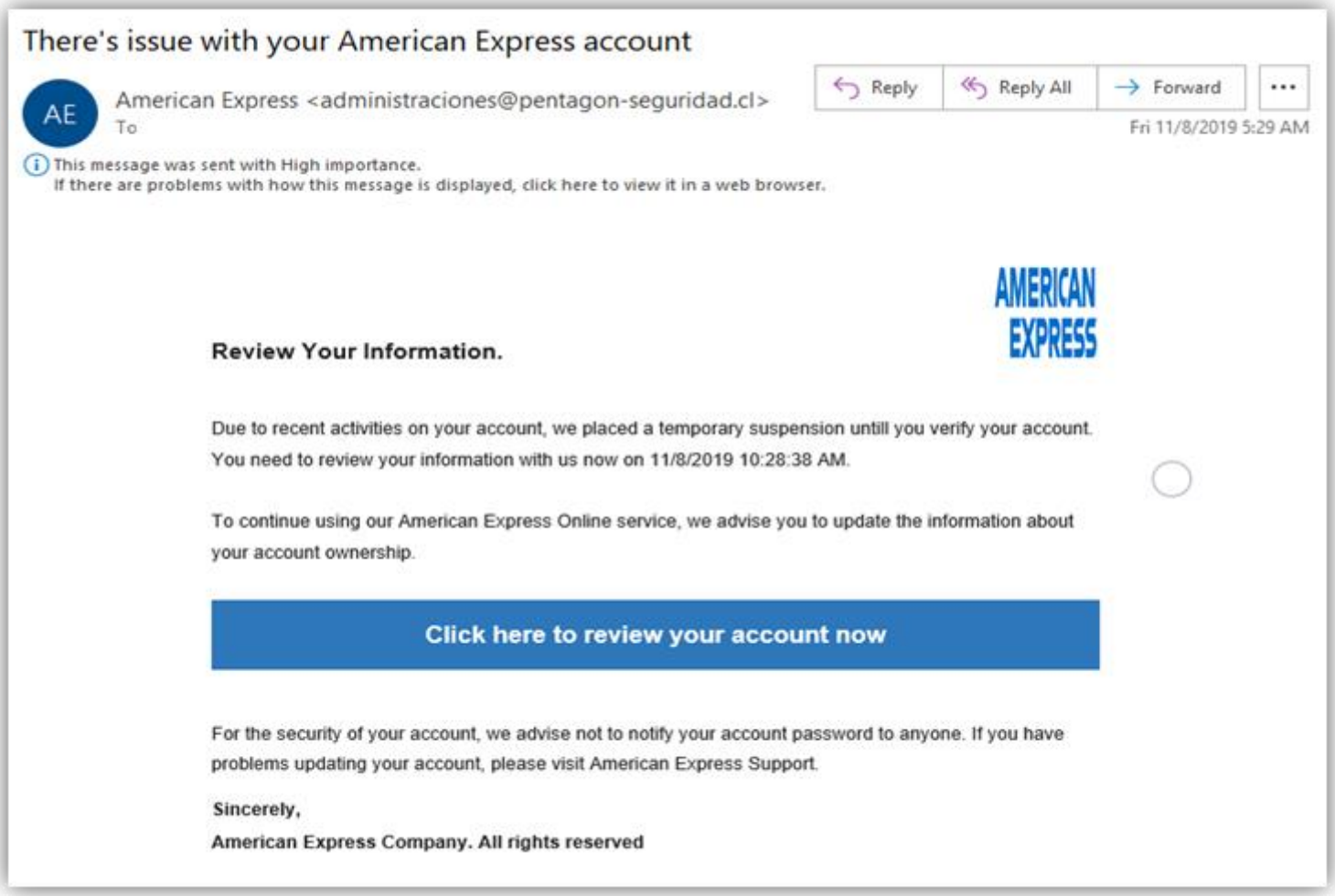
administraciones@pentagon-seguridad.cl

🔎 Analysis:

- Official American Express domain:
  - `@americanexpress.com`
- Sender domain:
  - `pentagon-seguridad.cl`
- `.cl` indicates Chile-based domain unrelated to American Express.

⚠ Critical Red Flag:

Domain mismatch → Clear brand impersonation attempt.



2️⃣ Verify Domain Legitimacy

The email claims to be from **American Express**, but:

- Domain is not owned by American Express.
- No visible corporate domain alignment.
- Likely spoofed display name:

  "American Express" (Display Name Spoofing)

🎯 This is called:

Display Name Spoofing Attack

Where attacker shows trusted brand name but uses fake backend email.

⚠ **Red Flag:** Fake sender infrastructure.

3️⃣ Check Email Header (Technical Perspective)

Visible indicators:

- Marked as **High Importance**
- Generic structure
- No official footer verification links
- No official privacy/legal disclaimer format

In real American Express emails:

- SPF, DKIM, DMARC authentication passes
- Consistent legal footer
- Official domain hyperlinks

⚠ Likely header would show:

- Third-party SMTP relay
- Domain authentication failure

4️⃣ Inspect Embedded Links

Call-to-action button:

"Click here to review your account now"

🕵️ Problem:

- Button link not shown clearly
- Likely redirects to phishing login page
- Classic **Credential Harvesting Page**

Financial phishing emails typically:

- Clone official login page
- Capture username/password
- Capture OTP or card details

⚠ **High Risk Indicator:** Financial brand + login verification request.

5️⃣ Look for Urgency Language

Email states:

We placed a temporary suspension until you verify your account.
Review your information now.

Psychological manipulation technique:

- Account suspension threat
- Time-based urgency
- Fear trigger

This is known as:

⚡ **Account Suspension Phishing Tactic**

Designed to override rational verification.

6️⃣ Check Grammar and Content Quality

Issues noticed:

- “There's issue with your American Express account” (Missing “an”)
- Slightly unnatural phrasing
- Generic wording
- No personalization (no full name)

Legitimate financial institutions:

- Address customer by full registered name
- Include masked account numbers
- Use consistent brand formatting

⚠ Poor grammar + generic message = phishing probability high.

📌 Final Security Assessment

Based on:

- Sender domain mismatch
- Foreign unrelated domain (.cl)
- Urgency-based manipulation
- Suspicious call-to-action button
- Grammar issues
- Financial credential request

✅ This email is a **High-Risk Financial Phishing Attack**

3.1 Check Sender Email Address

Shown sender:

Lychheng.Ngor@Ins.Maersk.co.cn

🔎 Analysis:

- Official Maersk domain:
  - @maersk.com
- Here domain is:
  - maersk.co.cn

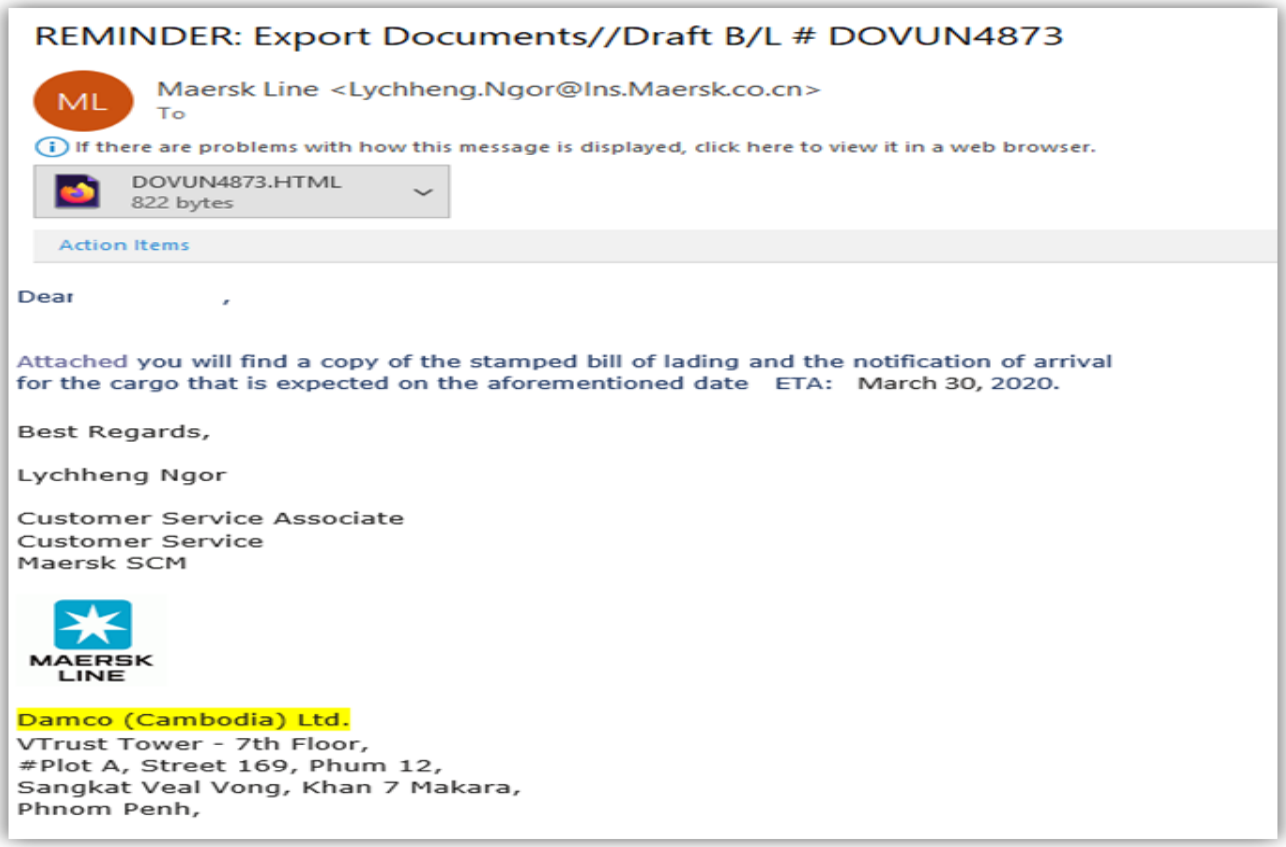
Important difference:

- .co.cn ≠ .com
- China-based secondary domain structure
- Suspicious variation of brand domain

⚠ **Red Flag:**
Brand domain look-alike (Typo squatting / Domain Variation Attack)

Attackers often:

- Add extra subdomains
- Use country-based variations
- Create similar-looking domains


REMINDER: Export Documents//Draft B/L # DOVUN4873

ML Maersk Line <Lychheng.Ngor@Ins.Maersk.co.cn>
To

If there are problems with how this message is displayed, click here to view it in a web browser.

DOVUN4873.HTML
822 bytes

Action Items

Dear ,

Attached you will find a copy of the stamped bill of lading and the notification of arrival for the cargo that is expected on the aforementioned date ETA: March 30, 2020.

Best Regards,

Lychheng Ngor

Customer Service Associate
Customer Service
Maersk SCM

MAERSK LINE

Damco (Cambodia) Ltd.
VTrust Tower - 7th Floor,
#Plot A, Street 169, Phum 12,
Sangkat Veal Vong, Khan 7 Makara,
Phnom Penh,

2️⃣ Verify Domain Legitimacy

Even if domain looks similar, we must verify:

- Is `maersk.co.cn` officially owned?
- Does it match company infrastructure?
- Is it listed in official DNS records?

In corporate BEC attacks (Business Email Compromise):

- Attackers register look-alike domains
- Impersonate shipping/logistics companies
- Send fake invoice or shipping documents

⚠ Strong suspicion of:

Business Email Compromise (BEC)

3️⃣ Check Email Header (Technical Red Flags)

Visible indicators:

- Generic subject:

  “REMINDER: Export Documents/Draft B/L”

- No personalization (Dear , ← blank)
- Minimal email body
- Attachment included

High probability header indicators:

- External mail server
- Possibly SPF/DKIM failure
- Suspicious relay path

In BEC scams:

- Header usually shows third-party SMTP relay
- Not from official corporate mail server

4️⃣ Inspect Links / Attachments

Attachment shown:

DOVUN4873.HTML

🚩 Major Red Flag:

HTML attachment in shipping email.

Why dangerous?

- HTML file can:
  - Open fake login page
  - Download malware
  - Redirect to credential harvesting site
  - Execute embedded script

Legitimate companies usually send:

- PDF
- Official secure portal link
- Digitally signed documents

⚠️ HTML attachment = High Risk Indicator

5️⃣ Look for Urgency Language

Subject contains:

“REMINDER”

Psychological trigger:

- Reminder creates mild urgency
- Business context increases trust
- Shipping ETA mentioned

Social engineering angle:

- Business professionals likely to open invoice
- Logistics sector frequently targeted

- Designed for corporate finance departments

This is typical:

📄 Invoice/Shipping Themed Phishing Attack

6 Check Grammar and Formatting

Observed issues:

- “Dear ,” (Missing recipient name)
- Very short message
- Generic closing
- Overuse of formal template style

Real corporate emails:

- Address recipient by name
- Include official tracking numbers
- Provide secure portal access
- Have structured legal footer

7 Sample Email Analysis

✉ Email 1 – Phishing (Netflix Account Suspension)

• Sender:
`info@confirm.com`

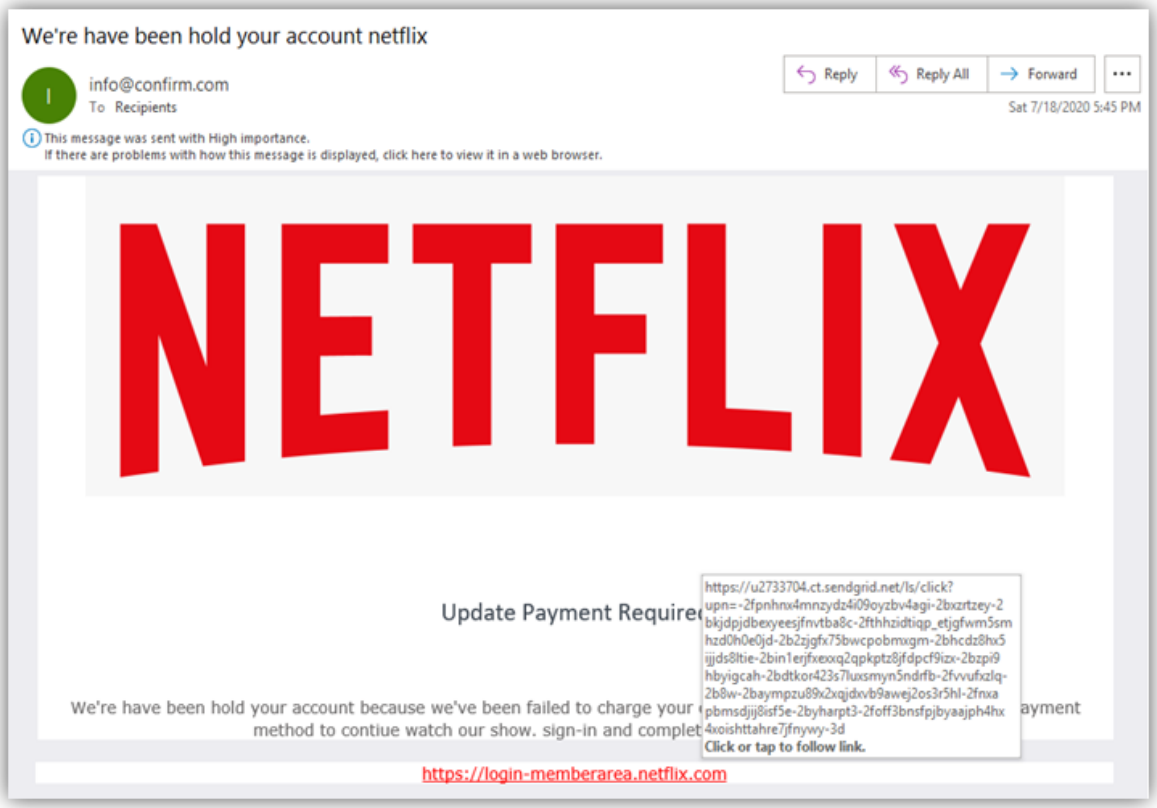
• Subject:
“We're have been hold your account netflix”

• Indicators:

- Suspicious sender domain (not netflix.com)
- Grammar mistake in subject line
- Fake login link (`login-memberarea.netflix.com`)
- Urgency related to payment failure
- Branded logo misuse
- Redirect link via third-party tracking (SendGrid)

• **Risk Level:**
🔴 High Risk

• **Reason:**
The email attempts credential harvesting by impersonating Netflix and redirecting users to a fake login portal. The sender domain does not belong to Netflix, and grammatical errors further indicate phishing intent.



✉ Email 2 – Phishing (American Express)

• **Sender:**
`administraciones@pentagon-seguridad.cl`

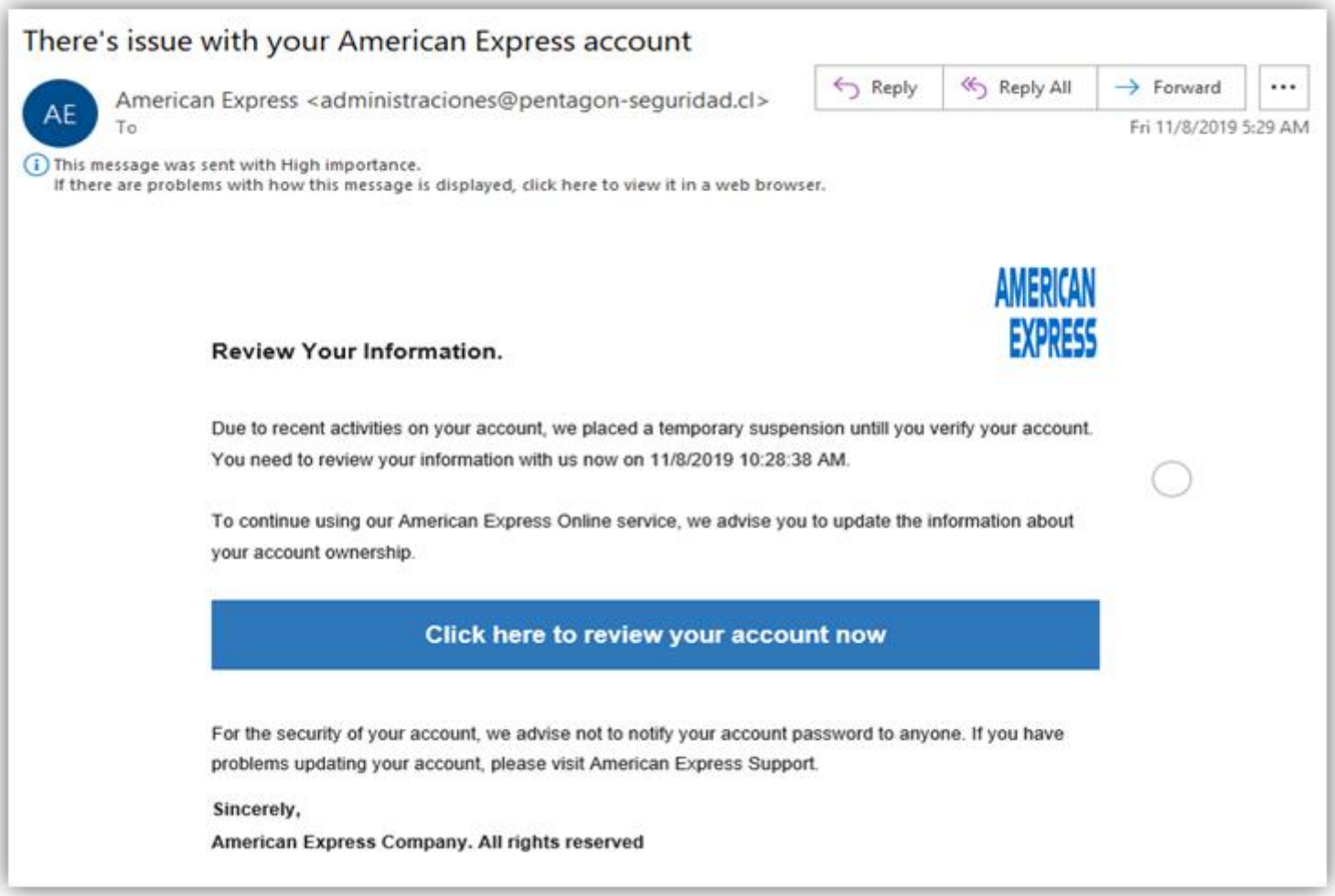
• **Subject:**
“There’s issue with your American Express account”

• **Indicators:**

- Sender domain unrelated to American Express
- Domain impersonation
- Urgency regarding account suspension
- Generic call-to-action button
- No personalization
- Financial data verification request

• **Risk Level:**
🔴 High Risk

• **Reason:**
The email impersonates American Express but originates from a suspicious domain. It attempts to trick users into verifying account information through a malicious link.



✉ Email 3 – Business Email Compromise (Maersk)

• **Sender:**
`Lychheng.Ngor@Ins.Maersk.co.cn`

• **Subject:**
“REMINDER: Export Documents/Draft B/L # DOVUN4873”

• **Indicators:**

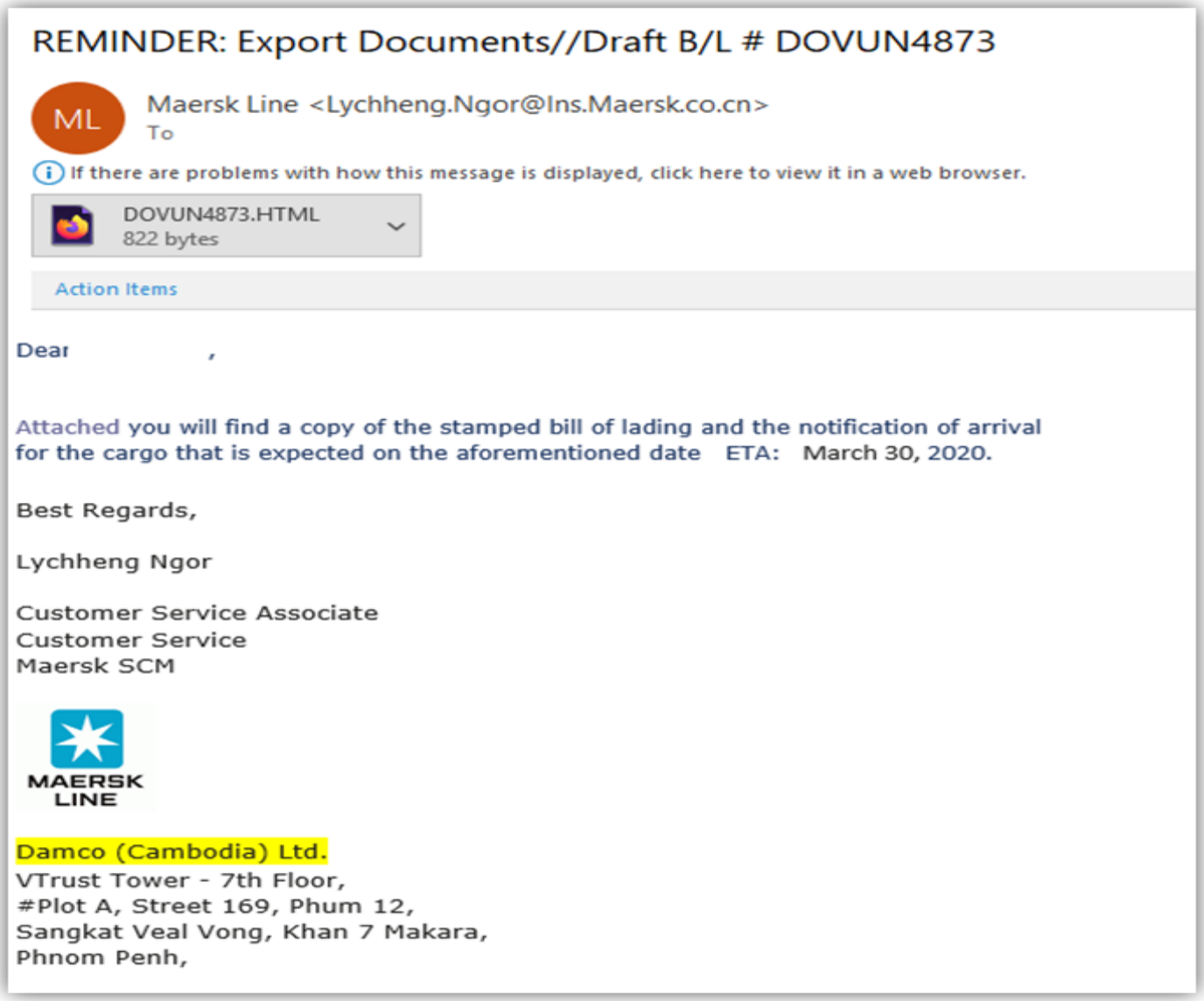
- Look-alike domain (maersk.co.cn instead of maersk.com)
- HTML attachment (DOVUN4873.HTML)
- Blank greeting (“Dear ,”)
- Business-themed urgency
- Shipping/invoice lure

• Risk Level:

High Risk

• Reason:

The email appears to be a Business Email Compromise attempt using a spoofed domain and malicious HTML attachment to deliver phishing content or malware.



✉ Email 4 – Advance Fee Scam (Google Forms Fraud)

• **Sender:**
`alhashimyreem7@gmail.com`

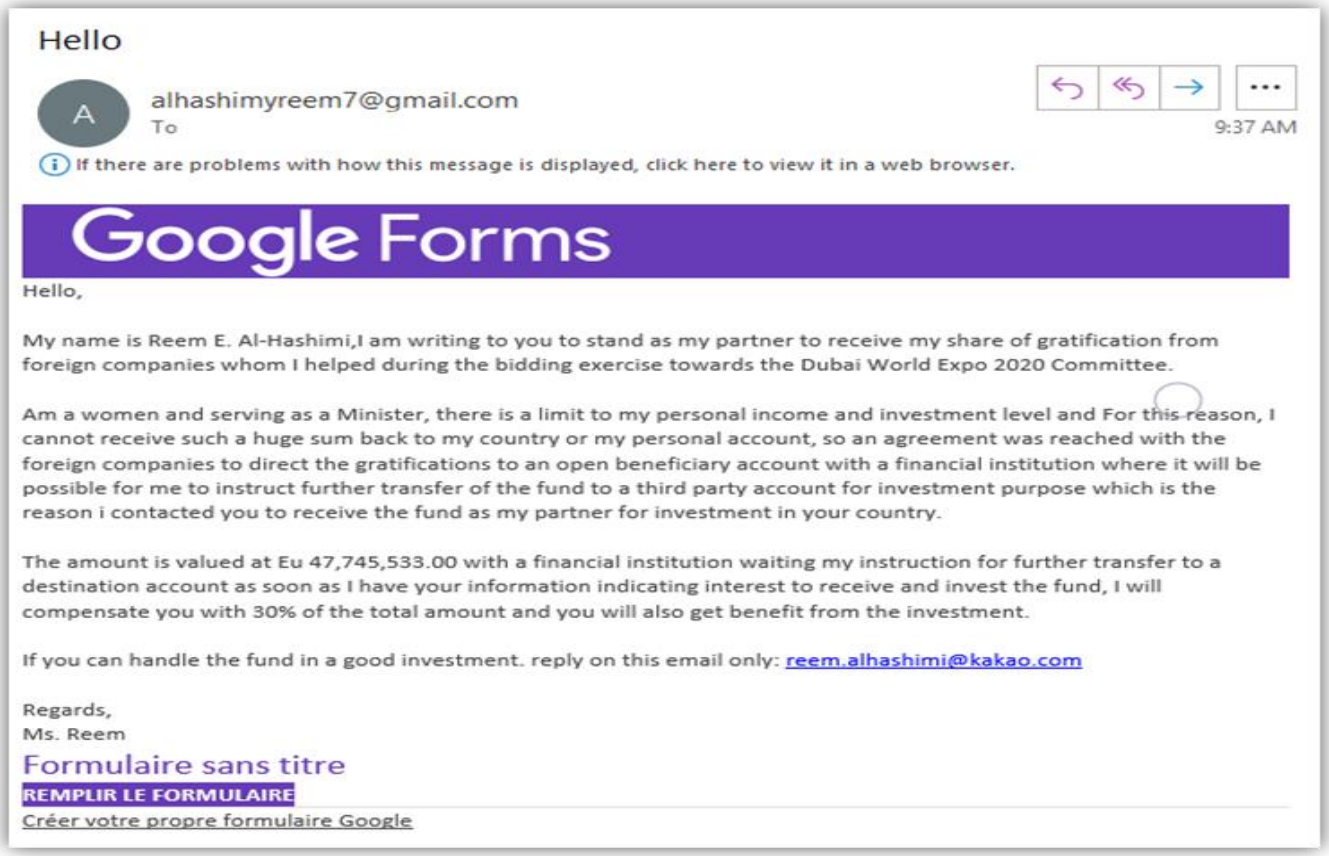
• **Subject:**
"Hello"

• **Indicators:**

- Free email service (Gmail)
- Large financial reward promise (€47 million)
- Investment partnership request
- 30% commission offer
- Unrealistic financial narrative
- Emotional manipulation

• **Risk Level:**
🔴 High Risk

• **Reason:**
This is a classic advance-fee fraud scam offering a share of large funds in exchange for cooperation, typically designed to extract money or personal information.



✉ Email 5 – Malware Delivery (Voicemail Scam)

• **Sender:**
Unknown/External Domain

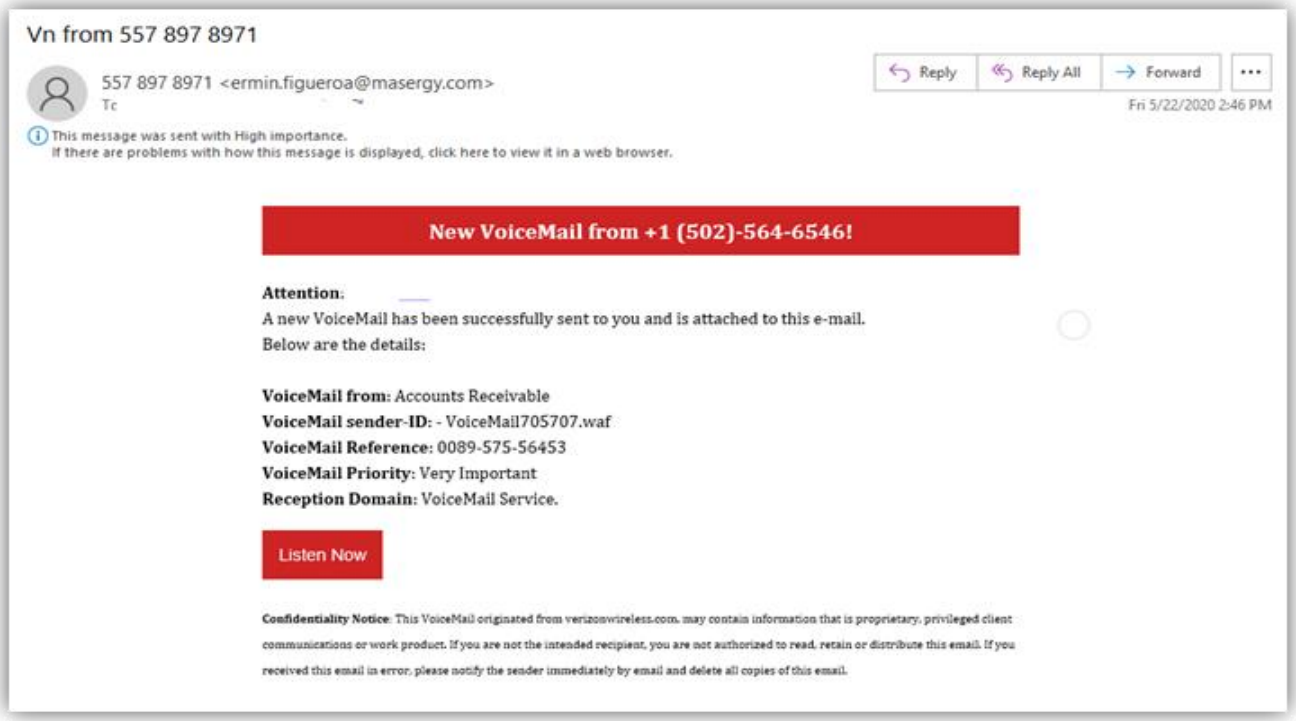
• **Subject:**
“New VoiceMail from +1 (502)-564-6546”

• **Indicators:**

- Unexpected voicemail notification
- Suspicious attachment (.wav file)
- Generic message
- No prior context
- High importance flag

• **Risk Level:**
🔴 High Risk

• **Reason:**
The email likely contains a malicious attachment disguised as voicemail audio, commonly used to distribute malware or redirect users to phishing portals.



🔎 Phishing Indicators Identified

Spoofed Domain – The sender's email domain does not match the official domain of the organization (e.g., *confirm.com* instead of *netflix.com*, *pentagon-seguridad.cl* instead of *americanexpress.com*).

Urgent Tone – The email uses urgency tactics such as account suspension, payment failure warnings, or document deadlines to pressure the recipient into taking immediate action.

Suspicious Link – The hyperlink appears to represent a legitimate brand; however, the actual URL redirects to a different or unrelated domain.

Malicious Attachment Risk – Attachments such as HTML or WAV files may contain malicious scripts or be used for credential harvesting attacks.

Grammar and Language Errors – The subject line and email body contain grammatical mistakes (e.g., "We're have been hold…", "There's issue…"), which are uncommon in legitimate corporate communications.

🔹 Low Risk

Definition:
An email or message that shows minor suspicious indicators but does not contain direct malicious links or harmful attachments.

Characteristics:

- Slight domain mismatch
- Generic greeting (e.g., "Dear User")
- Minor formatting issues
- No clickable link or attachment

Impact:
Limited immediate threat. However, it should still be reported and monitored.

Example:
Marketing-style emails from unknown domains with no active phishing payload.

◈ Medium Risk

Definition:
An email containing suspicious links or attachments but lacking strong evidence of active malware or credential harvesting.

Characteristics:

- Suspicious hyperlink redirect
- Unexpected attachment (HTML, PDF, DOC)
- Urgency language
- Brand impersonation

Impact:
Moderate risk of credential theft or malware download if the user interacts.

Example:
Fake invoice emails or document-sharing notifications.

🔴 High Risk

Definition:
An email clearly designed to steal credentials, distribute malware, or cause financial fraud.

Characteristics:

- Spoofed sender domain
- Credential harvesting login page
- Malicious attachments (HTML, executable, macro-enabled files)
- Strong urgency or threat language
- Multiple phishing indicators present

Impact:
Severe risk including:

- Account compromise
- Financial loss
- Data breach
- Malware infection

Example:
Fake Netflix / American Express login page asking for password update.

10 Impact on Organization

Phishing attacks can have serious consequences for organizations, affecting financial stability, data security, reputation, and regulatory compliance. The potential impacts include:

💰 Financial Loss

Successful phishing attacks can result in direct financial losses through fraudulent transactions, unauthorized fund transfers, or ransomware payments. In addition, organizations may incur indirect costs such as incident response expenses, system recovery costs, and business downtime.

🔐 Data Breach

Phishing often leads to unauthorized access to sensitive corporate data, including customer information, employee records, intellectual property, and financial documents. A single compromised credential can allow attackers to move laterally within systems and escalate the breach.

🏢 Reputational Damage

When customers or partners learn that an organization has suffered a phishing-related breach, trust can be significantly reduced. Loss of customer confidence may impact long-term business relationships, brand credibility, and market value.

⚖️ Legal and Regulatory Penalties

Organizations handling personal or financial data are subject to data protection regulations. A phishing-induced data breach may lead to regulatory investigations, compliance penalties, legal actions, and contractual liabilities

1️⃣ Prevention Guidelines

To reduce the risk of phishing attacks, organizations should implement the following preventive security measures:

🔐 **Enable Multi-Factor Authentication (MFA)**

📧 **Implement Advanced Email Filtering**

🎓 **Conduct Regular Security Awareness Training**

🛡️ **Configure SPF, DKIM, and DMARC**

🚫 **Avoid Clicking Unknown or Suspicious Links**

1️⃣2️⃣ Awareness Guidelines for Employees

Employees play a critical role in preventing phishing attacks, as most phishing attempts target human behavior rather than technical systems. The following awareness guidelines should be followed:

👀 **Carefully Verify the Sender**

🔍 **Hover Over Links Before Clicking**

📎 **Be Cautious with Attachments**

⏳ **Do Not React to Urgency Immediately**

🔐 **Never Share Sensitive Information**

📣 **Report Suspicious Emails Immediately**

Conclusion

The analysis of the selected email samples demonstrates how phishing attacks exploit domain spoofing, malicious links, suspicious attachments, urgency tactics, and grammatical inconsistencies to deceive users. Through structured evaluation and risk classification, it is evident that phishing remains a significant threat to both individuals and organizations. Implementing technical controls alongside continuous user awareness is essential to reduce the likelihood of successful phishing attacks and protect sensitive information.