PHISHING EMAIL DETECTION & AWARENESS SYSTEM

CYBER SECURITY INTERNSHIP PROJECT

PREPARED BY: SANJIVANI PANDEY

INTERNSHIP: FUTURE INTERNS

DOMAIN: CYBER SECURITY

DATE: 12 FEBRUARY 2026

EXECUTIVE SUMMARY

Phishing continues to represent one of the most significant and persistent cybersecurity threats to organizations globally. Unlike traditional technical attacks, phishing exploits human behavior through deception, urgency, and impersonation tactics to gain unauthorized access to sensitive information. These attacks frequently serve as the initial entry point for broader security incidents, including credential compromise, financial fraud, ransomware deployment, and data breaches.

As part of this assessment, three suspicious email samples were analyzed to evaluate their authenticity, identify phishing indicators, and determine associated risk levels. The analysis identified consistent use of social engineering techniques, including generic greetings, urgency-driven messaging, malicious or misleading hyperlinks, and suspicious sender domains. Each email demonstrated clear intent to harvest sensitive information or redirect users to fraudulent login portals.

Based on the findings, all examined samples were classified as High Risk – Phishing, with one instance exhibiting characteristics consistent with targeted spear-phishing. If interacted with, these emails could result in credential compromise, unauthorized system access, financial loss, and reputational damage to the organization.

The assessment highlights the critical importance of strengthening both human and technical defenses. While technical controls such as SPF, DKIM, DMARC, and advanced email filtering provide foundational protection, employee awareness and verification practices remain essential in mitigating phishing risks.

It is recommended that organizations implement regular phishing awareness training, enforce Multi-Factor Authentication (MFA), continuously monitor suspicious login activity, and maintain robust email authentication mechanisms. A layered security approach combining technology, policy, and user education is necessary to effectively reduce exposure to phishing-based threats.

OBJECTIVE

The objective of this engagement is to perform a structured analysis of selected suspicious email samples to determine whether they exhibit characteristics consistent with phishing or social engineering attacks.

This assessment seeks to evaluate the technical and behavioral indicators present within the emails, including sender authenticity, domain legitimacy, embedded links, and message intent. The purpose is to identify potential security risks, assess the likelihood of credential compromise or data exposure, and determine the potential operational and reputational impact to an organization if such emails were acted upon.

Additionally, this engagement aims to provide practical recommendations to strengthen email security posture, enhance user awareness, and reduce exposure to phishing-related threats.

This assessment was conducted in a controlled, read-only environment for analytical and educational purposes, without performing any active exploitation or unauthorized interaction with external systems.

SCOPE OF ASSESSMENT

This assessment was limited to the structured analysis of three selected suspicious email samples for the purpose of identifying phishing-related characteristics and evaluating associated security risks.

The scope of review included:

- Examination of email subject lines and message content
- Analysis of sender information and domain legitimacy
- Inspection of embedded hyperlinks and URL structures
- Identification of social engineering indicators
- Risk classification based on observed threat patterns

The assessment was conducted in a **read-only, non-intrusive manner**. No active exploitation, link clicking, credential submission, malware execution, or interaction with potentially malicious infrastructure was performed.

This engagement did not include:

- Live penetration testing
- Malware analysis
- Network traffic inspection
- Endpoint security evaluation
- Organizational email system configuration review

The findings presented in this report are based solely on observable indicators within the provided email samples and publicly available domain intelligence sources.

TOOLS

The following tools and resources were utilized to support the structured analysis of the selected email samples:

1️⃣ Email Header Analysis Tools

- Google Message Header Analyzer
- MXToolbox Email Header Analyzer

These tools were used to examine email routing information, sender authentication mechanisms (SPF, DKIM, DMARC), originating IP addresses, and potential spoofing indicators.

2️⃣ URL & Domain Inspection Tools

- Web Browser URL Inspection (Hover Analysis)
- WHOIS Lookup Services

These resources were used to evaluate embedded hyperlinks, verify domain registration details, assess domain legitimacy, and identify suspicious naming patterns commonly associated with phishing campaigns.

3️⃣ Open-Source Intelligence (OSINT) Techniques

Publicly available information was reviewed to validate sender authenticity and domain credibility without interacting directly with potentially malicious infrastructure.

4️⃣ Documentation & Reporting Tools

- Microsoft Word

These tools were used to structure findings in a professional, client-ready reporting format.

METHODOLOGY

This assessment was conducted using a structured, analytical approach aligned with standard cybersecurity review practices. The methodology focused on identifying phishing indicators through controlled, non-intrusive examination of selected email samples.

The process followed the stages outlined below:

1️⃣ Initial Email Review

Each email sample was reviewed to evaluate:

- Subject line language and urgency indicators
- Tone, grammar, and message structure
- Presence of social engineering techniques
- Requests for sensitive information

This step aimed to identify behavioral and psychological manipulation tactics commonly used in phishing campaigns.

2️⃣ Sender & Domain Verification

Sender email addresses and associated domains were analyzed to determine legitimacy. This included:

- Reviewing domain naming patterns
- Checking for spoofed or misleading variations
- Verifying domain registration details using WHOIS lookup
- Identifying inconsistencies between display name and actual sender address

3️⃣ URL & Link Analysis

Embedded hyperlinks were examined without direct interaction. The review included:

- Hover inspection to identify actual destination URLs
- Evaluation of domain structure and spelling anomalies
- Verification of HTTPS usage
- Identification of suspicious subdomains or redirect patterns

No links were clicked during this process.

4️⃣ Header Analysis (Where Applicable)

Where header data was available, email routing information was analyzed using header analysis tools to assess:

- Sender Policy Framework (SPF) validation
- DomainKeys Identified Mail (DKIM) status
- Domain-based Message Authentication, Reporting & Conformance (DMARC) alignment
- Originating IP address consistency

This step helped determine whether spoofing or unauthorized mail servers were involved.

5️⃣ Risk Evaluation & Classification

Based on the indicators identified, each email was classified according to risk level:

- Safe
- Suspicious
- Phishing (High Risk)

Risk classification considered the likelihood of credential compromise, financial fraud, and potential business impact.

6️⃣ Recommendation Development

Following analysis, practical and strategic recommendations were developed to strengthen both technical and human defenses against phishing threats.

Assessment Approach

The assessment was performed in a controlled, read-only environment. No active exploitation, credential submission, malware execution, or direct interaction with suspicious infrastructure was conducted.

Email Sample 1 Analysis

🔹 **Category: Generic Account Verification Phishing**

📌 **Subject:**

⚠️ Urgent: Your Account Will Be Locked

📌 **Email Body Reviewed:**

Dear User,

We noticed suspicious activity on your account.
To avoid account suspension, please verify your details immediately.

👉 Verify Now: http://secure-account-verify[.]com

Failure to verify within 24 hours will result in permanent account lock.

Regards,
Security Team

1️⃣ Overview

The email purports to notify the recipient of suspicious account activity and urges immediate verification to prevent account suspension. The message leverages urgency and fear-based language to prompt rapid user action.

Upon structured analysis, multiple indicators consistent with phishing activity were identified.

2️⃣ Identified Phishing Indicators

🔹 **Generic Greeting**

The use of “Dear User” indicates lack of personalization. Legitimate service providers typically address customers by their registered name.

🔹 **Urgency & Threat-Based Language**

The message imposes a 24-hour deadline and threatens permanent account lock. Such time-sensitive pressure is a common social engineering tactic designed to bypass rational verification.

🔹 **Suspicious Domain**

The embedded link:

http://secure-account-verify[.]com

does not correspond to any identifiable legitimate organization. The domain structure appears artificially constructed to mimic a security-related service.

🔹 **Non-Secure HTTP Protocol**

The use of "http" instead of "https" suggests absence of encryption, which is highly unusual for legitimate account verification portals.

🔹 **Lack of Organizational Identification**

The email does not specify:

- Company name
- Official contact details
- Customer support information
- Reference or ticket number

This absence reduces credibility and is consistent with phishing attempts.

3️⃣ Technical Risk Assessment

The embedded URL strongly indicates potential redirection to a fraudulent credential harvesting page. If a user were to input login information, the attacker could gain unauthorized access to the victim's account.

Potential consequences include:

- Credential compromise

- Unauthorized account access
- Financial fraud
- Identity theft
- Lateral movement within organizational systems

🛂 Risk Classification

Risk Level: High
Classification: Confirmed Phishing Attempt

The combination of urgency tactics, suspicious domain, non-secure protocol, and lack of legitimate identifiers clearly categorizes this email as a phishing attack.

EMAIL SAMPLE 2 ANALYSIS

🔹 **Category: Brand Impersonation Phishing**

📌 Subject:

Security Alert: Suspicious Login Attempt Detected

📌 Email Body Reviewed:

Dear Customer,

We detected a suspicious login attempt on your PayPal account from an unknown device.

For your protection, your account has been temporarily limited.

To restore full access, please confirm your identity immediately:

👉 http://paypal-account-verification[.]com

If no action is taken within 24 hours, your account may be permanently suspended.

Thank you,
PayPal Security Team

1️⃣ Overview

This email attempts to impersonate PayPal by notifying the recipient of a suspicious login attempt and temporary account limitation. The message creates urgency by implying potential permanent suspension if immediate action is not taken.

The structure, tone, and link analysis reveal multiple high-confidence phishing indicators.

2️⃣ Identified Phishing Indicators

🔹 Brand Impersonation

The email falsely claims to represent PayPal. However, the sender domain and embedded link do not correspond to the official PayPal domain (paypal.com). Brand impersonation is a common tactic used to exploit user trust.

🔹 Generic Greeting

The use of "Dear Customer" instead of the recipient's registered name indicates lack of personalization, which is typical in bulk phishing campaigns.

🔹 Fear & Urgency Tactics

The message references:

- Suspicious login activity
- Account limitation
- 24-hour deadline
- Potential permanent suspension

These elements are designed to induce panic and encourage immediate, unverified action.

🔹 Suspicious Domain Structure

The embedded link:

http://paypal-account-verification[.]com

This domain:

- Is not an official PayPal domain
- Uses keyword stuffing ("paypal", "account", "verification") to appear legitimate
- Is likely registered solely for phishing purposes

Legitimate PayPal URLs always resolve to domains ending in paypal.com.

🔹 Use of HTTP Instead of HTTPS

The link uses “http” rather than “https,” which is inconsistent with legitimate financial service providers that enforce encrypted connections.

3️⃣ Technical Risk Assessment

The structure of the URL strongly indicates a credential harvesting attempt. Users clicking the link would likely be redirected to a fraudulent login page designed to mimic PayPal’s official interface.

If credentials are entered, potential consequences include:

- Unauthorized PayPal account access
- Financial theft or fraudulent transactions
- Linked bank or card compromise
- Account takeover
- Secondary attacks using stolen credentials

Given the financial nature of the impersonated service, the potential impact is significant.

4️⃣ Risk Classification

Risk Level: High
Classification: Confirmed Phishing – Brand Impersonation

The presence of brand spoofing, urgency tactics, misleading domain construction, and potential credential harvesting clearly categorizes this email as a high-risk phishing attempt.

Email Sample 3 Analysis

🔹 **Category: Financial Institution Phishing Attempt**

📌 **Subject:**

Important Notice: Your Bank Account Has Been Restricted

📌 **Sender:**

Customer Support alerts@secure-bank-update.com

📌 **Email Body Reviewed:**

Dear Valued Customer,

Due to unusual activity detected on your bank account, we have temporarily restricted online transactions.

To avoid permanent account freeze, please verify your account information immediately.

Click below to secure your account:

👉 http://secure-bank-login-verification[.]com

Failure to complete verification within 12 hours may result in account suspension.

Sincerely,
Banking Security Department

1️⃣ Overview

This email impersonates a financial institution and claims that the recipient's bank account has been restricted due to unusual activity. The message pressures the recipient to verify account information within a 12-hour timeframe to prevent permanent suspension.

The structure and technical indicators strongly align with high-risk financial phishing campaigns.

2️⃣ Identified Phishing Indicators

- Suspicious Sender Domain

The sender email address:

alerts@secure-bank-update.com

This domain does not correspond to any identifiable legitimate banking institution. The naming pattern (“secure-bank-update”) appears artificially constructed to mimic official banking communication.

Legitimate banks use verified corporate domains and do not operate through generic keyword-based domains.

- Generic Greeting

The use of “Dear Valued Customer” indicates bulk distribution. Financial institutions typically address customers by full name and often reference partial account numbers for legitimacy.

- Severe Urgency & Reduced Timeframe

Unlike previous samples (24 hours), this email imposes a 12-hour deadline, significantly increasing psychological pressure. Shortened response windows are a common tactic used to bypass rational decision-making.

- Suspicious Embedded Link

http://secure-bank-login-verification[.]com

Indicators include:

Non-official banking domain

Keyword-stuffed naming pattern

Use of HTTP (unencrypted connection)

Likely redirection to a credential harvesting page

No legitimate bank would request sensitive verification through an unsecured third-party domain.

🔹 Request for Sensitive Information

The email explicitly requests verification of "account information," which may include:

Online banking credentials

Card details

One-time passwords (OTP)

Personal identification data

This behavior is consistent with credential harvesting attacks.

3️⃣ Technical Risk Assessment

Given the financial context, this phishing attempt poses a critical financial risk. If a user submits banking credentials, potential impact may include:

- Unauthorized bank transfers
- Account takeover
- Identity theft
- Fraudulent transactions
- Long-term financial compromise

Additionally, stolen banking credentials are often sold on dark web marketplaces or used for further targeted attacks.

4️⃣ Risk Classification

Risk Level: Critical / High
Classification: Confirmed Financial Phishing Attempt

Due to impersonation of a financial institution, shortened response deadline, suspicious sender domain, and credential harvesting indicators, this email presents a severe risk to individuals and organizations.

PHISHING INDICATORS SUMMARY TABLE

The following table summarizes the key phishing indicators identified across the three analyzed email samples:

Phishing Indicator	**Email Sample 1**	**Email Sample 2**	**Email Sample 3**
Generic Greeting	✓	✓	✓
Urgency / Time Pressure	24 Hours	24 Hours	12 Hours
Threat of Account Suspension	✓	✓	✓
Suspicious Sender Domain	✓	✓	✓
Brand Impersonation	✗	✓ (PayPal)	✓ (Bank)
Financial Context	✗	✓	✓
Suspicious Embedded Link	✓	✓	✓
Non-HTTPS Link	✓	✓	✓
Keyword-Stuffed Domain	✓	✓	✓
Request for Sensitive Information	✓	✓	✓
Lack of Official Branding Details	✓	✓	✓

● Indicator Severity Observation:-

Email Sample 1 demonstrates characteristics of generic mass phishing.

Email Sample 2 introduces brand impersonation, increasing credibility and financial risk.

Email Sample 3 presents the highest potential impact due to banking impersonation and reduced response timeframe (12 hours), indicating elevated urgency pressure.

🟣 Overall Pattern Identified

Across all samples, consistent phishing traits were observed:

- Psychological manipulation through urgency
- Credential harvesting attempts
- Domain spoofing techniques
- Absence of legitimate verification mechanisms
- Lack of personalized or verifiable sender information

This pattern confirms a coordinated social engineering approach rather than isolated suspicious communication.

Risk Classification Summary

Based on structured analysis of the three email samples, each message was evaluated against phishing indicators, likelihood of credential compromise, financial impact potential, and social engineering intensity.

📊 Risk Rating Overview

Email Sample	Category	Likelihood of Exploitation	Business Impact	Overall Risk Level
Sample 1	Generic Credential Phishing	High	Moderate	**High**
Sample 2	Brand Impersonation (PayPal)	High	High	**High**
Sample 3	Banking Phishing	Very High	Critical	**Critical**

🟣 Risk Evaluation Criteria

Risk levels were determined based on:

- Presence of social engineering tactics
- Brand impersonation severity
- Financial targeting
- Credential harvesting likelihood
- Potential operational and reputational impact

🟣 Risk Analysis Observations

🔹 Email Sample 1 – High Risk

Although generic in nature, the email clearly attempts credential harvesting using urgency tactics. Successful exploitation could result in unauthorized account access.

🔹 Email Sample 2 – High Risk

Brand impersonation increases credibility and trust exploitation. Given the financial service context, the potential impact includes direct financial loss and account takeover.

🔹 Email Sample 3 – Critical Risk

This email represents the highest risk due to:

- Banking impersonation
- Direct financial targeting
- Reduced response timeframe (12 hours)
- High probability of credential compromise

Successful exploitation could result in severe financial loss, identity theft, and regulatory implications.

🟣 Overall Risk Conclusion

All analyzed emails demonstrate strong phishing characteristics and pose significant security risks. The consistent use of urgency, impersonation, and suspicious domains indicates deliberate social engineering strategy.

Immediate reporting and user awareness are essential to prevent successful exploitation.

PREVENTION GUIDELINES

Based on the findings of this assessment, the following preventive measures are recommended to mitigate phishing-related risks and strengthen overall email security posture.

Phishing attacks rely heavily on human interaction and weak verification practices. Therefore, a layered security approach combining technical, administrative, and behavioral controls is essential.

1️⃣ Technical Security Controls

To reduce the likelihood of phishing emails reaching end users:

Implement and enforce **SPF, DKIM, and DMARC** email authentication protocols.

Deploy advanced **email filtering and anti-phishing solutions**.

Enable **Multi-Factor Authentication (MFA)** across all user accounts.

Enforce secure browsing policies and URL filtering.

Monitor abnormal login activity and suspicious IP addresses.

Regularly update endpoint protection and security patches.

These controls help prevent spoofed emails, unauthorized access, and credential compromise.

2️⃣ Administrative & Policy Controls

Organizations should establish structured internal controls, including:

Defined procedure for reporting suspicious emails.

Periodic phishing simulation exercises.

Clear escalation process for suspected security incidents.

Strong password policy enforcement.

Restricted administrative privileges based on role.

Formal security governance reduces response time and impact.

3️⃣ User Awareness & Behavioral Controls

Since phishing primarily targets human psychology, user education is critical:

Conduct regular cybersecurity awareness training.

Educate employees on identifying urgency tactics and impersonation attempts.

Encourage a “verify before you trust” culture.

Promote immediate reporting of suspicious emails without fear of penalty.

An informed workforce significantly lowers the success rate of phishing campaigns.

🟣 Preventive Strategy Summary

Effective phishing mitigation requires a multi-layered defense strategy combining:

Technology

Process

People

Organizations that integrate technical controls with continuous user education demonstrate significantly higher resilience against social engineering attacks.

DO'S AND DON'TS FOR EMPLOYEES

Email Security & Phishing Protection Guidelines:-

Phishing attacks target employees as the primary entry point into organizational systems. Every employee plays a critical role in protecting company data, financial assets, and customer information. The following behavioral guidelines must be followed when handling emails.

✅ Do's

1️⃣ Verify Before You Trust

Always verify the sender's full email address — not just the display name. Be cautious of slight spelling variations in domains.

2️⃣ Inspect Links Before Clicking

Hover over hyperlinks to review the actual destination URL. Ensure it matches the legitimate organization's official domain.

3️⃣ Report Suspicious Emails Immediately

If an email appears suspicious, report it to the IT or Security Team using the organization's defined reporting procedure. Early reporting prevents wider impact.

4️⃣ Confirm Sensitive Requests Through Official Channels

For financial transfers, payroll changes, password resets, or account verification requests, confirm through official company contact methods (phone or verified internal systems).

5️⃣ Use Multi-Factor Authentication (MFA)

Ensure MFA is enabled and never approve login requests you did not initiate.

6️⃣ Maintain Credential Confidentiality

Keep passwords, OTPs, banking details, and access credentials strictly confidential. Follow company password policy requirements.

7️⃣ Stay Security-Aware

Participate in periodic cybersecurity training and phishing simulation exercises to remain updated on evolving attack techniques.

❌ Don’ts

1️⃣ Do Not Click Unknown or Suspicious Links

Avoid clicking links from unverified senders, especially those creating urgency or requesting sensitive information.

2️⃣ Do Not Download Unexpected Attachments

Attachments may contain malware or ransomware. Verify with the sender before opening.

3️⃣ Do Not Share Credentials via Email

Legitimate organizations will never request passwords, OTPs, or confidential data through email.

4️⃣ Do Not Act Under Pressure

Phishing emails often create artificial urgency (e.g., “12 hours left”). Take time to verify before responding.

5️⃣ Do Not Trust Branding Alone

Logos and company names can be easily replicated. Always validate domain authenticity.

6️⃣ Do Not Ignore Security Alerts

If you suspect phishing, do not delete the email silently — report it to prevent organizational exposure.

🔐 Employee Responsibility Statement

Cybersecurity is a shared responsibility. Human vigilance is the first line of defense against phishing and social engineering attacks. Adhering to these guidelines significantly reduces the risk of credential compromise, financial loss, and reputational damage to the organization.

CONCLUSION

The structured analysis of the three selected email samples confirms the presence of clear and consistent phishing indicators aligned with modern social engineering attack methodologies. Each email demonstrated deliberate manipulation techniques designed to exploit user trust, induce urgency, and harvest sensitive credentials.

The progression from generic account verification phishing (Sample 1) to brand impersonation (Sample 2) and financial institution targeting (Sample 3) illustrates increasing levels of potential business impact. In particular, the banking-themed phishing email represents a critical threat due to its direct financial implications and heightened urgency tactics.

Phishing attacks remain highly effective because they target human behavior rather than system vulnerabilities. Even organizations with strong technical defenses remain exposed if users are not adequately trained to identify and report suspicious communications.

To mitigate phishing-related risks, a layered security strategy is essential. This includes:

- Implementation of email authentication standards (SPF, DKIM, DMARC)
- Enforcement of Multi-Factor Authentication (MFA)
- Continuous monitoring of suspicious login activity
- Regular phishing awareness training programs
- Clear internal reporting procedures

Proactive investment in both technical controls and user education significantly reduces organizational exposure to phishing attacks and enhances overall cybersecurity resilience.

In conclusion, the analyzed emails represent high to critical risk threats. Strengthening preventive controls and fostering a culture of security awareness are imperative to safeguarding sensitive information and maintaining operational integrity.

DISCLAIMER

This report has been prepared as part of a cybersecurity internship project for educational and analytical purposes. The assessment was conducted in a controlled, read-only environment using publicly available sample emails and open-source analysis techniques.

No active exploitation, unauthorized access, credential submission, malware execution, or interaction with live production systems was performed during the course of this assessment. All analysis was limited strictly to observable email content, sender information, and non-intrusive link and domain evaluation.

The findings, risk classifications, and recommendations provided in this report are based solely on the reviewed samples and are intended for awareness, training, and informational purposes only. This document does not constitute a full security audit, penetration test, or comprehensive organizational security assessment.

Any resemblance to actual organizations, domains, or systems is purely coincidental and used only for illustrative analysis. The author assumes no liability for misuse of the information contained within this report.

This document is intended solely for academic evaluation and authorized review.