Phishing Email Detection & Awareness Report

Prepared By: Adarsh Dipak Gurav
Prepared for: Future Interns
Date: 16 February 2026

1 Collection of Phishing Samples

This report documents the detailed analysis of five intercepted phishing email samples. These samples represent a diverse array of attack vectors targeting both enterprise environments and personal consumer accounts. The collected samples include HR/Payroll impersonation, consumer streaming service spoofing, Executive Fraud (BEC), malware dropping via fake invoices, and enterprise cloud document credential harvesting.

Analysis Findings

The following sections break down each intercepted sample based on header intelligence, domain inspection, psychological indicators, and overall risk classification.

Sample 1: The HR/Payroll Phish (Urgent Policy)

2 Email Header Analysis

From: HR Department <hr-update@company-bamboohr-portal[.]com>

To: Employee <employee@company[.]com>

Subject: ACTION REQUIRED: Q3 Bonus & Policy Acknowledgement

Date: Fri, 13 Feb 2026 09:15:00 +0530

Email Body Transcript

> ***Dear Employee,***
>
> ***Please review the attached addendum to the 2026 Employee Handbook regarding changes to the Q3 bonus structure and remote work policies.***
>
> ***You are required to review and digitally sign this document by the end of the day to ensure there are no disruptions to your upcoming payroll cycle.***
>
> ***Access your secure document here:***
> ***hxxps://employee-portal[.]company-bamboohr-portal[.]com/login***
>
> ***Thank you,***
> ***Human Resources***

3 Domain & Payload Inspection

hxxps://employee-portal[.]company-bamboohr-portal[.]com/login

4 Identified Phishing Indicators

- Relies heavily on organizational authority (HR) to force compliance.
- Exploits employee anxiety regarding compensation (Q3 Bonus) and employment status.
- Creates an artificial time constraint ('by the end of the day').
- Threatens negative consequences ('disruptions to your upcoming payroll cycle').

5 Risk Classification

Risk Level: HIGH

Classification Details: Credential Harvesting / Enterprise Access. The attacker aims to steal employee portal credentials, which could lead to lateral movement within the corporate network.

Sample 2: The Streaming Service Phish (Panic/Account Loss)

2 Email Header Analysis

From: Netflix Billing <support@netfiix-billing-update[.]com>

To: Subscriber <victim@yahoo[.]com>

Subject: Payment Declined: Your Netflix Account is Suspended

Date: Fri, 13 Feb 2026 14:05:10 +0530

Email Body Transcript

> ***Hi there,***
>
> ***We are having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.***
>
> ***Your account has been temporarily suspended until this issue is resolved.***
>
> ***Update your payment details now to restore your access: hxxps://account-update[.]netfiix-billing-update[.]com/login***
>
> ***Need help? We're here if you need it. Visit the Help Centre or contact us now.***
>
> ***-Your friends at Netflix***

3 Domain & Payload Inspection

hxxps://account-update[.]netfiix-billing-update[.]com/login

4 Identified Phishing Indicators

- Uses a 'homoglyph' typo-squatting domain in the sender email ('netfiix' instead of 'netflix').
- Attacks the user's personal life by threatening the loss of a paid entertainment service.
- Creates panic and an artificial sense of urgency claiming the account is already 'suspended'.

5 Risk Classification

Risk Level: MEDIUM

Classification Details: Personal Financial Fraud. Designed to harvest consumer credit card details and personal billing information.

Sample 3: The Executive Fraud / BEC (Spear-Phishing)

2 Email Header Analysis

From: John Smith (CEO) <john.smith.ceo.exec882@gmail[.]com>

To: Jane Doe (Finance Manager) <jane.doe@company[.]com>

Subject: Are you available? (Urgent Request)

Date: Fri, 13 Feb 2026 16:45:00 +0530

Email Body Transcript

> ***Jane,***
>
> ***Are you at your desk? I am currently in a board meeting and cannot take any calls, but I need you to handle a quick task for me regarding client gifts.***
>
> ***Let me know as soon as you get this so I can send you the instructions. I need this done in the next 30 minutes.***
>
> ***Sent from my iPhone***
> ***John Smith***
> ***CEO, Company Inc.***

---

3 Domain & Payload Inspection

No explicit URLs. Relies purely on social engineering dialogue.

4 Identified Phishing Indicators

- Spoofs a person of high authority (CEO).
- Originates from a free, external webmail address (gmail[.]com) rather than the corporate domain.
- Preemptively cuts off verification channels ('in a board meeting and cannot take any calls').
- Demands extreme urgency ('next 30 minutes') for financial tasks ('client gifts/wire transfers').

5 Risk Classification

Risk Level: CRITICAL

Classification Details: Business Email Compromise (BEC). Highly targeted attack aiming for direct, unrecoverable financial loss via unauthorized wire transfers or gift card purchases.

Sample 4: The Fake Invoice (Malware Dropper)

2 Email Header Analysis

From: Accounts Receivable <billing@vendor-finance-llc[.]com>

To: Accounts Payable <ap@company[.]com>

Subject: OVERDUE INVOICE #90210 - Immediate Payment Required

Date: Fri, 13 Feb 2026 08:00:15 +0530

Email Body Transcript

> *To the Accounts Payable Team,*
>
> *Attached is the overdue invoice #90210 for the services rendered last month. This is our third attempt to contact you regarding this balance.*
>
> *Please note that our banking details have recently changed. Open the attached invoice to view the new wire routing instructions and the itemized list of charges.*
>
> *If payment is not received by Monday, a 5% late fee will be applied to the account.*
>
> *Regards,*
> *Sarah Jenkins*
> *Billing Coordinator*

---

3 Domain & Payload Inspection

Attachment: Invoice_90210_Overdue.xls (124 KB)

4 Identified Phishing Indicators

- Specifically targets the accounting/finance department.
- Contains a suspicious attachment (.xls) rather than a secure payment portal link.
- Mentions 'banking details have recently changed', a classic indicator of payment diversion fraud.
- Applies financial pressure ('5% late fee').

5 Risk Classification

Risk Level: CRITICAL

Classification Details: Malware / Ransomware Dropper. The macro-enabled Excel file is likely designed to execute malicious code upon opening, compromising the endpoint.

Sample 5: The Cloud Document Share (Credential Harvesting)

2 Email Header Analysis

From: Microsoft SharePoint <no-reply@sharepoint-document-vault[.]com>

To: Employee <employee@company[.]com>

Subject: "Project_Alpha_Q4_Financials.pdf" has been shared with you

Date: Fri, 13 Feb 2026 10:22:40 +0530

Email Body Transcript

> ***SharePoint Online***
>
> ***External Partner (partner@external-firm[.]com) has shared a secure document with you.***
>
> ***File: Project_Alpha_Q4_Financials.pdf***
> ***Size: 2.4 MB***
> ***Permissions: View and Edit***
>
> ***This link will work for anyone in your organization. You will need to verify your identity to access this secure file.***
>
> ***Open Document: hxxps://login[.]microsoftonline-secure-auth[.]com/verify***
>
> ***Microsoft Corporation, One Microsoft Way, Redmond, WA 98052***

---

3 Domain & Payload Inspection

hxxps://login[.]microsoftonline-secure-auth[.]com/verify

4 Identified Phishing Indicators

- Fakes a legitimate, highly recognizable enterprise workflow (Microsoft SharePoint document sharing).
- Uses a highly deceptive look-alike domain for the sender ('sharepoint-document-vault[.]com').
- Prompts the user to 'verify your identity', leading to a fake Microsoft 365 login page.
- Uses an enticing, confidential-sounding file name ('Project_Alpha_Q4_Financials.pdf').

5 Risk Classification

Risk Level: HIGH

Classification Details: Enterprise Credential Theft. Designed to steal Microsoft 365 or Google Workspace credentials to gain full access to corporate emails and files.

7 Prevention & Awareness Guidelines

Based on the analysis of the above samples, the following actionable guidelines should be distributed to all staff:

Verify Sender Identity: Always expand the sender's details to view the actual email address, not just the display name. Be highly suspicious of 'homoglyphs' (e.g., netfiix vs netflix) and free webmail accounts (Gmail/Yahoo) claiming to be executives.

Neutralize Urgency: Cybercriminals manufacture panic. If an email threatens account deletion, payroll disruption, or demands a wire transfer within 30 minutes, stop. Do not click. Verify the request through a secondary channel (e.g., call the HR department or the CEO directly).

Inspect URLs Before Clicking: Hover your mouse over any 'Secure Document' or 'Update Payment' buttons. If the destination URL does not exactly match the official corporate domain, close the email.

Beware of the 'Changed Banking Details' Ploy: Any invoice claiming that routing numbers or banking details have changed must be treated as hostile until verified by a phone call to a known contact at the vendor.

Treat Attachments as Toxic: Never open unexpected .xls, .doc, or .zip files, especially those from external sources claiming to be invoices. These often contain macro-based malware or ransomware droppers.

Report, Don't Just Delete: If you spot a phishing attempt, use the organization's 'Report Phishing' tool. Deleting it protects you, but reporting it allows the SOC team to scrub the threat from the rest of the company's inboxes.