THINK BEFORE YOU CLICK

PHISHING DETECTION & AWARENESS REPORT

PRESENTED BY- ANSHIKA SINGH

DATE- 13/02/2026

Phishing Detection & Awareness Report

This report presents a structured analysis of a sample phishing email and provides awareness guidance to help individuals and organizations recognize and prevent phishing attacks. Phishing is one of the most widespread cyber threats, targeting users through deceptive communication rather than technical vulnerabilities. Attackers impersonate trusted entities to manipulate recipients into revealing confidential information or clicking malicious links.

The purpose of this report is to identify phishing indicators present in a sample email, analyze technical and behavioral warning signs, classify the level of risk, and explain how such attacks operate. The report also provides practical recommendations for prevention and employee awareness to reduce the likelihood of successful phishing attempts.

The analysis reveals multiple red flags, including urgency-based messaging, a suspicious verification link, and a generic greeting. These indicators strongly suggest a high-risk phishing attempt designed to steal user credentials.

Based on the findings, the email is classified as malicious. Users are advised not to interact with similar messages and to report suspicious communications immediately.

This report highlights the importance of cybersecurity awareness and demonstrates how informed users play a critical role in protecting organizational systems and sensitive information

INTRODUCTION

Phishing is a form of cybercrime that uses deception to trick individuals into revealing sensitive information such as usernames, passwords, financial details, or personal data. Unlike technical hacking methods that exploit software vulnerabilities, phishing attacks exploit human trust and psychological response. Attackers send fraudulent emails that appear legitimate, often impersonating well-known organizations, service providers, or internal departments.

These emails typically create urgency, fear, or curiosity to prompt immediate action. Common tactics include account suspension warnings, security alerts, payment requests, or verification requirements. When users click malicious links or provide information, attackers gain unauthorized access to accounts or systems.

The increasing reliance on email communication makes phishing a major security concern for organizations worldwide. Even well-protected systems can be compromised if users are deceived.

This report analyzes a sample phishing email to demonstrate how such attacks are structured and how they can be identified. The analysis focuses on message content, technical indicators, and behavioral manipulation techniques.

The goal is to improve awareness and provide practical strategies for prevention. Understanding phishing tactics is essential for reducing security risks and protecting digital assets in both personal and professional environments.

OBJECTIVES OF THE STUDY

The primary objective of this study is to analyze a sample phishing email and identify the characteristics that distinguish it from legitimate communication. By examining both technical and psychological indicators, this report aims to provide a clear understanding of how phishing attempts operate.

One key objective is to detect common phishing warning signs such as suspicious links, urgency-based language, generic greetings, and unverifiable sender details. Identifying these indicators helps users recognize threats before interacting with malicious content.

Another objective is to evaluate the level of risk associated with the email. Classifying emails as safe, suspicious, or phishing allows organizations to respond appropriately and implement preventive measures.

This study also aims to explain the phishing process in simple, non-technical language so that users without cybersecurity expertise can understand how attackers manipulate victims.

Additionally, the report seeks to develop practical awareness guidelines, including prevention tips and recommended employee behavior when handling suspicious emails.

Overall, the goal is not only to detect phishing but also to strengthen user awareness and promote safer digital practices that reduce the likelihood of successful cyberattacks.

Evidences

There's issue with your American Express account

AE

American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

Reply | Reply All | Forward | ...

Fri 11/8/2019 5:29 AM

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

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)
to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

Overview of the Sample Phishing Email

The uploaded screenshots present three different examples of phishing emails that impersonate trusted institutions to manipulate recipients into taking immediate action. Each email uses a different theme to appeal to specific emotions or situations. The first email claims to be from a university IT department warning that the user's password will expire within 24 hours. It urges the recipient to click a link to renew credentials, creating urgency and authority. The second email appears to come from a Human Resources department informing the recipient about a salary raise and requesting access to attached or linked documents. This message exploits curiosity and financial motivation. The third email impersonates American Express and claims suspicious account activity, pressuring the recipient to verify account details immediately.

Although the emails appear professional and include logos, formal language, and structured formatting, they share a common objective: to trick users into clicking malicious links or providing sensitive information. These emails demonstrate common phishing strategies such as impersonation, urgency, emotional manipulation, and deceptive hyperlinks. By mimicking legitimate communication channels, attackers attempt to bypass user suspicion and gain unauthorized access to personal or financial data. Understanding these patterns is essential for identifying and preventing phishing attacks.

Identification of Phishing Indicators

Several warning signs clearly indicate that the uploaded emails are phishing attempts rather than legitimate communications. One of the most prominent indicators is the use of urgency. Messages stating that passwords will expire soon or accounts will be suspended force users to act quickly without verifying authenticity. This psychological pressure is a common tactic used by attackers to prevent rational decision-making.

Another indicator is suspicious sender information. Even when the display name appears legitimate, the actual email address may belong to an unrelated or unusual domain. This mismatch between identity and domain is a strong sign of spoofing. Additionally, generic greetings such as “Dear network user” or “Hello” instead of personalized names suggest mass distribution rather than official communication.

Unsolicited offers or unexpected notifications are also warning signs. For example, a sudden salary raise announcement or urgent financial verification request should raise suspicion if not previously communicated through official channels.

The presence of embedded links encouraging credential entry or document downloads is another key indicator. Attackers often disguise malicious links with legitimate-looking text.

Finally, subtle grammar inconsistencies, unusual formatting, or overly formal tone can signal phishing. Collectively, these indicators demonstrate manipulation, impersonation, and deception typical of phishing attacks.

Email Header Analysis

Email header analysis is an essential step in determining whether an email is authentic or malicious. The header contains technical information about the sender, routing path, and authentication results. In phishing emails like the ones shown, header details often reveal inconsistencies not visible in the main message body.

One common issue is sender spoofing. The displayed sender name may appear legitimate, such as a university or financial institution, but the underlying email address may originate from an unrelated or suspicious domain. This mismatch is a major red flag. Attackers frequently manipulate the “From” field to imitate trusted organizations while sending messages from external or compromised servers.

Authentication failures may also appear in the header. Email systems often include SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC verification results. If these fail or are missing, the email may not be authorized by the claimed sender’s domain.

Another important factor is the message routing path. Unexpected or foreign mail servers in the transmission chain may indicate suspicious activity.

Time stamps that do not align with expected time zones or unusual sending patterns can also raise suspicion. By carefully examining header metadata, users and security professionals can identify technical evidence of phishing that may not be obvious from visual inspection alone.

Link and Domain Investigation

Investigating links and domains is one of the most effective ways to detect phishing emails. In the uploaded examples, each email contains a clickable link prompting the recipient to take action, such as renewing a password, accessing documents, or verifying financial information. These links are often disguised to appear legitimate but may redirect users to fraudulent websites designed to steal credentials.

A key step in link investigation is hovering over the hyperlink to view the actual destination URL. Phishing links often contain subtle variations of official domain names, such as misspellings, extra characters, or unrelated domain extensions. For example, attackers may use lookalike domains that visually resemble legitimate ones but are registered independently.

Secure organizations typically use official domains with HTTPS encryption and recognizable naming conventions. Suspicious domains may include random strings, unusual country codes, or shortened URLs. Additionally, attackers may embed links within buttons or anchor text that hides the real address.

Another warning sign is redirection behavior. Clicking a phishing link may lead to login pages that closely imitate real websites but are hosted on fraudulent servers.

Domain reputation checks, WHOIS lookups, and security scanning tools can help verify legitimacy. Careful link and domain analysis significantly reduces the risk of credential theft.

Risk Classification and Impact Analysis

The phishing emails presented in the screenshots pose a high level of risk because they target sensitive information and rely on psychological manipulation. Each example attempts to obtain credentials or personal data by impersonating trusted organizations. If users fall victim to such attacks, the consequences can be severe and widespread.

From a technical perspective, these emails represent credential harvesting and potential malware distribution risks. Clicking malicious links may lead to fake login pages that capture usernames and passwords. Once attackers gain access, they may exploit accounts for unauthorized transactions, identity theft, or further phishing campaigns.

Financial impact is particularly significant in cases involving banking or payment services, such as the American Express impersonation. Unauthorized transactions, account lockouts, and recovery costs can create substantial financial losses. Institutional emails, such as university or HR impersonation, may lead to compromised internal systems, data breaches, or unauthorized access to confidential information.

Psychological impact should also be considered. Victims often experience stress, loss of trust, and reputational damage. Organizations affected by phishing attacks may face legal consequences and operational disruption.

Overall, these phishing attempts should be classified as high-risk threats due to their potential to compromise credentials, financial assets, and organizational security.

Prevention and Awareness Guidelines

Preventing phishing attacks requires both technical safeguards and user awareness. Individuals should always verify unexpected emails, especially those requesting urgent action or sensitive information. Instead of clicking links directly, users should access services through official websites or trusted applications.

Email verification practices are essential. Users should check sender addresses carefully, examine domain names, and be cautious of generic greetings or suspicious language. Hovering over links before clicking helps reveal hidden destinations. If an email appears suspicious, it should be reported to the organization’s IT or security department.

Organizations can strengthen defenses by implementing email filtering systems, spam detection tools, and authentication protocols such as SPF, DKIM, and DMARC. Multi-factor authentication (MFA) significantly reduces risk even if credentials are compromised.

Regular cybersecurity awareness training is critical. Employees and students should learn to recognize phishing patterns, social engineering tactics, and safe email practices. Simulated phishing exercises can help reinforce awareness and improve response readiness. Software updates and antivirus protection also play an important role in preventing malware infections from malicious links or attachments.By combining education, verification habits, and technical controls, individuals and organizations can significantly reduce the likelihood and impact of phishing attacks.

Conclusion

The analysis of the uploaded phishing email examples demonstrates how attackers exploit trust, urgency, and emotional triggers to manipulate users into revealing sensitive information. By impersonating institutions such as universities, employers, and financial service providers, cybercriminals create convincing messages that appear legitimate at first glance. However, closer inspection reveals clear warning signs, including suspicious sender addresses, deceptive links, generic greetings, and urgent requests for action.

Technical examination through email header analysis and domain investigation further exposes inconsistencies that confirm malicious intent. These emails pose serious risks, including credential theft, financial loss, data breaches, and organizational disruption. Their potential impact highlights the importance of proactive detection and user awareness.

Effective prevention depends on a combination of technical security measures and informed user behavior. Email authentication systems, secure browsing practices, and multi-factor authentication provide strong protection, while cybersecurity awareness training helps individuals recognize and avoid phishing attempts.

Ultimately, phishing remains one of the most common and dangerous forms of cyberattack due to its reliance on human vulnerability. Continuous vigilance, education, and verification are essential for minimizing risk. Understanding how phishing emails operate is the first step toward building a secure digital environment.