



# Phishing Report

Awareness and Detection  
Insights



# **TASK 2:Phishing Email Detection & Awareness System**

**NAME: Weddy Gacheri**

**DATE: 10/2/2026**

**Future Interns**

# Executive Summary

The objective of the phishing email analysis was to examine a real-world phishing email sample, identify indicators of malicious intent, and create an awareness document that can help users recognize and avoid similar threats.

## Overview

The analyzed email claims to be an internal voice message notification from target.example.com. Through comprehensive header analysis using industry-standard tools, the email was found to have failed all three critical email authentication protocols: **SPF** (Sender Policy Framework), **DKIM** (DomainKeys Identified Mail), and **DMARC** (Domain-based Message Authentication, Reporting & Conformance) .

## Key Findings

Authentication Check	Result	Implication
SPF	FAIL	Sending server not authorized by the claimed domain
DKIM	NONE	No cryptographic signature to verify email integrity
DMARC	FAIL	Domain policy violated - email should be rejected

## Additional Red Flags Identified

- **HTML Obfuscation:** The email uses encoded characters (&#959;) to hide the word "from" from spam filters
- **Urgency Tactics:** Subject line contains "Exception" and "Access" to pressure recipients
- **Curiosity Bait:** "Voice Message" entices users to click without thinking
- **Spoofed Sender:** The "From" address is forged, as proven by authentication failures

## Conclusion

Based on the technical analysis, this email is definitively **malicious and should be classified as PHISHING**. If a recipient were to interact with this email, they could be redirected to credential-harvesting pages or tricked into downloading malware. This analysis underscores

the importance of email authentication protocols and user awareness in defending against phishing attacks.

# Email Metadata

Field	Value
Subject	target.example.com - (Voice Message-Access for Clients.Pass-Key-Exception)
Date	Fri, 04 Mar 2022 14:28:18 +0000
From (Display)	"target.example.com" <noreply@target.example.com>
To	john.doe@target.example.com
Return-Path	noreply@target.example.com
Message-ID	<8b14d0ea@target.example.com>
Source IP	192.0.2.1
Email Format	HTML with embedded image

Authentication-Results: spf=fail (sender IP is 192.0.2.1)  
smtp.mailfrom=target.example.com; dkim=none (message not signed)  
header.d=none;dmarc=fail action=reject header.from=target.example.com;  
Received-SPF: Fail (protection.outlook.com: domain of target.example.com does  
not designate 192.0.2.1 as permitted sender)  
receiver=protection.outlook.com; client-ip=192.0.2.1;  
helo=mail.example.com;  
Content-Type: multipart/mixed;  
boundary="\_66c1c8ad-223a-4c3b-871d-fd76339f929c\_"  
From: "target.example.com" <noreply@target.example.com>  
To: john.doe@target.example.com  
Subject: target.example.com :- (Voice Message-Access for  
Clients.Pass-Key-Exception)  
Message-ID: <8b14d0ea@target.example.com>  
Date: Fri, 04 Mar 2022 14:28:18 +0000  
Return-Path: noreply@target.example.com  
MIME-Version: 1.0  
  
--\_66c1c8ad-223a-4c3b-871d-fd76339f929c\_  
Content-Type: text/html  
Content-Transfer-Encoding: quoted-printable  
  
<html><head>  
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dus-ascii"=  
><meta name=3D"GENERATOR" content=3D"MSHTML 11.00.10570.1001"></head>  
<body>  
<div style=3D"BACKGROUND-COLOR: #f4f8f5">  
<div style=3D"WIDTH: 94%; FLOAT: left; PADDING-BOTTOM: 5px; PADDING-TOP: 5px;  
MARGIN-LEFT: 18px; PADDING-RIGHT: 5px">  
<div style=3D"FONT-SIZE: 13px; FONT-FAMILY: &quot;wf\_segoe-ui\_normal&quot;, =  
&quot;Segoe UI&quot;, &quot;Segoe WP&quot;, Tahoma, Arial, sans-serif; BACKGROU=   
ND-COLOR: #f4f8f5"><span>Internal Notification: Vmail Recieved for &nb=   
sp;<DATE></span></div></div>  
<div>

Figure 1: Email headers showing sender information and metadata

# Authentication Analysis

Email authentication protocols verify whether an email truly comes from the domain it claims to represent. The analyzed email was tested against three industry-standard authentication mechanisms with the following results:

## Authentication Results Summary

Authentication Check	Result	Status
SPF (Sender Policy Framework)	FAIL	✗
DKIM (DomainKeys Identified Mail)	NONE	✗
DMARC (Domain-based Message Authentication)	FAIL	✗

## Detailed Analysis

### 1. SPF (Sender Policy Framework)

**What it does:** SPF allows domain owners to specify which mail servers are authorized to send email on their behalf.

**Result:** FAIL

**Evidence from headers:**

Authentication-Results: spf=fail (sender IP is 192.0.2.1) smtp.mailfrom=target.example.com

Received-SPF: Fail (protection.outlook.com: domain of target.example.com does not designate 192.0.2.1 as permitted sender)

**What this means:** The sending server with IP address 192.0.2.1 is **not authorized** by target.example.com to send emails. This is a clear indication of spoofing.

### 2. DKIM (DomainKeys Identified Mail)

**What it does:** DKIM adds a digital signature to emails, allowing receivers to verify that the email was not tampered with during transit.

**Result:** NONE

**Evidence from headers**

dkim=none (message not signed)

**What this means:** The email lacks any cryptographic signature. Legitimate emails from target.example.com would typically include a DKIM signature. Its absence means the email's integrity cannot be verified.

### 3. DMARC (Domain-based Message Authentication)

**What it does:** DMARC tells receiving servers what to do if SPF and/or DKIM fail, and provides alignment checks between the various domains.

**Result: FAIL**

**Evidence from headers:**

dmarc=fail action=reject header.from=target.example.com

**What this means:** The email failed DMARC alignment checks. According to the domain's published policy, this email should be **rejected**.

## Overall Authentication Verdict

Criterion	Verdict
SPF	✗ Fail
DKIM	✗ None
DMARC	✗ Fail
Alignment	✗ None

**Conclusion:** The email failed all three authentication mechanisms. This provides definitive technical proof that the sender is not authorized by the claimed domain and the email is malicious.

## Header Analyzed

Email Subject: [target.example.com - \(Voice Message-Access for Clients.Pass-Key-Exception\)](#)

[Analyze New Header](#)

### Copy/Paste Warning

Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

## Delivery Information

- DMARC Compliant
- SPF Alignment
- SPF Authenticated
- DKIM Alignment
- DKIM Authenticated

## Relay Information

Received	0 seconds
Delay:	

Figure 2: MXToolbox/Google Header Analyzer results showing authentication failures

# Phishing Indicators

Beyond the authentication failures, this email contains multiple behavioral and technical red flags that are commonly used in phishing attacks. These indicators help users recognize malicious emails even without technical tools.

Indicator	Found in This Email	Risk Level
SPF/DKIM/DMARC Failures	Yes	Critical
HTML Obfuscation	Yes	Medium
Urgency Tactics	Yes	Medium
Curiosity Bait	Yes	Medium
Spoofed Sender	Yes	Critical
Suspicious Format	Yes (HTML)	Low

## Detailed Breakdown

### 1. Email Authentication Failures : CRITICAL

**What we found:** The email failed SPF, DKIM, and DMARC authentication.

**Why it matters:** This is **definitive technical proof** that the sender is not who they claim to be. Legitimate emails from target.example.com would pass these checks.

### 2. HTML Obfuscation : MEDIUM

**What we found:** The email uses HTML encoding to hide characters:

fr&#959;m

The &#959; is HTML code for the letter "o". This displays as "from" in the email but appears different to spam filters.

**Why it matters:** Attackers use this trick to bypass spam filters that scan for suspicious words. If a filter looks for the word "from" in raw text, it won't find it because it's encoded.

Attackers are trying to hide their tracks by writing words in a secret code that only your browser understands.

### 3. Urgency Tactics :MEDIUM

**What we found:** The subject line contains:

Voice Message-Access for Clients.Pass-Key-Exception

Words like "Exception" and "Access" create a sense of urgency. The recipient feels they must act quickly to avoid missing something important.

**Why it matters:** Urgency overrides rational thinking. When people feel pressured, they're more likely to click without verifying.

Phishers create fake emergencies to make you act before you think.

### 4. Curiosity Bait :MEDIUM

**What we found:** The email claims to contain a "Voice Message"

**Why it matters:** Everyone is curious about who left them a message. This natural curiosity is exploited to trick recipients into clicking malicious links or opening infected attachments.

Attackers use what you're curious about as bait

### 5. Spoofed Sender :CRITICAL

**What we found:** The "From" address claims to be:

noreply@target.example.com

However, authentication failures prove this is forged.

**Why it matters:** The email looks like it's from a trusted domain, but it's actually from an attacker. This is the core of email spoofing.

**Simple explanation:** Just like someone putting a fake return address on a letter, the sender is lying about where this email came from.

### 6. HTML Format : LOW

**What we found:** The email is sent in HTML format rather than plain text.

**Why it matters:** While not malicious by itself, HTML allows attackers to:

- Hide the real destination of links
- Embed images that can track when you open the email
- Make the email look like a legitimate company's branding

HTML emails can be made to look exactly like real company emails, making them harder to spot.

## Visual Indicators Summary

What to Look For	In This Email
Generic greeting	Not clearly visible
Spelling mistakes	"Recieved" (misspelled)
Mismatched links	Image URL points to sendgrid.net, not target.example.com
Suspicious attachments	HTML attachment present
Unusual sender domain	Uses target.example.com but fails authentication

```
<h4>New &nbsp;Message &nbsp;fr#959;m (801) 477-6790</h4><p>
<p style=3D"color:blue;">Attention : john.doe@target.example.com<p>
Ca&#8288;l&#8288;ler-ID :(801) 477-6753.<br>
Len&#8288;gth : 00:60 Sec<br>
Da&#8288;te : 2022-03-04 <br>
Re&#8288;cep&#8288;tion &nbsp; :Vossloh-schwabe V#959;ice Message Service<b= r>
```

Figure 3: Screenshot showing HTML obfuscation or suspicious elements

## Risk Classification

Based on the comprehensive analysis of technical indicators, behavioral red flags, and authentication results, this email has been evaluated using industry-standard threat scoring methodologies.

## Threat Scoring Matrix

Risk Category	Score	Weight	Weighted Score
Authentication Failures (SPF/DKIM/DMARC)	30/30	High	30
Spoofing Indicators	15/15	High	15
URL/Link Analysis	10/15	Medium	10
Urgency/Manipulation Tactics	15/20	Medium	15
HTML Obfuscation	10/10	Medium	10
Attachment Risk	5/10	Low	5

TOTAL THREAT SCORE :85/100

## Risk Level Determination

Score Range	Risk Level	Action Required
0-30	LOW	No immediate action
31-60	MEDIUM	Monitor, user caution advised
61-85	HIGH	Block, delete, alert users
86-100	CRITICAL	Immediate incident response

## FINAL VERDICT

Threat Score	85/100
Risk Level	HIGH
Classification	PHISHING
Confidence Level	Very High (authentication failures provide definitive proof)

## Justification

This email is classified as **HIGH RISK PHISHING** for the following reasons:

- Definitive Authentication Failures:** The email failed SPF, DKIM, and DMARC checks simultaneously. This is irrefutable technical proof of spoofing.
- Active Obfuscation:** The use of HTML encoding (&#959;) demonstrates deliberate intent to evade security filters.
- Psychological Manipulation:** The email combines urgency ("Exception") with curiosity ("Voice Message") to override rational decision-making.
- Spoofed Trust:** By forging target.example.com, the attacker exploits trust in a known brand.

## Recommended Actions

<b>Priority</b>	<b>Action</b>
Immediate	Delete this email immediately. Do not click any links or open attachments.
Short-term	Block the sender domain and source IP (192.0.2.1) at the email gateway.
Long-term	Conduct user awareness training on voice message phishing tactics.

# Prevention Guidelines: How to Spot Phishing Emails

Phishing attacks continue to bypass technical controls, making **user awareness** the last line of defense. The following guidelines can help anyone recognize and avoid phishing attempts like the one analyzed in this report.

## 7 Red Flags to Look For

### 1. CHECK THE SENDER'S EMAIL ADDRESS

**What to do:** Always verify the sender's full email address, not just the display name.

**Why:** Display names are easy to fake. In this email, "target.example.com" looks legitimate, but authentication failures proved it was spoofed.

**Example:**

- Fake: "PayPal" <paypal@secure-verify.net>
- Real: "PayPal" <service@paypal.com>

### 2. HOVER OVER LINKS BEFORE CLICKING

**What to do:** Mouse over any link (without clicking) to see the actual destination URL.

**Why:** The text you see (like "Click here") can be different from where the link really goes.

**Example:** If an email claims to be from Amazon but the link goes to amazon-secure-login.ru — it's phishing.

### 3. LOOK FOR URGENCY OR THREATS

**What to do:** Be suspicious of emails demanding immediate action.

**Why:** Attackers create urgency to make you act before thinking. This email used "Exception" and "Access" to create pressure.

**Common phrases:**

- "Your account will be suspended"
- "Immediate action required"
- "Unauthorized login attempt"
- "Payment declined"

### 4. EXAMINE GREETINGS AND LANGUAGE

**What to do:** Be wary of generic greetings like "Dear Customer" or "Dear User."

**Why:** Real companies usually address you by name. Phishing emails are sent to thousands of people at once.

**Also watch for:**

- Poor grammar
- Spelling mistakes (like "Recieved" in this email)
- Awkward phrasing

## 5. BE CAUTIOUS WITH ATTACHMENTS

**What to do:** Never open unexpected attachments, especially from unknown senders.

**Why:** Attachments can contain malware. Common dangerous file types:

- .exe, .scr (executables)
- .zip, .rar (archives)
- .docm, .xlsm (macro-enabled Office files)
- .htm, .html (can contain phishing forms)

## 6. VERIFY UNEXPECTED REQUESTS

**What to do:** If an email asks for personal information, passwords, or payments, verify through another channel.

**Why:** Legitimate companies never ask for sensitive information via email.

**Example:** Call the company directly using a phone number from their official website—not from the email.

## 7. TRUST YOUR GUT

**What to do:** If something feels off, it probably is.

**Why:** Attackers rely on you ignoring that uneasy feeling. When in doubt, delete and verify separately.

## Quick Reference Checklist

Print this or keep it handy:

<input checked="" type="checkbox"/>	Check This
<input type="checkbox"/>	Does the sender's email address match the company name?
<input type="checkbox"/>	Are you being asked to act urgently?
<input type="checkbox"/>	Does the email address you by name?
<input type="checkbox"/>	Are there spelling or grammar mistakes?
<input type="checkbox"/>	Do links match where they claim to go?
<input type="checkbox"/>	Was the attachment expected?
<input type="checkbox"/>	Does the email ask for personal information?

If you answer "YES" to any of the first two, or "NO" to any of the others – proceed with extreme caution.

## What to Do If You Suspect Phishing

Step	Action
1	DO NOT click any links or open attachments
2	DO NOT reply to the email
3	Report it to your IT/security team
4	Delete the email
5	If you clicked a link, contact IT immediately

## **Company Policies to Implement**

Organizations should also implement technical controls:

- **Email Authentication:** Enforce SPF, DKIM, and DMARC to block spoofed emails
- **Link Protection:** Use email security tools that rewrite and scan links
- **Attachment Sandboxing:** Open attachments in isolated environments
- **Regular Training:** Conduct phishing simulations and awareness sessions
- **Clear Reporting:** Make it easy for employees to report suspicious emails

# Conclusion

## Summary of Findings

This report analyzed a phishing email claiming to be a voice message notification from target.example.com. Through comprehensive technical analysis and behavioral assessment, the email was definitively identified as malicious.

### Key Findings Recap

Category	Result
Authentication Status	SPF: FAIL
Phishing Indicators	6 confirmed red flags
Threat Score	85/100
Risk Level	HIGH
Final Classification	PHISHING

## Why This Matters

Phishing remains one of the most common and successful attack vectors used by cybercriminals. A single successful phishing email can lead to:

- **Data Breaches:** The 2023 Verizon Data Breach Investigations Report found that **74% of breaches involve the human element**, including phishing
- **Financial Loss:** The FBI's Internet Crime Complaint Center reported phishing-related losses exceeding **\$52 million** in 2022
- **Account Takeover:** Stolen credentials are often used to access other systems
- **Ransomware:** Many ransomware attacks begin with a phishing email
- **Reputation Damage:** Customer trust is eroded when breaches occur

## Lessons Learned from This Analysis

Lesson	Application
<b>Authentication is critical</b>	SPF/DKIM/DMARC failures are definitive proof of spoofing
<b>Attackers use psychology</b>	Urgency and curiosity bypass rational thinking
<b>Technical controls aren't enough</b>	User awareness is essential
<b>Obfuscation is common</b>	HTML encoding and other tricks evade filters
<b>Documentation matters</b>	Clear reporting helps organizations improve defenses

## Recommendations Recap

### For Individuals

- Always verify sender addresses
- Hover over links before clicking
- Be suspicious of urgency and unexpected attachments
- When in doubt, verify through another channel

### For Organizations

- Implement and enforce SPF, DKIM, and DMARC
- Deploy email filtering with link and attachment protection
- Conduct regular phishing awareness training
- Create clear reporting procedures for suspicious emails

The analyzed email is **undoubtedly a phishing attempt**. It combines:

- **Technical spoofing** (failed authentication)
- **Active evasion** (HTML obfuscation)
- **Psychological manipulation** (urgency + curiosity)

If a recipient were to interact with this email, they would likely be directed to a credential-harvesting page or infected with malware.

This analysis demonstrates the importance of a multi-layered approach to email security. While technical controls like SPF, DKIM, and DMARC provide the first line of defense, user

**awareness remains critical.** By understanding what to look for, individuals can become the last and most effective line of defense against phishing attacks.

As cyber threats continue to evolve, continuous learning and vigilance are essential. This task has provided hands-on experience in real-world phishing analysis—a skill that is increasingly valuable in today's threat landscape.