Phishing Email Detection & Awareness System

Project : 02

Assessment Type: Analysing phishing emails

Date: 13-01-2026

1. Analysing Phishing Emails :

Sample 1:

Von	target.example.com <noreply@target.example.com> ☆
Betreff	**target.example.com :- (Voice Message-Access for Clients.Pass-Key-Exception)**
An	john.doe@target.example.com ☆

Internal Notification: Vmail Recieved for

Office 365

New Message from (801) 477-6790

Attention : john.doe@target.example.com

Caller-ID :(801) 477-6753.
Length : 00:60 Sec
Date : 2022-03-04
Reception :Vossloh-schwabe Voice Message Service

Download attached file to listen to your voice message

This message was sent to **john.doe@target.example.com**

Delivery Information

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

SPF and DKIM Information

dmarc:target.example.com [Show] [Solve Email Delivery Problems]

DMARC Record for target.example.com

No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: example.com Inbox Receivers will apply example.com DMARC record to mail sent from target.example.com

SP Tag 'reject' found: Inbox Receivers will reject 100% of all mail sent from target.example.com that fails DMARC.

DMARC Record for example.com (organizational domain)

v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s

spf:target.example.com:192.0.2.1 [Hide] [Solve Email Delivery Problems]

	Test	Result	
❌	SPF Record Published	No SPF Record found	ℹ️ More Info

Phishing Indicators :

Indicator	Meaning
SPF fail	Sender not authorized
DKIM fail	Message altered or fake
DMARC fail	Domain spoofing

Risk Classification : PHISHING

Sample 2 :

RenewalbyAndersen <info@ujjufjrm.spaghettimoon.nl> (sent by Trusted Sender)
to me

from:	RenewalbyAndersen <info@ujjufjrm.spaghettimoon.nl>
sent by:	Trusted Sender <amareswar13724@gmail.com>
to:	me@aol.com
date:	Jan 10, 2026, 10:21PM
subject:	Your Home Renovations Happen With Us
mailing list:	<.xt.local> Filter messages from this mailing list
mailed-by:	kjhgfiuytr.spaghettimoon.nl
signed-by:	ujjufjrm.spaghettimoon.nl
security:	Standard encryption (TLS) Learn more

amareswar13724 SAVE ON REPLACING YOUR WINDOWS

>> BOGO 40% off* with us! <<

Transform Your Home with Renewal by Andersen

Limited Time Offer!

Ready to upgrade your home with stunning new windows and doors? Now's the perfect time! Renewal by Andersen is excited to offer a special deal just for you:

Buy One, Get 40% Off* PLUS $200 Off Your Entire Order*!

Our energy-efficient windows and doors not only enhance your home's beauty but also may help you save on energy bills. With a wide range of styles and customization options, you're sure to find the perfect fit for your home.

Don't miss out on this incredible offer! Click below to get started:

Start My Free Quote

Transform your home today and experience the Renewal by Andersen difference. This offer won't last long, so act now!

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

Phishing Indicators :

Indicator	Meaning
SPF pass	Sender authorized and authenticated
DKIM fail	Message altered or fake
DMARC fail	DMARC Quarantine/Reject policy not enabled
URL check	only 1 vendor flagged
Luring Language	Offers will make users click links
Greeting	Used mail to greet not specific name which is suspicious

Risk Classification : Suspicious

Sample 3:

BHEL has announced openings for Engineer Trainee and Supervisor Trainee positions   Spam ×

BHEL recruitment 2025 <info@wayfarertrip.com>
to me ▾

Why is th...

Report

from:	BHEL recruitment 2025 <info@wayfarertrip.com>
reply-to:	BHEL recruitment 2025 <info@wayfarertrip.com>
to:	amareswar13724@gmail.com
date:	Dec 29, 2025, 11:02 AM
subject:	BHEL has announced openings for Engineer Trainee and Supervisor Trainee positions
mailed-by:	mail.wayfarertrip.com
signed-by:	wayfarertrip.com
security:	🔒 Standard encryption (TLS) Learn more

Hello,

Please find the details regarding the **BHEL Recruitment 2025** below:

Post: Engineer Trainee, Supervisor Trainee & Support Roles
Total Vacancies: 1,285
Last Date to Apply: 30 December 2025

Bharat Heavy Electricals Limited (BHEL) has announced openings for Engineer Trainee and Supervisor Trainee positions as part of the 2025 recruitment cycle.

Application Link:
https://careers.bhel.in

Regards,

- ❌ **DMARC Compliant**
  - ✅ **SPF Alignment**
  - ✅ **SPF Authenticated**
  - ✅ **DKIM Alignment**
  - ❌ **DKIM Authenticated**

---

0 / 97
Community Score

✅ No security vendors flagged this URL as malicious   ⟳ Reanalyze   🔍 Search

https://lnkt.wayfarertrip.com/vtrack?clientid=181800&ul=VVcMCgsGVw5EUkhYXgVKVUUTBEIHUIIEB3leWFleDR9aCltMGU9S&ml=VVMODAgGV0UIHwYIBF...
lnkt.wayfarertrip.com

Last An...
a momen

DETECTION   **DETAILS**   **COMMUNITY**

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis ⓘ   Do you want to automat

Abusix	✅ Clean	Acronis	✅ Clean
ADMINUSLabs	✅ Clean	AILabs (MONITORAPP)	✅ Clean
AlienVault	✅ Clean	Antiy-AVL	✅ Clean
Artists Against 419	✅ Clean	benkow.cc	✅ Clean

Phishing Indicators :

Indicator	Meaning
SPF pass	Sender authorized and authenticated
DKIM pass	Message Authenticated
DMARC fail	DMARC Quarantine/Reject policy not enabled
URL check	Passed
Job Opportunity	Users are desperate to click links

Risk Classification : SAFE

Sample 4:

You have a pending transaction that requires your attention! #33422! Spam ×

info <my@vienacapellanes.com>
to me ▾

Wed, Dec 24, 2025, 9:23 PM

from:	info <my@vienacapellanes.com>
to:	amareswar13724 <amareswar13724@gmail.com>
date:	Dec 24, 2025, 9:23 PM
subject:	You have a pending transaction that requires your attention! #33422!
mailed-by:	eu-west-1.amazonses.com
signed-by:	vienacapellanes.com
security:	🔒 Standard encryption (TLS) Learn more

This me...
Messages...

Looks

...nents, or reply with personal information.

OpenSea

You have successfully sold your item!

Congratulations! You successfully sold **item**
#3677482 for **1.1004 ETH** using OpenSea.

View Transaction on Etherscan

Open$

Want to receive funds faster?

Connect your wallet to track this transaction in real-time and speed up confirmation if
needed.

---

https://eliteconstruction.ae/ssl/?id=0570

1 / 97

Community
Score

⚠ 1/97 security vendor flagged this URL as malicious

Reanalyze   Search   M

https://eliteconstruction.ae/ssl/?id=0570
eliteconstruction.ae

text/html

Status
404

Content type
text/html; charset=UTF-8

Last Analysis Date
a moment ago

DETECTION   DETAILS   COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis ⓘ

Do you want to automate

Trustwave	⚠ Phishing	Fortinet	⚠ Spam
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AiLabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean

Delivery Information

❌ DMARC Compliant
  ❌ SPF Alignment
  ✅ SPF Authenticated
  ✅ DKIM Alignment
  ❌ DKIM Authenticated

AbuseIPDB » *54.240.3.23*

Check an IP Address, Domain Name, Subnet, or ASN
e.g. **2405:201:c03a:e9c6:e8fa:86f5:2a34:24c6, microsoft.com,**
5.188.10.0/24, or **AS15169**

54.240.3.23

CHECK

54.240.3.23 was found in our database!

This IP was reported **53** times. Confidence of Abuse is **22%**:   ?

22%

ISP	Amazon Web Services, Inc.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS16509
Hostname(s)	a3-23.smtp-out.eu-west-1.amazonses.com
Domain Name	amazon.com
Country	🇺🇸 United States of America
City	Seattle, Washington

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

REPORT IP   WHOIS SEARCH

Phishing Indicators :

Indicator	Meaning
SPF fail	Sender not authorized
DKIM Pass	Message not altered as attacker made it since beginning
DMARC fail	Domain spoofing
IP report	IP is reported 53 times for abuse
URL check	Reported as spam
Money Incentives	Sale proceedings on item which will make user to click without verifying legitimacy

Risk Classification : PHISHING

2. Common Phishing Indicators :

Employees should treat emails as suspicious if they include:

Non-technical :

- Urgent or threatening language
- Generic greetings
- Unexpected links or attachments
- Requests for passwords or verification
- Sender and link domain mismatch
- Poor branding or missing contact details

Technical :

- Check SPF and DKIM Records: check if the sender's domain has proper SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records. These records help prevent email spoofing and phishing.
- use this tools :
  - https://toolbox.googleapps.com/apps/messageheader/
  - https://mxtoolbox.com/EmailHeaders.aspx

3. Check for URLs and IPs :

Inspect links in the email. Hover over each link without clicking to view the destination URL. Ensure the displayed URL matches the linked text. Verify that the domain is correctly spelled and does not contain unusual characters or substitutions.

1. https://www.virustotal.com/gui/
2. https://www.abuseipdb.com

4. Risk Classification Model :

Risk Level	Description
Safe	Verified sender, expected content . SPF , DKIM , DMARC should be aligned and authenticated
Suspicious	Unclear intent, requires validation .SPF is algined and authenticated but not DKIM,DMARC
Phishing	Clear deception and malicious indicators.SPF,DKIM,DMARC arent aligned or authenticated

5. How Phishing Attacks Work :

1. Attacker sends a fake email pretending to be trusted.
2. Email creates fear or urgency.
3. Victim clicks a malicious link.
4. Fake website captures credentials or data.
5. Attacker uses the information for fraud or access.

6. Prevention & Awareness Guidelines

☐ Employee Do's

- Stop and think before clicking
- Hover over links to inspect URLs
- Access accounts via official websites
- Report suspicious emails immediately
- Verify unusual requests with IT or HR

☐ Employee Don'ts

- Click urgent links from emails
- Enter passwords through email links
- Download unexpected attachments
- Reply to suspicious messages
- Ignore reporting procedures