

Mastercard Email Phishing Analysis

This project is designed to enhance security awareness and demonstrate how easily phishing attacks can be made believable. It includes two main tasks to help improve email security and provide a practical solution for teams to recognise and defend against phishing attempts.

Tasks

Task 1: Examine an Obvious Fake Email and Make It More Believable

In this task, a clearly fake phishing email will be reviewed and improved to make it more convincing.

Techniques such as improved email design, social engineering tactics, and realistic content will be used to enhance the believability of the email.

Task 2: Create a Short Presentation to Help Teams Improve Security Awareness

A concise presentation aimed at educating teams about phishing risks and how to spot suspicious emails.

The presentation will cover key security tips, red flags to look for, and best practices to follow to reduce the likelihood of falling for phishing attacks.

Objective

The goal of this project is to provide practical insights into how phishing attacks operate and equip teams with the knowledge to identify and respond to these threats effectively.

Task 1 Introduction-

We will look at various tools that will aid us in analyzing phishing emails. We will:

1. Look at tools that will aid us in examining email header information.
2. Cover techniques to obtain hyperlinks in emails, expand the URLs if they're URL shortened.
3. Look into tools to give us information about potentially malicious links without directly interacting with a malicious link.
4. Cover techniques to obtain malicious attachments from phishing emails and use malware sandboxes to detonate the attachments to understand further what the attachment was designed to do.

Warning: The samples throughout this room contain information from actual spam and/or phishing emails. Proceed with caution if you attempt to interact with any IP, domain, attachment, etc.

Answer to the questions of this section-

No Answer needed

Task 2 What information should we collect?-

Below is a checklist of the pertinent information an analyst (you) is to collect from the email header:

1. Sender email address
2. Sender IP address
3. Reverse lookup of the sender IP address
4. Email subject line
5. Recipient email address (this information might be in the CC/BCC field)
6. Reply-to email address (if any)
7. Date/time

Afterward, we draw our attention to the email body and attachment(s) (if any).

Below is a checklist of the artifacts an analyst (you) needs to collect from the email body:

1. Any URL links (if an URL shortener service was used, then we'll need to obtain the real URL link)
2. The name of the attachment
3. The hash value of the attachment (hash type MD5 or SHA256, preferably the latter)

Warning: Be careful not to click on any links or attachments in the email accidentally.

Answer to the questions of this section-

No Answer needed

Task 3 Email header analysis –

Usage: Copy and paste the entire email header and run the analysis tool.

Messageheader: <https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

Another tool is called **Message Header Analyzer**.

Message Header Analyzer: <https://mha.azurewebsites.net/>

you can also use <https://mailheader.org/>

Even though not covered in the previous Phishing rooms, a Message Transfer Agent (MTA) is software that transfers emails between sender and recipient. Read more about MTAs [here](#). Since we're on the subject, read about MUAs (Mail User Agent) [here](#).

Note: The option on which tool to use rests ultimately on you. It is good to have multiple resources to refer to as each tool might reveal information that another tool may not reveal.

The tools below can help you analyze information about the sender's IP address:

IPinfo.io: <https://ipinfo.io/>

URLScan.io: <https://urlscan.io/>

You can use other tools that provide the same functionality and more, such as [URL2PNG](#) and [Wannabrowser](#).

Talos Reputation Center: <https://talosintelligence.com/reputation>

Answer to the questions of this section-

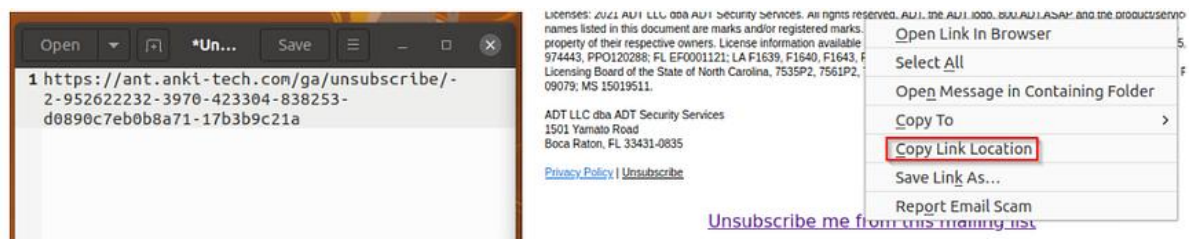
capticalone.com

Task 4 Email body analysis –

Now it's time to direct your focus to the email body. This is where the malicious payload may be delivered to the recipient either as a link or an attachment.

Links can be extracted manually, either directly from an HTML formatted email or by sifting through the raw email header.

Below is an example of obtaining a link manually from an email by right-clicking the link and choosing Copy Link Location.



The same can be accomplished with the assistance of a tool. One tool that can aid us with this task is URL Extractor.

URL Extractor: <https://www.convertcsv.com/url-extractor.htm>


You can copy and paste the raw header into the text box for **Step 1: Select your input**.

A screenshot of the "URL Extractor For Web Pages and Text" web application. The interface has a dark header with the title and a sub-header "Use this tool to extract URLs in web pages, data files, text and more." Below this, there are sections for "From CSV/Excel" and "To CSV/Excel" with various conversion options. The main section is "Step 1: Select your input", which is highlighted with a red box. It contains a text area where a raw email header has been pasted. The header text includes "Received: from 10.197.39.201 by atlas117.free.mail.bf1.yahoo.com with HTTP/1.1; Wed, 30 Jun 2021 13:59:41 +0000", "Return-Path: <return@beginfo.club>", "X-Originating-IP: [38.92.176.109]", "Received-SPF: softfail (domain of transition@beginfo.club does not designate 38.92.176.109 as permitted sender)", "Authentication-Results: asas117.free.mail.bf1.yahoo.com; dkim=unknown, spf=softfail smtp.mailfrom=beginfo.club; dmarc=unknown header.from=beginfo.club", "X-Apparently-To: [redacted]@yahoo.com; Wed, 30 Jun 2021 13:59:42 +0000", and "X-YMailISG: nAyU0sVLDcy2b9ca92T6ynP7Ph8d3yPq1JjeVWnlprS". Below the text area are buttons for "Clear Input" and "Example". At the bottom, there are sections for "Step 2: Choose output options (optional)" and "Step 3: Extract URLs" with buttons for "Extract" and "Extract To Excel".

The extracted URLs are visible in Step 3.

Step 3: Extract URLs

Extract Extract To Excel

Result Data: 

```
http://devret.xyz/4833aq11254939bv6888vn22032ip1508=
http://devret.xyz/4833fx11254939ea6888wk22032mk1269ep1508rr
http://devret.xyz/4833jo11254939iz6888xo22032gu1269jm1508uu
http://devret.xyz/4833mt11254939vf6888zq22032si1269du1508rr
http://devret.xyz/Creatives/Tracking.png
http://devret.xyz/Creatives/unsub.png
```

Save your result: convertcsv .csv Download Result EOL: CRLF

You may also use **CyberChef** to extract URLs with the Extract URLs recipe.

It's important to note the root domain for the extracted URLs. You will need to perform an analysis on the root domain as well.

After extracting the URLs, the next step is to check the reputation of the URLs and root domain. You can use any of the tools mentioned in the previous task to aid you with this.

If the email has an attachment, you'll need to obtain the attachment safely. Accomplishing this is easy in Thunderbird by using the Save button.



After you have obtained the attachment, you can then get its hash. You can check the file's reputation with the hash to see if it's a known malicious document.

Obtain the file's **SHA256 hash**

```
user@machine$ sha256sum Double\ Jackpot\ Slots\ Las\ Vegas.dot
```

```
c650f397a9193db6a2e1a273577d8d84c5668d03c06ba99b17e4f6617af4ee83 Double Jackpot Slots
Las Vegas.dot
```

There are many tools available to help us with this, but we'll focus on two primarily; they are listed below:

Talos File Reputation: https://talosintelligence.com/talos_file_reputation

VirusTotal — <https://www.virustotal.com/gui/home/upload>

Another tool/company worth mentioning is <https://www.reversinglabs.com/>, which also has [a file reputation service](#).

Answer to the questions of this section-

Copy Link Location

Task 5 Malware Sandbox –

Luckily as Defenders, we don't need to have malware analysis skills to dissect and reverse engineer a malicious attachment to understand the malware better.

There are online tools and services where malicious files can be uploaded and analyzed to better understand what the malware was programmed to do. These services are known as malware sandboxes.

For instance, we can upload an attachment we obtained from a potentially malicious email and see what URLs it attempts to communicate with, what additional payloads are downloaded to the endpoint, persistence mechanisms, Indicators of Compromise (IOCs), etc.

Some of these online malware sandboxes are listed below.

Any.Run: <https://app.any.run/>

Hybrid Analysis: <https://www.hybrid-analysis.com/>

Joe Security — <https://www.joesecurity.org/>

Answer to the questions of this section-

No Answer needed

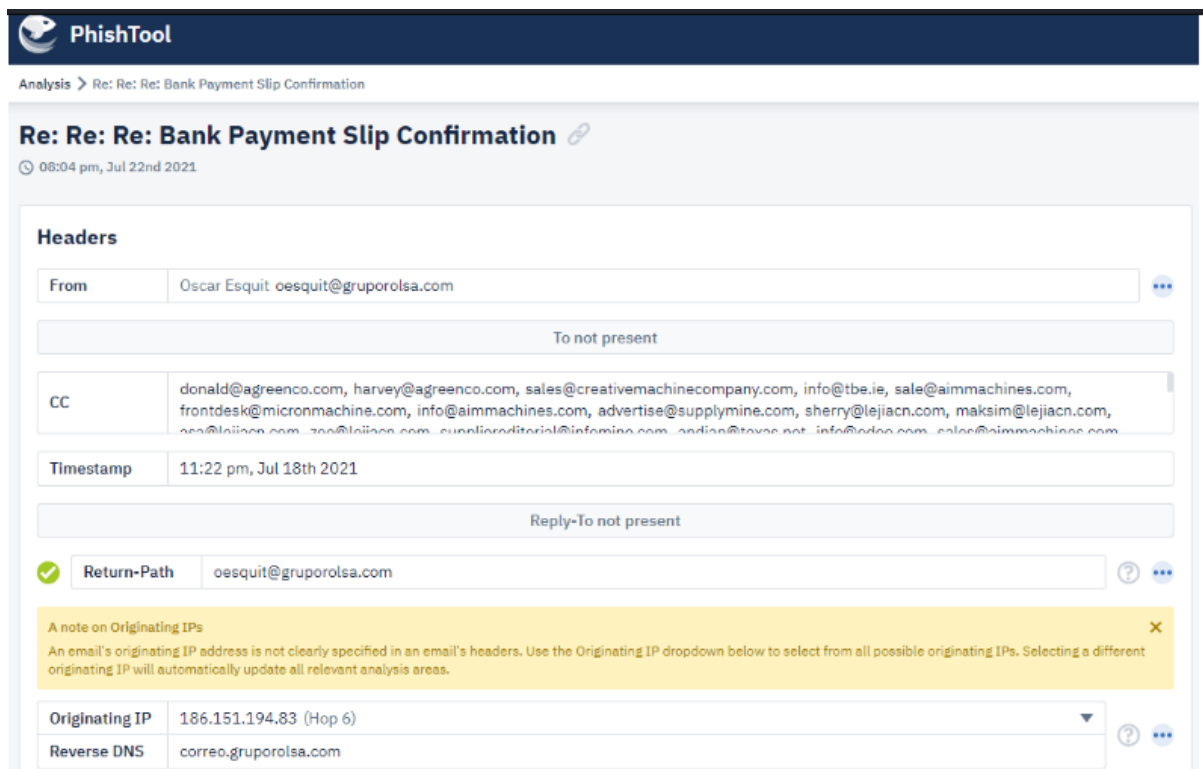
Task 6 PhishTool –

A tool that will help with automated phishing analysis is PhishTool — <https://www.phishtool.com/>

Note: There is a free community edition you can download and use. :)

I uploaded a malicious email to PhishTool and connected VirusTotal to my account using my community edition API key.

Below are a few screenshots of the malicious email and the PhishTool interface.



From the image above, you can see the PhishTool conveniently grabs all the pertinent information we'll need regarding the email.

1. Email sender
2. Email recipient (in this case, a long list of CCed email addresses)
3. Timestamp
4. Originating IP and Reverse DNS lookup

We can obtain information about the SMTP relays, specific X-header information, and IP info information.

Answer to the questions of this section-

Look at the Strings output. What is the name of the EXE file?

Correct Answer

Task 7 Phishing Case 1 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

Task: Use the tools discussed throughout this room (or use your own resources) to help you analyze each email header and email body.

Answer to the questions of this section-

What brand was this email tailored to impersonate?

Correct Answer

What is the From email address?

Correct Answer

What is the originating IP? Defang the IP address.

Correct Answer

💡 Hint

From what you can gather, what do you think will be a domain of interest? Defang the domain.

Correct Answer

💡 Hint

What is the shortened URL? Defang the URL.

Correct Answer

💡 Hint

For Email Header Analysis is used- <https://mha.azurewebsites.net/>

Message Header Analyzer

Insert the message header you would like to analyze

X-Hash: 80810362954852045903
X-AHash: 0
X-TID: 26475
X-EID: 3
X-RPCampaign: DollarGeneral22476023
X-TemplateID: 568
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="b1_81a6e0d83774c7653204fb72c08ccd60"
Content-Length: 52326

This is a multi-part message in MIME format.
--b1_81a6e0d83774c7653204fb72c08ccd60
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Analyze headers Clear Copy

Submit feedback on github

Subject: Your Netflix Account is on Hold
Message Id: <60e50e16.1c69fb81.186da.9717SMTPIN_ADDED_MISSING@mx.google.com>
Creation time: Wed, 7 Jul 2021 04:14:40 +0200
From: Netflix <JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQwWdR-yVvCaBkTnp.gogolecloud.com>
To: redacted@yahoo.com

Received headers

Message Header Analyzer

Insert the message header you would like to analyze

X-Hash: 80810362954852045903
X-AHash: 0
X-TID: 26475
X-EID: 3
X-RPCampaign: DollarGeneral22476023
X-TemplateID: 568
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="b1_81a6e0d83774c7653204fb72c08ccd60"
Content-Length: 52326

This is a multi-part message in MIME format.
--b1_81a6e0d83774c7653204fb72c08ccd60
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Analyze headers Clear Copy

#:	Header	Value
1	Return-Path	<postmaster@etekno.xyz>
2	X-Originating-IP	[209.85.167.226]
3	Received-SPF	none (domain of etekno.xyz does not designate permitted sender hosts)
4	Authentication-Aspects	atlas105.free.mail.bf1.vahoo.com: dkim=unknown: spf=none smtp.mailfrom=etekno.xyz: dmarc=unknown header.from=JOg7ODDQwWdR-yVvCaBkTnp.gogolecloud.com:

For Email Body Analysis I used- <https://www.convertcsv.com/url-extractor.htm>

Step 1: Select your input

☐ Scan list of web pages

Use this Regular Expression instead

```

Received: from 10.197.37.234
by atlas105.free.mail.bf1.yahoo.com with HTTPS; Wed, 7 Jul 2021 02:14:46 +0000
Return-Path: <postmaster@etekno.xyz>
X-Originating-IP: [209.85.167.226]
Received-SPF: none (domain of etekno.xyz does not designate permitted sender hosts)
Authentication-Results: atlas105.free.mail.bf1.yahoo.com;
dkim=unknown;
spf=none smtp.mailfrom=etekno.xyz;
dmarc=unknown header.from=JQg7QDDQwWdR-yVvCaBkTnp.gogolecloud.com;
X-Apparently-To: redacted@yahoo.com; Wed, 7 Jul 2021 02:14:47 +0000

```

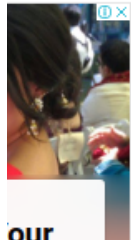
Step 2: Choose output options (optional) ▼

Step 3: Extract URLs

Result Data:

```

http://schema.org/
https://=
https://assets.nflxext.com/us/email/gem/icons/icon_play_white.png=
https://fonts.=
https://fonts.gstatic.com/s/quickand/y15/6xK-dsZaM9iE8KbpRA=
https://image.e.krogermail.com/lib/fe9813727564007f7d/m/16/Kroge=
https://image.e.krogermail.com/lib/fe98137275=
https://t.=
https://t.co/yuxfZm8KPg?amp=3D1
https://t.co/yuxfZm8KPg?amp=3D=
    
```



Task 8 Phishing Case 2 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

Task: Investigate the analysis and answer the questions below.

Link: <https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59>

Answer to the questions of this section-

All the answers can be found from here -

https://any.run/report/cc6f1a04b10bcb168aeec8d870b97bd7c20fc161e8310b5bce1af8ed420e2c24/8bfd4c58-ec0d-4371-bfeb-52a334b69f59?_gl=1*3nm857*_ga*Mjc2ODg2NDM1LjE2NjI4ODQ1MzQ.*_ga_53KB74YDZR*MTY2Mjg4NDUzNC4xLjEuMTY2Mjg4NDkwOC4zNS4wLjA.&_ga=2.250087872.752651539.1662884534-276886435.1662884534

What does AnyRun classify this email as?

Suspicious activity

Correct Answer

What is the name of the PDF file?

Payment-updateid.pdf

Correct Answer

What is the SHA 256 hash for the PDF file?

cc6f1a04b10bcb168aee8d870b97bd7c20fc161e8310b5bce1af8ed420e2c24

Correct Answer

What two IP addresses are classified as malicious? Defang the IP addresses. (answer: IP_ADDR,IP_ADDR)

2[.]16[.]107[.]24,2[.]16[.]107[.]83

Correct Answer

Hint

What Windows process was flagged as **Potentially Bad Traffic**?

svchost.exe

Correct Answer

Task 9 Phishing Case 3 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

Task: Investigate the analysis and answer the questions below.

Link: <https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83>

Answer to the questions of this section-

All the answers can be found from here

— https://any.run/report/5f94a66e0ce78d17afc2dd27fc17b44b3ffc13ac5f42d3ad6a5dcfb36715f3eb/82d8adc9-38a0-4f0e-a160-48a5e09a6e83?_gl=1*7s6t7g*_ga*Mjc2ODg2NDM1LjE2NjI4ODQ1MzQ.*_ga_53KB74YDZR*MTY2Mjg4NDUzNC4xLjAuMTY2Mjg4NDU0OC40Ni4wLjA.&_ga=2.6843892.752651539.1662884534-276886435.1662884534

What is this analysis classified as?

Malicious activity

Correct Answer

What is the name of the Excel file?

CBJ200620039539.xlsx

Correct Answer

What is the SHA 256 hash for the file?

5f94a66e0ce78d17afc2dd27fc17b44b3ffc13ac5f42d3ad6a5dcfb36715f3eb

Correct Answer

What domains are listed as malicious? Defang the URLs & submit answers in alphabetical order. (answer: URL1,URL2,URL3)

biz9holdings[.]com,findresults[.]site,ww38[.]findresults[.]site

Correct Answer

Hint

What IP addresses are listed as malicious? Defang the IP addresses & submit answers from lowest to highest. (answer: IP1,IP2,IP3)

75[.]2[.]11[.]242,103[.]224[.]182[.]251,204[.]11[.]56[.]48

Correct Answer

Hint

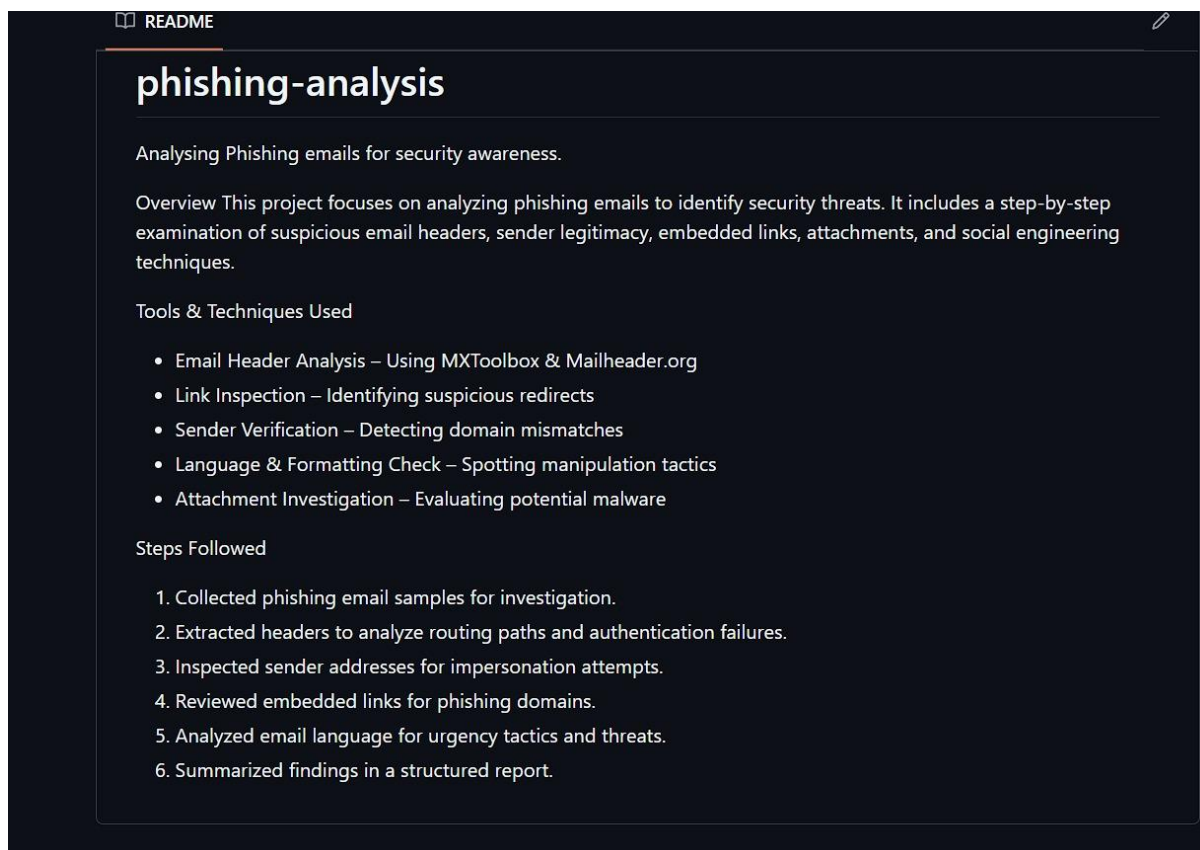
What vulnerability does this malicious attachment attempt to exploit?

CVE-2017-11882

Correct Answer

Hint

That is all for this Write-up, hoping this will help you in solving the challenges of Phishing Emails 3. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.



How to Spot a Phishing Email in 2025 –with Real Examples and Red Flags

[IT Governance](#) 16th May 2025

Despite growing awareness and increasingly sophisticated security tools, phishing is still one of the most persistent and pernicious threats of the modern age: according to [Proofpoint's 2024 State of the Phish](#) report, 86% of organisations experienced a phishing attempt last year and over 70% suffered a successful compromise due to human error.

Phishing is also the most prevalent form of attack: the UK government's [Cyber Security Breaches Survey 2025](#) found that phishing accounted for 93% of all cyber crime in the UK.

So why is phishing so effective? Simply because it exploits the weakest link in any cyber security setup: people. Phishing attacks are designed to manipulate people into giving up sensitive information, clicking malicious links or downloading dangerous attachments.

But while phishing tactics are evolving, so are the ways we can identify and mitigate them. This guide walks you through the most common red flags, updated for 2025 with real examples to help you stay vigilant.

Quick phishing checklist: is this email a scam?

Answering 'yes' to any of the questions below is a sign the email may be fraudulent.

Sender clues

- Is it from a public domain (e.g. @gmail.com) but pretending to be from a company?
- Is the domain slightly misspelled (e.g. amazOn.com)?
- Does it differ from how that organisation normally emails you?

Content and tone

- Are there spelling or grammatical errors?
- Does it urge immediate action (e.g. “Act now”, “Your account will be closed”)?
- Is the tone inconsistent with the sender’s usual communication style?

Links and attachments

- Does the link URL differ from the anchor text?
- Is there an unexpected attachment?
- Are the call-to-action buttons vague (e.g. “Click here”, “Log in now”)?

Security pressure

- Does it ask for personal information or passwords?
- Are you asked to bypass company protocols?
- Does it threaten negative consequences if you don’t comply?

If you can answer ‘yes’ to any of these questions, do not click and always verify through a known, trusted contact method.

Let’s look at those points in more detail.

1. The sender uses a public or suspicious email domain

Legitimate organisations don’t email you from addresses like supportcompany@gmail.com.

Not even Google.

Except for some small operations, most companies will have their own email domain and email accounts. For example, genuine emails from Google will read ‘@google.com’.

If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate.

By contrast, if the email comes from an address that isn’t affiliated with the apparent sender, it’s almost certainly a scam.

However, it’s not always immediately obvious that a domain isn’t legitimate: [some 85% of users open emails on their smartphones](#), where inboxes show only names rather than email addresses.

Tip: Always tap or hover over the sender name to reveal the full address.

2. The domain name is slightly altered

There's another clue hidden in domain names that provides a strong indication of phishing scams – unfortunately, it complicates our previous clue.

The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

For example, in early 2025, a campaign imitating Microsoft Teams used `micros0ft-teams.net` and tricked users into entering their credentials on fake login portals.

These domains exploit quick-glance habits. Just one character difference can deceive even careful readers.

Remember, criminal hackers only require one mistake from one employee for their operation to be a success. Everyone in your organisation must be confident in their ability to spot a scam upon first seeing it.

3. The email is poorly written

Although [phishing emails are generally better written nowadays thanks to generative AI](#), many still reveal themselves with misspellings and awkward phrasing.

Many scammers are from non-English-speaking countries and backgrounds where they have limited access to, or opportunity to learn, the language.

When crafting phishing messages, they'll therefore use a spellchecker or translation machine, giving them all the right words but not necessarily in the right context.

That's not to say any email with a mistake is a scam, however. Everyone makes typos from time to time, especially when they're in a hurry.

It's the recipient's responsibility to look at the context of the error and determine whether it's a clue to something more sinister. You can do this by asking:

- Is it a common sign of a typo (like hitting an adjacent key)?
- Is it a mistake a native speaker shouldn't make (grammatical incoherence, words used in the wrong context)?
- Is this email a template which should have been crafted and copy-edited?
- Is it consistent with previous messages I've received from this person?

If you're in any doubt, look for other clues that we've listed here or contact the sender using another line of communication, whether in person, by phone, via their website, an alternative email address or through an instant message client.

4. It includes malicious attachments or links

Phishing emails come in many forms. We've focused on emails in this article, but you might also get scam text messages, phone calls or social media posts.

But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment you're asked to download or a link to a bogus website.

The purpose of these payloads is to capture sensitive information, such as login credentials, credit card details, phone numbers and account numbers.

Malicious links

In January 2025, scammers posed as Chase Bank with emails linking to chase-secure-login.com, stealing banking credentials from unsuspecting users.

Hover over or hold down on all links before clicking.

Infected attachments

Phishing attachments often appear as invoices or tax documents. [In March 2025](#), an IRS-themed scam used ZIP files with embedded malware.

If you weren't expecting a file, don't open it. And definitely don't enable macros unless you've confirmed the source.

5. The message creates urgency or fear

Scammers play on panic. The longer you think about something, the more likely you will notice things that don't seem right. That's why so many scams request that you act now, or else it will be too late.

Criminals know that we're likely to drop everything if there's apparently a problem with a critical service or if our boss emails us with a vital request – especially when other senior colleagues are supposedly waiting for us.

Some examples seen in recent months:

- “Your Google Ads will be paused in 15 minutes – confirm billing now.”
- “Internal policy breach – click here to resolve before HR escalates.”
- “Your parcel is being returned – reschedule delivery within 30 minutes.”

This tactic pushes people to act before thinking critically.

Train your team to spot the threats

According to [IBM's Cost of a Data Breach Report 2024](#), phishing-related breaches now cost organisations \$5.1 million (£3.8 million) on average – the highest among all attack vectors.

The best defence is continuous education. Phishing awareness training helps your team recognise subtle red flags before it's too late.

Regular staff awareness training will ensure that employees know how to spot a phishing email, even as fraudsters' techniques become increasingly more advanced.

It's only by reinforcing advice on avoiding scams that your team can develop good habits and detect signs of a phishing email as second nature.

With our [Phishing Staff Awareness Training Programme](#), these lessons are straightforward.

The online subscription course explains everything you need to know about phishing and is updated each month to cover the latest scams.

```
(kali@kali)~$ git clone https://github.com/andreif/phishing-emails.git
Cloning into 'phishing-emails'...
Username for 'https://github.com': kali
Password for 'https://kali.github.com':
remote: Support for password authentication was removed on August 13, 2021.
remote: Please see https://docs.github.com/get-started/getting-started-with-git/about-remote-repositories#cloning-with-https-urls for information on currently recommended modes of authentication.
fatal: Authentication failed for 'https://github.com/andreif/phishing-emails.git/'
(kali@kali)~$
```

kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

```
(kali@kali)~$ git clone https://github.com/htr-tech/fake-mailer.git
Cloning into 'fake-mailer'...
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 24 (delta 5), reused 10 (delta 2), pack-reused 0 (from 0)
Receiving objects: 100% (24/24), 76.33 KiB | 78.00 KiB/s, done.
Resolving deltas: 100% (5/5), done.

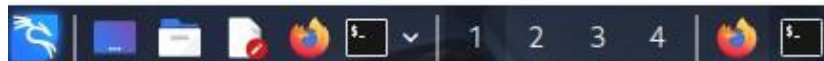
(kali@kali)~$ cd fake-mailer

(kali@kali)~/fake-mailer$ ls
LICENSE  mailer.py  README.md

(kali@kali)~/fake-mailer$ python2 mailer.py
```

kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



File Actions Edit View Help

Fake Mailer

[+] CREATED BY HTR-TECH (TAHMID RAYAT)

Launching Fake Mailer ...

Send Mail To : **itshitanshu@gmail.com**

Input Mail Subject : **Your account is Hacked!!**

Input Mail Content : **Ha Ha Ha !**

Sending Email >>>>>>>>

Mail Successfully Sent !!

Process can take some time !!

Visit **www.github.com/htr-tech** for More Tools