Phishing Email Analysis

By Mohammed AlSubayt

What is Phishing?

Phishing is a type of cyber attack where attackers impersonate legitimate organizations to trick individuals into revealing sensitive information. It often occurs through email, but can also happen through other communication channels.

Common Phishing Techniques

Phishing is a cyber attack that involves tricking individuals into revealing sensitive information, such as login credentials or financial details. There are several common phishing techniques that attackers use to deceive their targets and gain unauthorized access to their accounts or systems.

Common Phishing Techniques

Technique	Description
Email Spoofing	Attackers forge the email sender's address to make it appear as if the email is coming from a trusted source. This can trick individuals into clicking on malicious links or downloading infected attachments.
Spear Phishing	Attackers target specific individuals or organizations with personalized messages that appear legitimate. These messages often contain information that is relevant to the target, increasing the likelihood of a successful attack.
Pharming	Attackers redirect users to fraudulent websites that mimic legitimate ones. This can be done by manipulating DNS records or exploiting vulnerabilities in the target's network infrastructure.
Vishing	Attackers use voice calls to deceive individuals into revealing sensitive information, such as credit card numbers or social security numbers. They may impersonate trusted organizations, such as banks or government agencies.
Smishing	Attackers send fraudulent text messages to trick individuals into clicking on malicious links or providing sensitive information. These messages often appear as urgent notifications or requests for action.

What Are Email Headers?

You can think of an email in terms of its basic anatomy. There's the envelope, the body of the message, and its header. The body of the message is something you're already familiar with—it's the content you write. The envelope is something you generally don't need to think about; it's part of an internal process that's used to route the email.

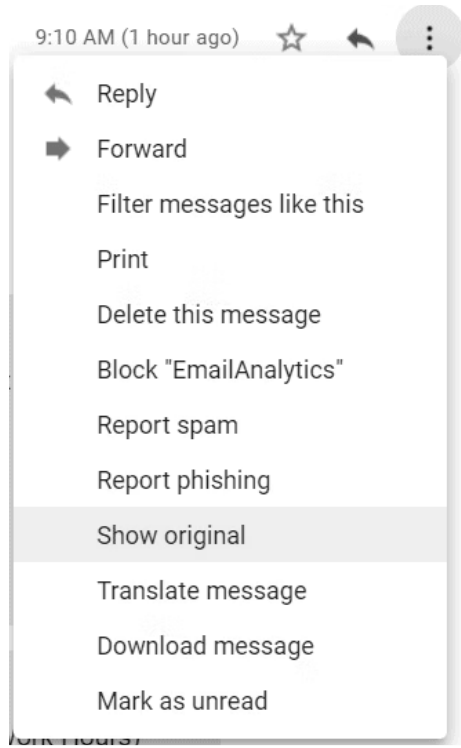
An email header is something different. When emails are sent, the body of the message is part of the transmission (obviously).

But preceding that core content are header lines that include information like the sender, the recipient, the subject line, and the date; these bits of information are parsed by your email client, and some are made visible to you so you have a better understanding of the message's context.

How to Analyze Email Headers in Gmail

Before you can analyze an email header, you first need to obtain it. Here's how to do that in Gmail:

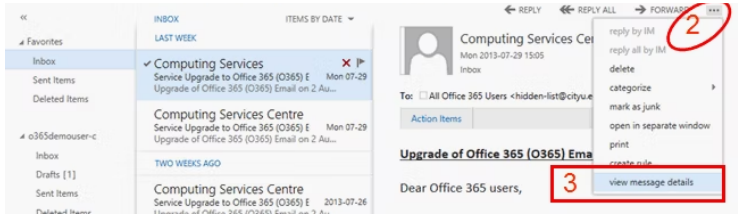
1. Open Gmail.
2. Find the message you want to analyze.
3. Click the three vertical dots in the upper-right of the message.
4. Click "Show Original."



Here, you'll see a brief breakdown of the information found in the header. If you scroll down, you can also see the full text of the email header, which will end just before the body content of the message.

From there, you can copy the email header into an email header analysis tool to learn more details.

How to Analyze Email Headers in Outlook



Here's how to obtain your email header in Outlook:

1. Open Microsoft Outlook.
2. Click on the message you want to analyze.
3. Click on the dropdown arrow in the upper-right of the message.
4. Click "View message details."

Here, you'll see the full text of the email header.

From there, you can copy the email header into an email header analysis tool to learn more details.

Email Header Analyzer Tools

Once you have a copy of the email header, you can analyze it using one of the following email header analysis tools.

Almost all of these tools are free, and function in the same way, so I won't go into detail describing the minor differences. With all of them, you'll copy and paste your email header, click a button, and review the information after it is parsed.

1- Mx Toolbox.

Mx Toolbox has a great standalone email header analyzer, as well as detailed information on email headers for the uninitiated:

Website: https://mxtoolbox.com/EmailHeaders.aspx

2- G Suite Toolbox Messageheader.

If you're already using Gmail, you might as well try:

Website: https://toolbox.googleapps.com/apps/messageheader/

3- Mailheader.org.

There's also Mailheader.org, where you can review mail header samples in addition to the header you've selected.

Website : https://mailheader.org/

4- Azure Header Analyzer:

Website : https://mha.azurewebsites.net/

5- Gaijin

In case you needed more options, you could also try:

Website : https://www.gaijin.at/en/tools/e-mail-header-analyzer

URL / IP Reputation Check

If you need to check the IP or domain you can try below tools:

- Virustotal: https://www.virustotal.com/gui/home/search
- Talosintelligence: https://www.talosintelligence.com/
- AbuseIPdb: https://www.abuseipdb.com/
- WebCheck: https://web-check.xyz/
- CyberGordon: https://cybergordon.com/

Visualization Tools and Sandbox

Visualize a malicious URL without visiting the site:

- URLScan: https://urlscan.io/
- URL2PNG: https://www.url2png.com/
- CheckPhish: https://lnkd.in/ejERWRXV
- browserling: https://www.browserling.com/

Check email attachment

If the email has attachment you can check the attachment using below tools:

- VirusTotal: https://www.virustotal.com/gui/home/search
- Anyrun Sandboxing: https://any.run/
- Hybrid-Analysis Sandboxing: https://www.hybrid-analysis.com/
- Joesandbox: https://www.joesandbox.com/#windows
- Cuckoo Sandbox: https://cuckoo.cert.ee/
- CapeSandbox: https://capesandbox.com/
- Triage: https://tria.ge/dashboard

Whois domain record

Centralops:

Website : https://centralops.net/co/

DomainTools:

Website : https://reverseip.domaintools.com/

Whois:

Website :https://www.whois.com/

Phishing analysis tool

Automatically Collecting Artifacts:

- Phish Tool: https://www.phishtool.com/
- EML analyzer: https://eml-analyzer.herokuapp.com/#/
- CyberChef: https://gchq.github.io/CyberChef/

Protecting Yourself from Phishing

Phishing attacks are a common method used by cybercriminals to trick individuals into revealing sensitive information or downloading malware. It is essential to take proactive measures to protect yourself and your organization from these threats. Here are some key steps to follow:

Phishing Protection Measures

Step	Description
1. Be Cautious of Unsolicited Emails	Avoid opening emails from unknown senders or suspicious email addresses. Be wary of emails requesting personal or financial information.
2. Avoid Clicking on Suspicious Links	Do not click on links in emails or messages from unknown sources. Hover over links to check the URL before clicking.
3. Avoid Downloading Attachments	Do not download attachments from untrusted sources, especially if they are executable files (e.g., .exe) or macros in documents.
4. Keep Software and Antivirus Programs Up to Date	Regularly update your operating system, web browsers, and antivirus software to ensure they have the latest security patches.
5. Regularly Change Passwords	Use strong, unique passwords for each online account and change them regularly. Enable two-factor authentication whenever possible.
6. Educate Yourself and Others	Stay informed about the latest phishing techniques and educate yourself and others about how to identify and report phishing attempts.
7. Report Phishing Attempts	If you receive a phishing email, report it to your organization's IT department or the appropriate authorities. Do not respond to or engage with the sender.