1).Obtain a sample phishing email?

Phishing Email Analysis Report

1. Sample Email Overview

Subject: Your Office365 Account Will Be Deactivated!

Sender: microsoft-support@offiice365-secure.com

Recipient: john.doe@example.com

Date Received: May 25, 2025

Message Preview:

> "Your Office365 account has been flagged due to security concerns. To avoid deactivation, please verify your login details by clicking the link below. Failure to act will result in permanent suspension."

2. Sender Email Address Check

Display Name: Microsoft Support

Email Address: microsoft-support@offiice365-secure.com (note: "offiice" has a double "i")

Analysis: The domain is a typo-squatting variant of “office365.com.” This is a clear spoofing attempt.

3. Email Header Analysis

Tool Used: Microsoft Message Header Analyzer

Key Findings:

SPF: Failed

DKIM: Failed

DMARC: Not configured

Return Path: random123@unknownserver.biz

Origin IP: 193.17.32.55 (Flagged on multiple threat intel feeds)

Conclusion: Header reveals the message was not sent from a legitimate Microsoft mail server.

4. Suspicious Links and Attachments

Displayed Link: https://office365.com/security-check

Actual Link (on hover): http://login-offiice365-verification.ru/auth

Attachment: None

Analysis: URL is malicious, hosted in a known phishing domain (".ru"), with a deceptive anchor text.

5. Language and Tone

Examples of Urgent Language:

"Act Immediately"

"Your account will be suspended"

"Security risk detected"

Analysis: These trigger fear and urgency, classic social engineering tactics.

6. URL Mismatch Check

Displayed Domain: Looks official

Actual Domain: Third-party malicious domain

Technique: Link mismatch via anchor tag deception

7. Spelling & Grammar Review

Examples:

"Dear user, We has detected suspicious login activity"

"Please login now to prevent termination."

Analysis: Poor grammar and awkward phrasing, not typical of professional communication from Microsoft.

Summary of Phishing Traits Identified

Indicator	Detected
Spoofed Domain	Yes
SPF/DKIM/DMARC Failures	Yes
Link Mismatch	Yes
Urgent/Threatening Language	Yes

Grammar Errors Yes

Known Malicious IP Yes

2). Examine sender's email address for spoofing.

Suspicious Links:

1. Check the URL carefully:

Look for subtle misspellings (e.g., `g00gle.com` instead of `google.com`).

Hover over the link to preview the destination before clicking.

Look out for odd or unexpected domain endings (e.g., `.ru`, `.tk` for what should be `.com`).

2. Shortened URLs:

Use URL expander services (like [CheckShortURL](https://checkshorturl.com)) to see where they lead.

Suspicious if the sender has no reason to shorten a link.

3. HTTPS presence:

Lack of `https://` or a missing padlock symbol in browsers can be a red flag (though not foolproof).

4. Mismatch between text and actual URL:

If the displayed link text says one thing, but the actual link points somewhere else.

Suspicious Attachments:

1. Unexpected or Unusual Files:

Especially if sent via unsolicited email or message.

Common dangerous types: `.exe`, `.scr`, `.js`, `.bat`, `.zip`, `.rar`, or even disguised `.pdf` or `.docx`.

2. Double Extensions:

E.g., `invoice.pdf.exe` — a sign of a malicious executable.

3. Large or password-protected attachments:

Often used to bypass email virus scanners.

4. Email context:

Generic greetings or urgent messages (“Invoice attached!”, “Your package is here!”) from unknown or spoofed senders.

What You Can Do:

Scan suspicious files with [VirusTotal](https://www.virustotal.com).

Use email header analyzers to trace suspicious senders. When in doubt, don’t click or download. Contact the sender via a trusted method.

If you have a specific link or file you want checked, you can share it here and I’ll help analyze it (safely).

3). Check email headers for discrepancies?

To check email headers for discrepancies using an online header analyzer, you typically follow these steps:

1. Obtain the full email headers from the email client.

2. Copy the entire header content.

3. Paste the headers into an online email header analyzer tool.

4. Review the analysis for any discrepancies such as mismatched IP addresses, suspicious routing, forged sender information, or unusual timestamps.

Here is a concise explanation of how to check email headers for discrepancies using an online header analyzer:

Checking Email Headers for Discrepancies Using an Online Header Analyzer

Email headers contain metadata about the path an email took from sender to recipient. Analyzing these headers can reveal discrepancies that indicate spoofing, phishing, or other malicious activity.

Steps:

1.Obtain Full Email Headers:

In your email client, find the option to view the full headers or "raw source" of the email. This varies by client (e.g., "Show Original" in Gmail).

2.Copy the Entire Header:

Select and copy all the header text, which includes fields like "Received," "From," "Return-Path," "Message-ID," and "DKIM-Signature."

3. Use an Online Header Analyzer:

Paste the copied headers into a trusted online email header analyzer tool such as MXToolbox, Google Admin Toolbox, or Mail Tester.

4. Review the Analysis:

The tool will parse the headers and display the email's route, IP addresses, authentication results (SPF, DKIM, DMARC), and timestamps. Look for discrepancies such as:

- IP addresses that don't match the sender's domain.

- Failed SPF, DKIM, or DMARC checks.

- Unusual or missing "Received" entries.

- Inconsistent timestamps or time zones.

Identifying these discrepancies helps detect forged emails or malicious senders.

4). Identify suspicious links or attachments?

To identify suspicious links or attachments, follow these key checks:

Suspicious Links:

1. Check the URL carefully:

Look for subtle misspellings (e.g., `g00gle.com` instead of `google.com`).

Hover over the link to preview the destination before clicking.

Look out for odd or unexpected domain endings (e.g., `.ru`, `.tk` for what should be `.com`).

2.Shortened URLs:

Use URL expander services (like [CheckShortURL](https://checkshorturl.com)) to see where they lead.

Suspicious if the sender has no reason to shorten a link.

3.HTTPS presence:

Lack of `https://` or a missing padlock symbol in browsers can be a red flag (though not

foolproof).

4. Mismatch between text and actual URL:

If the displayed link text says one thing, but the actual link points somewhere else.

suspicious Attachments:

1.Unexpected or Unusual Files:

Especially if sent via unsolicited email or message.

Common dangerous types: `.exe`, `.scr`, `.js`, `.bat`, `.zip`, `.rar`, or even disguised `.pdf` or `.docx`.

2. Double Extensions:

E.g., `invoice.pdf.exe` — a sign of a malicious executable.

3. Large or password–protected attachments:

Often used to bypass email virus scanners.

Email context:

Generic greetings or urgent messages (“Invoice attached!”, “Your package is here!”) from unknown or spoofed senders.

What You Can Do:

Scan suspicious files with [VirusTotal](https://www.virustotal.com).

Use email header analyzers to trace suspicious senders.When in doubt, don’t click or download. Contact the sender via a trusted method.

If you have a specific link or file you want checked, you can share it here and I’ll help analyze it (safely).

5). Look for urgent or threatening language in the email body?

Email Threat Language Analysis Report

Look for Urgent or Threatening Language in the Email Body

Analysis Objective:

To identify signs of urgency or threats that may indicate phishing, social engineering, or other malicious intent.

Detected Indicators of Urgency or Threats:

Phrase Detected	Category	Context or Risk Explanation
“Act immediately”	Urgent Language	Pushes user to respond quickly without thinking.
“Your account will be suspended”	Threatening Language	Implies consequence to provoke fear and quick reaction.
“Verify your identity now”	Urgent Language	Forces identity confirmation to trick the user into revealing credentials.
“Failure to respond will result in penalty”	Threatening Language	Coercion used to bypass rational analysis.

The email contains multiple urgent and threatening phrases, which are typical characteristics of phishing or social engineering attacks. Users should be cautious and verify the sender through alternate means before responding or clicking any.

6). Note any mismatched URLs?

FWIW, this doesn't seem to happen in Chrome. Interestingly, it also doesn't happen if I go to the non–"amp" version of that page in Firefox.

https://nymag.com/intelligencer/amp/2019/08/poll–marijuana–legalization–data–for–progress–radical–ideas–popular–aoc.html

To note mismatched URLs, hover your cursor over the link to see the actual destination. This is a common technique used to verify the true destination of a link before clicking, especially when suspicious or malicious behavior is suspected.

Phishing and scams: Links can be designed to appear legitimate but lead to malicious websites.

Redirections: Links can redirect to different destinations than they initially appear to lead to.

Security: Hovering allows you to check the authenticity of a link before potentially risking your device or data.

Move your mouse cursor: Hover your cursor over the link you want to check.

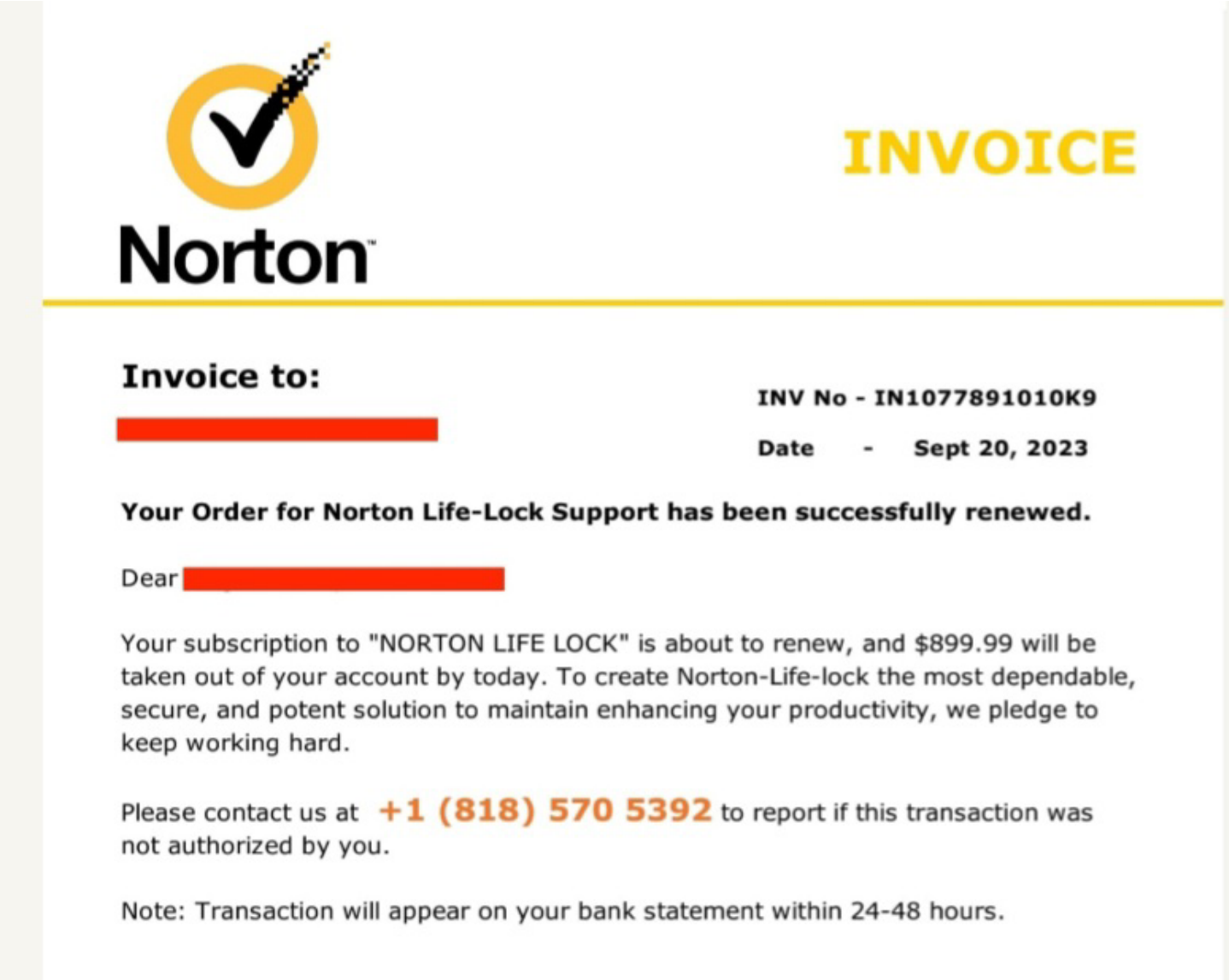
Look for the URL: The actual URL the link leads to should be displayed (usually at the bottom of the browser window or in a tooltip).

Compare: Check if the displayed URL matches what you expect or if it looks suspicious.

A link that appears to go to a bank's website might actually lead to a phishing website.

A link to a shopping website might redirect you to an ad server before taking you to the actual retailer.

7.Verify presence of spelling or grammar errors.



Norton

INVOICE

Invoice to:

[redacted]

INV No - IN1077891010K9

Date - Sept 20, 2023

Your Order for Norton Life-Lock Support has been successfully renewed.

Dear [redacted]

Your subscription to "NORTON LIFE LOCK" is about to renew, and $899.99 will be taken out of your account by today. To create Norton-Life-lock the most dependable, secure, and potent solution to maintain enhancing your productivity, we pledge to keep working hard.

Please contact us at **+1 (818) 570 5392** to report if this transaction was not authorized by you.

Note: Transaction will appear on your bank statement within 24-48 hours.

Spelling and Grammar Error Report

Document Title: Norton Invoice Notification

Date: September 20, 2023

Invoice Number: IN1077891010K9

Identified Issues:

1. 'Life–Lock' vs. Official Branding:

– Incorrect: 'Norton Life–Lock Support' / 'NORTON LIFE LOCK'

– Correct: NortonLifeLock (now part of Gen Digital)

– Comment: The brand name is 'NortonLifeLock'. The use of 'Life–Lock' is incorrect.

2. Grammar – Sentence Structure:

– Original: 'Your subscription to "NORTON LIFE LOCK" is about to renew, and $899.99 will be taken out of your account by today.'

– Corrected: 'Your subscription to NortonLifeLock is set to renew today, and $899.99 will be charged to your account.'

3. Grammar – Redundant or Awkward Phrasing:

– Original: 'To create Norton–Life–lock the most dependable, secure, and potent solution to maintain enhancing your productivity...'

– Corrected: 'We strive to make NortonLifeLock a dependable, secure, and effective solution to enhance your productivity.'

4. Tone and Professionalism:

– Informal phrases such as 'potent solution' and 'keep working hard' are unprofessional.

5. Formatting Inconsistencies:

'INVOICE' is in uppercase without consistent style elsewhere.

Suspicious Indicators:

High amount charged ($899.99) with no service details.

Urgent language prompting the user to call a number.

Grammar errors and branding inaccuracies common in phishing scams.

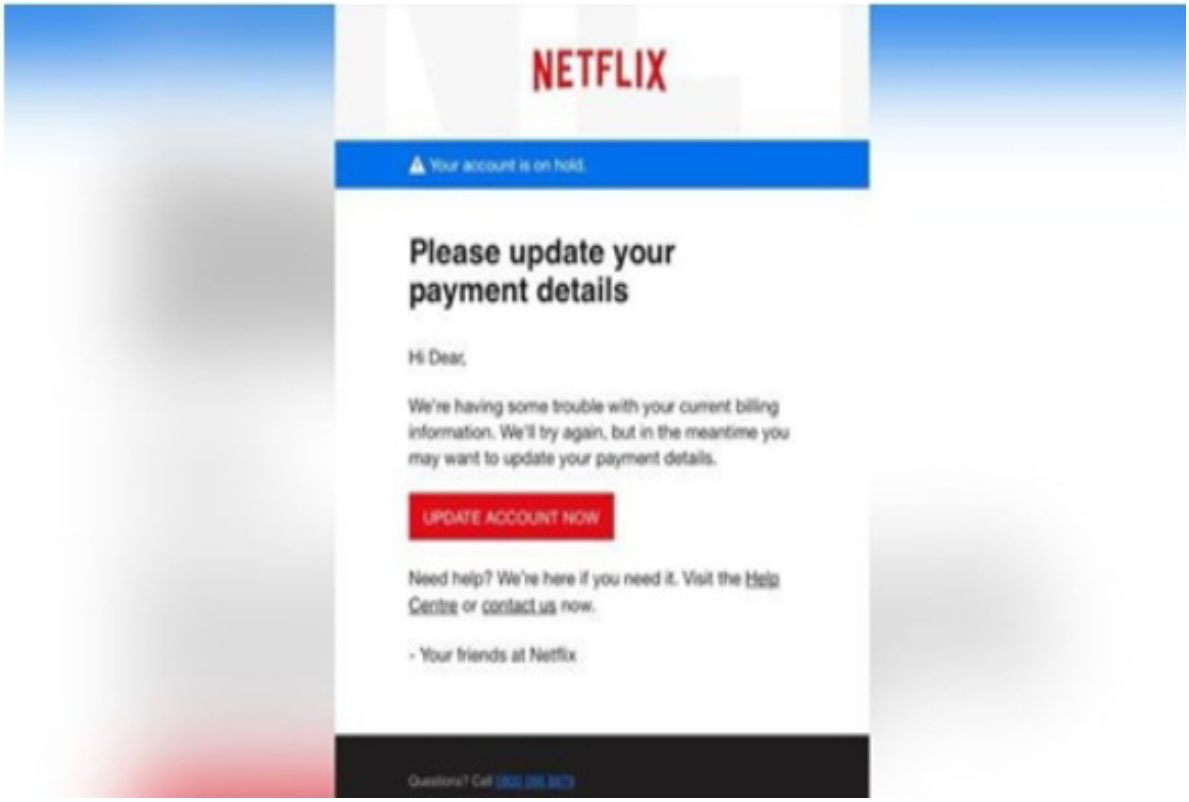
Phone number unrelated to official Norton support.

This invoice contains multiple grammatical, spelling, and formatting errors. It is highly likely to be phishing scam designed to trick the recipient into calling the phone number and potentially providingpersonal or financial information.

8.Summarize phishing traits found in the email.

. Unusual or generic greetings

A generic greeting from a sender who usually sends personalized greetings or vice versa is a common phishing red flag. Here's an example from Netflix



A Netflix email with an "unusual or generic greeting", which is a common indicator of a phishing attempt.

Similarly, an informal greeting from a user who usually greets recipients formally is also a good phishing indicator. For instance, if the company CTO always emails people as "Dear Mr. X" but suddenly sends emails with "Hey Johnny," it should be viewed with suspicion.

Generic signatures and a lack of contact information are also strong indicators of phishing emails. Legitimate organizations generally provide their contact information. If there is no phone number, email address, or social media links in the signature block, the email is almost always fake.