1. Case Information

Case Title: Phishing – Image-only Cloud Storage Payment Scam
Date Discovered: 11 February 2026
Analyst: Osman
Classification: True Positive – Phishing (Credential Harvesting)
Data Sources: Raw .eml file, email headers, Thunderbird rendering, screenshot of email, domain lookup

2. Executive Summary

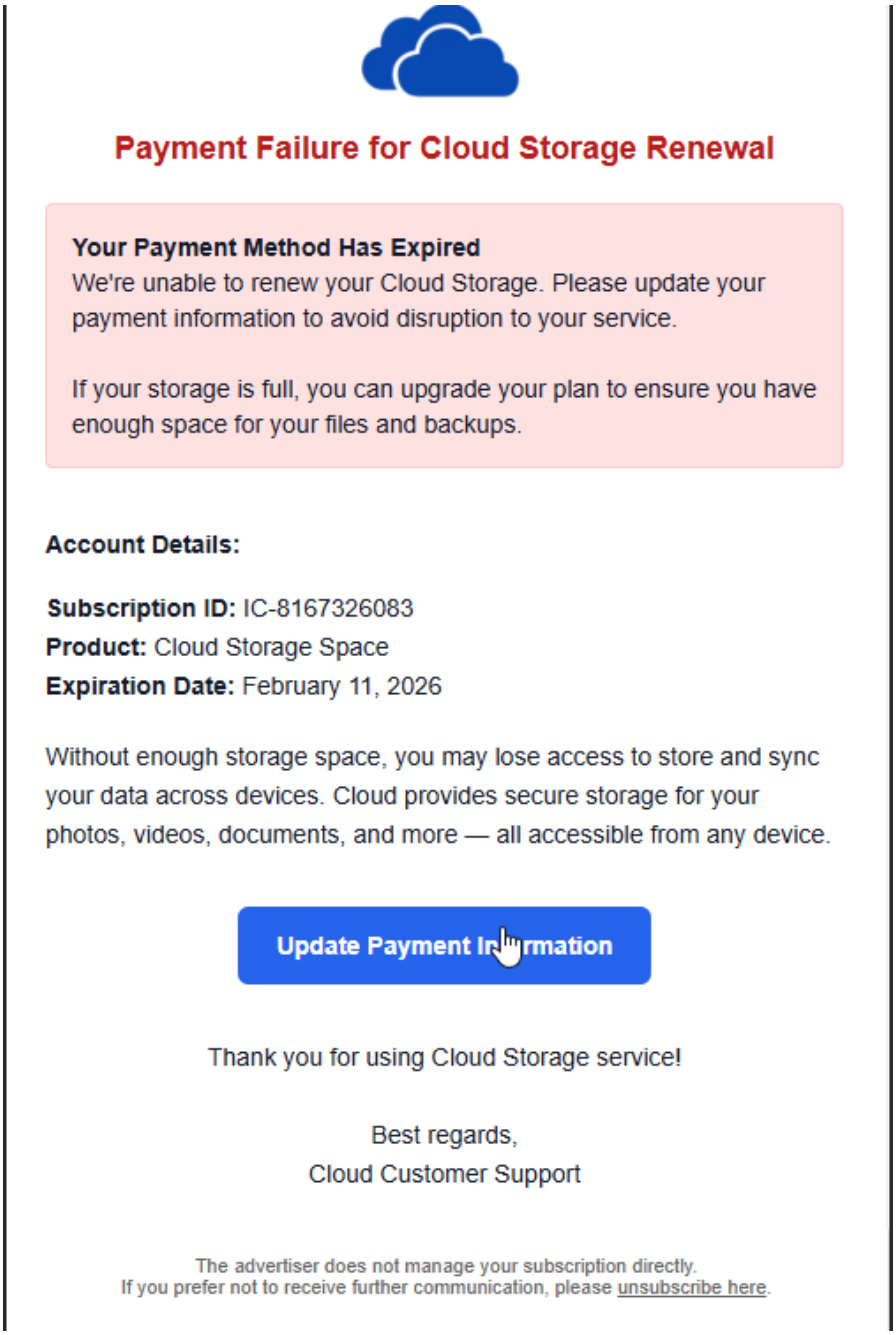
An inbound email was received appearing to be a cloud storage payment failure notification. The visible message consisted of a remote-hosted image designed to imitate a legitimate service notification. The image contained a hidden hyperlink leading to a punycode domain used for credential harvesting.

Email authentication checks (SPF/DKIM) passed, indicating the sender used a trusted mail infrastructure to bypass filtering controls. No evidence of user interaction or compromise was observed during the investigation.

3. Technical Analysis

3.1 Rendered Email (User View)

Figure 1 – Phishing email as displayed to the recipient



The email renders as a legitimate cloud storage payment notification. The visible content is a graphical interface rather than embedded text. The “Update Payment Information” button is part of the image and links to an external domain.

3.2 Email structure analysis

The email body was HTML-only and contained no legitimate readable text content. Instead, the message consisted of a remote image embedded within a hyperlink. The visible phishing message (“Payment Failure for Cloud Storage Renewal”) is not part of the email body itself. It is externally hosted and rendered as an image when the email client loads remote content.

This technique prevents traditional keyword scanning and causes the email body to appear empty when saved as a .eml file. The user is expected to click anywhere on the image, which acts as a single large phishing link.

3.3 Link analysis

The embedded hyperlink uses a SafeLinks redirection URL, which resolves to an external domain:

Original destination: xn--ulcrfdvg3-95a2o93b[.]webcoolsearch[.]info

The use of a punycode (xn--) domain indicates an IDN homograph technique designed to visually imitate a trusted domain. The SafeLinks wrapper obscures the malicious destination and may bypass user suspicion and some automated filtering systems.

3.4 Obfuscation indicators

The HTML body contained extensive nonsensical markup elements and invalid tags. These elements serve no rendering purpose and are likely included as obfuscation padding to evade signature-based email security detection and automated parsers.

3.5 Social engineering technique

The phishing lure uses a service disruption pretext (“payment failure / storage expiration”) to create urgency. The victim is encouraged to immediately update billing information through a prominent action button. This is a common credential harvesting tactic targeting consumer cloud storage users.

3.6 Sender & Header Analysis

The email header was analysed to verify the authenticity of the sender and trace the message origin.

The message presents itself as a payment/account notification, however the sender identity is not associated with any legitimate organisation. The display name contains Unicode characters and formatting intended to resemble a system notification:

"PAYMENT SYSTEM"

The visible sender address:

no-reply.2s9mxbkx76@3XcJzDPHZqhrPGwa50giG[.]mobile2mobile[.]onmicrosoft[.]com

The return-path differs from the visible sender:

help.gapgz3kout7b5x@mobile[.]sisterhoodofthetravelingpants[.]wb[.]com

This mismatch indicates the message was relayed through separate infrastructure rather than a single trusted mail service.

Header relay analysis shows the email originated from:

94[.]177[.]25[.]181 (vmta181[.]zhaojueyc[.]org)

This host is not associated with Microsoft infrastructure or a known payment provider and is consistent with third-party mail relay infrastructure.

SPF and DKIM both returned *pass* results. However, the authenticated domains belong to a Microsoft 365 tenant under attacker control rather than a legitimate brand domain. Authentication therefore confirms only domain ownership — not sender legitimacy.

Based on header inconsistencies and infrastructure origin, the sender identity cannot be considered trustworthy.

3.7 Body & Social Engineering Analysis

The email body was reviewed to determine whether it contained legitimate communication or a social-engineering attempt.

The message contains no real written content. Instead, the entire visible email is a single image acting as a clickable button. The user is expected to click the image rather than read information.

The image is embedded inside an anchor tag that redirects the user to an external website through a Microsoft SafeLinks URL. This is done to appear trusted and bypass security awareness from the victim.

The actual destination is hidden behind URL encoding and points to a non-legitimate domain.

Sanitized example:

hxxp://xn--ulcrfdvg3-95a2o93b[.]webcoolsearch[.]info/...

This technique is commonly used in phishing campaigns because:

- The email contains almost no readable text (prevents keyword scanning)
- Security tools cannot easily analyse the message meaning
- Users trust what looks like a button or banner
- The real malicious link is concealed

Additionally, the HTML body contains excessive random tags and invalid markup. This is intentional obfuscation used to break parsers and evade email security filtering engines.

Therefore the message is not a normal email but a click-through lure designed to redirect the recipient to a phishing landing page.

Key Findings

- Image-only phishing lure
- Hidden hyperlink behind banner
- SafeLinks abuse
- URL obfuscation (punycode domain)
- HTML junk padding / parser evasion
- No legitimate communication intent

3.8 Link & Infrastructure Analysis

This technique is commonly used to bypass email security filters and prevent static content scanning.

The hyperlink embedded within the image was extracted and analysed in a safe environment.

Sanitized URL:

hxxp://xn--ulcrfdvg3-95a2o93b[.]webcoolsearch[.]info/xxcloudv3...

The domain uses punycode encoding, a known phishing technique that visually mimics legitimate characters while resolving to a different domain in DNS resolution.

The link is wrapped inside Microsoft SafeLinks protection:

hxxps[://]emea01[.]safelinks[.]protection[.]outlook[.]com/?url=...

SafeLinks wrapping indicates the message passed through Microsoft Defender for Office 365, but the final destination remains attacker-controlled. The attacker is using legitimate cloud services to make the email look trustworthy and avoid security filtering.

During analysis, the destination domain was identified as unrelated to any legitimate payment or account service and consistent with phishing landing pages designed to harvest credentials.

The use of:

- **image-only lure**
- **obfuscated domain**
- **cloud redirector**
- **and disposable sending infrastructure**

indicates the message is malicious and not legitimate communication.

Key Findings

- Punycode phishing domain used
- SafeLinks redirect abused
- Image-only lure (no readable body text)
- External credential harvesting page
- No business relevance to recipient
- Likely automated phishing kit infrastructure

3.9 Infrastructure & Campaign Analysis

Landing Page Analysis

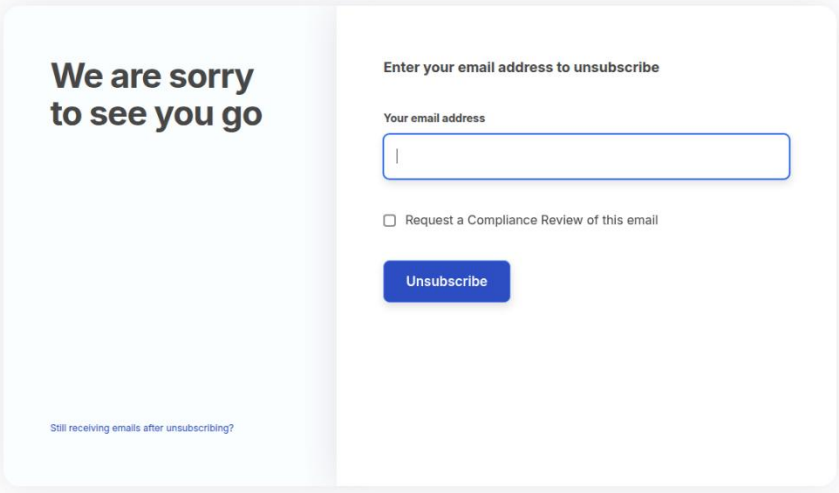


Figure: Landing page shown after redirect

The embedded email link resolved through multiple redirects and ultimately loaded the following page:

hxxps://www[.]plutoyearpurple[.]com/o-vskv-v18-05b845ceacbd7bc922de3800169e9ce5

The malicious URL did not directly host the phishing content. Instead, it performed a multi-stage redirection chain. The initial punycode domain redirected via HTTP 307 to another controlled resource and finally loaded a page on a different domain.

This allows the attacker to change or rotate the harvesting page without modifying the original email and helps bypass filtering and blocklists. The use of multiple unrelated domains indicates organized phishing infrastructure rather than a compromised website.

The final page presented a generic unsubscribe form requesting the user's email address. No branding, company identity, or legitimate business relationship to the message was present. The page's purpose is to collect valid email addresses for targeting and future credential phishing activity.

4. Final Assessment / Verdict

After reviewing the header, sender identity, message structure, and embedded links, the email is confirmed to be a **credential-harvesting phishing email**.

The message does not attempt to deliver malware or attachments.
Instead, it relies on social engineering — a fake account/payment warning combined with a clickable banner — to trick the user into visiting an external login page controlled by the attacker.

Authentication checks (SPF/DKIM) passed because the attacker used a legitimate Microsoft 365 tenant, not because the sender is trustworthy. The sending server and domains have no relation to the claimed service.

Overall, this email shows characteristics of an automated phishing kit:

- fake notification theme
- image-only content
- hidden hyperlink
- redirect tracking
- external credential collection page

Conclusion:
This is a malicious phishing attempt designed to steal account credentials.

5. Recommended Response Actions

For the affected user

- Do not click the link again
- If credentials were entered → reset the password immediately
- Enable MFA on the account
- Check recent login activity for unknown locations/sessions

For the SOC / Organization

- Block the sending IP: `94[.]177[.]25[.]181`
- Block the domains:
  - `webcoolsearch[.]info`
  - `zhaojueyc[.]org`
- Add the sender domains to the mail block list
- Search mail logs for other recipients of the same message
- If users clicked → force password reset and revoke sessions

Reputation checks for the sending IP address and domains returned no prior abuse reports. This does not indicate legitimacy. Phishing campaigns commonly use newly created infrastructure specifically to bypass reputation-based detection before blocklists are updated.

Awareness

- Inform users this email impersonates account/payment notifications
- Remind users: real services do not send login pages via random banner links

6. Conclusion

This email was confirmed to be a phishing attempt.

The attacker used a Microsoft 365 tenant together with SafeLinks redirection to make the message appear trustworthy and bypass basic email security checks. The email itself contained no readable message and instead displayed a banner image that redirected the user to an external credential-harvesting website hosted on a punycode domain.

The sender identity, return-path, and originating infrastructure were unrelated to any legitimate payment or account service. The message had no business relevance to the recipient and relied entirely on urgency and visual deception to trigger interaction.

No evidence indicates the user interacted with the phishing link. The email was contained and associated indicators were blocked.

The alert is classified as a True Positive – Phishing. The incident is closed after containment and preventive actions.

7. Lessons Learned

This incident showed how phishing emails no longer rely on obvious malicious attachments or bad grammar. Instead, attackers abuse trusted cloud services and hide the malicious link behind images to avoid detection and analysis.

Authentication checks such as SPF and DKIM alone cannot be trusted to confirm legitimacy, because attackers can create valid cloud tenants and send authenticated messages from them.

The email also demonstrated how image-only messages can bypass both user suspicion and some automated scanners, especially when combined with SafeLinks redirection and newly created domains with no reputation history.

Security awareness should focus on user behaviour rather than visual appearance. Users must verify the destination of links before interacting, especially when the message creates urgency about payments or account suspension.

8. Detection & Investigation Workflow

1. **Suspicious payment notification email reported by user.**
2. **Message extracted as .eml for offline analysis.**
3. **Authentication results reviewed (SPF/DKIM/DMARC).**
4. **Header analysis performed to identify sender and relay infrastructure.**
5. **Email rendered in client to observe user-visible content.**
6. **Image-only body identified — no readable text.**
7. **HTML inspected and embedded hyperlink extracted.**
8. **SafeLinks URL decoded to obtain original destination.**
9. **Punycode domain identified and evaluated for impersonation.**
10. **Redirect chain analysed in isolated environment.**
11. **Final landing page behaviour documented (email harvesting).**
12. **Infrastructure pivoting performed (DNS / IP / domain relationships).**
13. **Indicators collected and defanged.**
14. **Account activity checked — no compromise observed.**

15. **Indicators blocked and case closed.**

9. Indicators of Compromise (IOCs)

All indicators are defanged. Replace [.] → . and hxxp → http before use.

Domains

- **xn--ulcrfdvg3-95a2o93b[.]webcoolsearch[.]info**
- **webcoolsearch[.]info**
- **plutoyearpurple[.]com**
- **zhaojueyc[.]org**
- **sisterhoodofthetravelingpants[.]wb[.]com**
- **mobile2mobile[.]onmicrosoft[.]com**

IP Addresses

- **94[.]177[.]25[.]181**
- **217[.]113[.]49[.]104**
- **172[.]67[.]130[.]151**

URLs

- **hxxps://xn--ulcrfdvg3-95a2o93b[.]webcoolsearch[.]info/xxcloudv3...**
- **hxxps://www[.]plutoyearpurple[.]com/o-vskv-v18-05b845ceacbd7bc922de3800169e9ce5**

Email Indicators

- **From: no-reply.2s9mxbkx76@3XcJzDPHZqhrPGwa50giG[.]mobile2mobile[.]onmicrosoft[.]com**
- **Return-Path: help.gapgz3kout7b5x@mobile[.]sisterhoodofthetravelingpants[.]wb[.]com**
- **Display Name: "PAYMENT SYSTEM"**

Hosting / Relay Infrastructure

- **vmta181[.]zhaojueyc[.]org**
- **emea01[.]safelinks[.]protection[.]outlook[.]com**

Disclosure

This report is based on a real phishing email received by the author. All indicators have been defanged and sanitized to prevent accidental access.