aryaka

Scam in the Cloud

How Fraudsters Exploit Google Cloud Storage (GCS) for Deceptive Campaigns

Aryaka Threat Research Lab

Bikash Dash, Varadharajan Krishnasamy

Table of Contents

Introduction

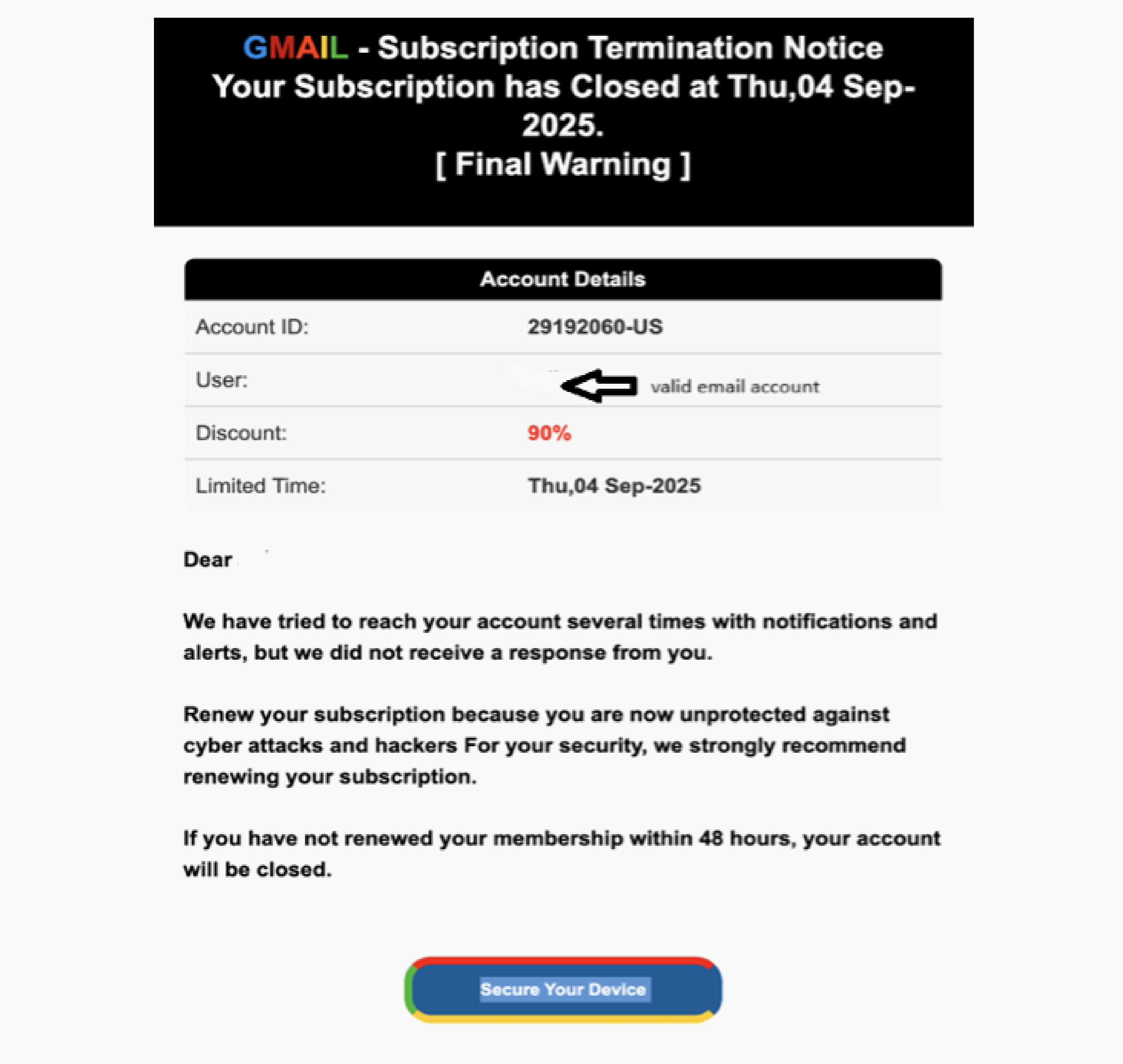
Scam campaigns continue to evolve, blending legitimate cloud infrastructure with deceptive tactics to bypass both human caution and technical safeguards. In recent months, one recurring trend has been the abuse of Google Cloud Storage (GCS) — a service typically used to host files and websites — to deliver highly convincing email- and web-based scams. These campaigns exploit trusted domains, sometimes pass basic authentication checks like SPF, and redirect users through multiple legitimate services before prompting them to provide personal information or make payments. This article examines how these scams operate, why they are effective, and what lessons defenders can draw from them.

Email as the Scam Vector

The scam begins with an email that appears authentic and urgent. The subject lines often mimic service notifications from popular brands like Gmail, Google Drive, or even internal corporate alerts. The language is clean and professional, free from the usual grammatical errors that characterized older scams. Recipients are urged to verify their accounts, review a pending document, or “secure their mailbox” to avoid suspension.

These messages are dangerous because the sender information looks legitimate at first glance. The emails often pass **SPF (Sender Policy Framework)** validation, meaning the sending IP address is authorized for the domain that appears in the SMTP envelope. This small success is enough to convince many email filters that the message is safe. However, deeper inspection shows that **DKIM (DomainKeys Identified Mail)** signatures either fail validation or are missing entirely, meaning the message wasn’t cryptographically signed by the domain it claims to represent. When SPF passes but DKIM fails, the message presents mixed signals to email gateways — and if **DMARC (Domain-based Message Authentication, Reporting & Conformance)** is not strictly enforced by the sender domain, these scam emails often slip through.

In our investigation, we observed a suspicious message delivered to Gmail with the subject line "Subscription Termination Notice," as shown in the Figure 1.



GMAIL - Subscription Termination Notice
Your Subscription has Closed at Thu,04 Sep-2025.
[Final Warning]

Account Details	
Account ID:	**29192060-US**
User:	valid email account
Discount:	**90%**
Limited Time:	**Thu,04 Sep-2025**

Dear

We have tried to reach your account several times with notifications and alerts, but we did not receive a response from you.

Renew your subscription because you are now unprotected against cyber attacks and hackers For your security, we strongly recommend renewing your subscription.

If you have not renewed your membership within 48 hours, your account will be closed.

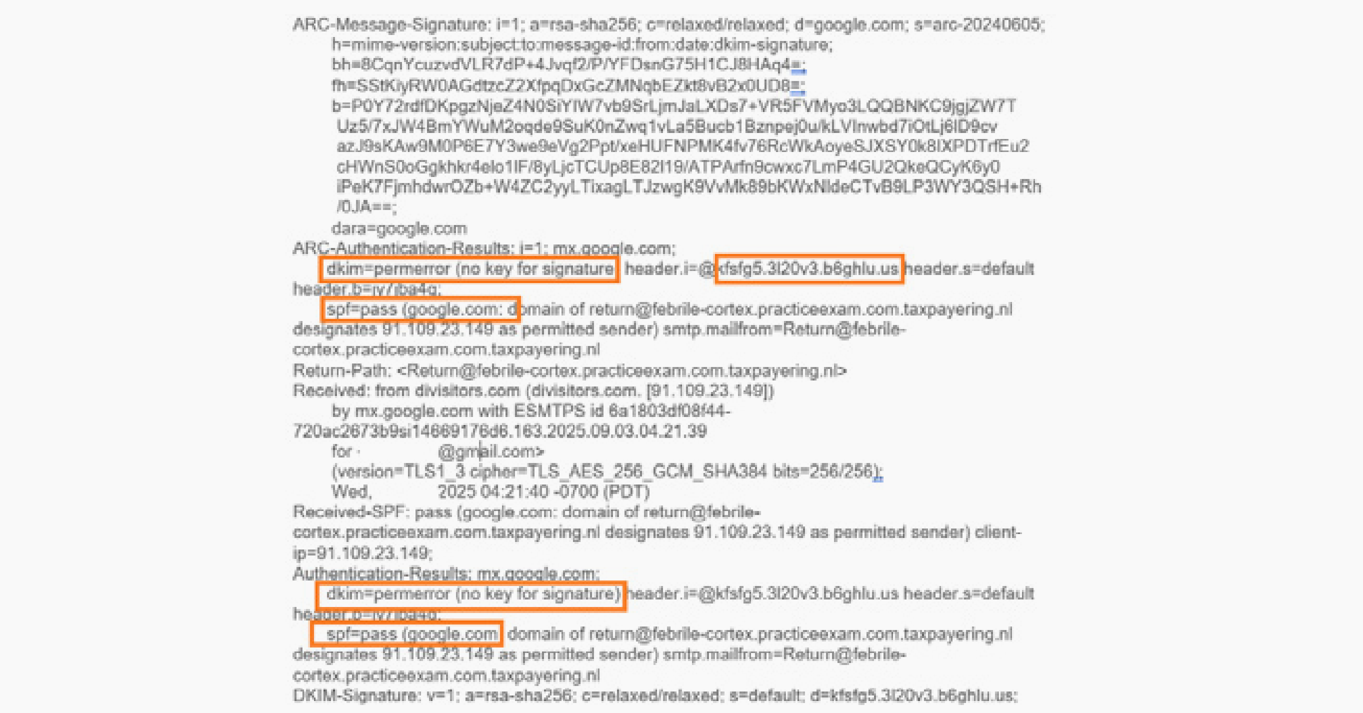
Figure 1- Suspicious Gmail message

The initial email typically contains a link that looks harmless: a **Google Cloud Storage URL** such as storage.googleapis.com/bucket-name/index.html. Because the link points to a highly trusted domain owned by Google, users are far more likely to click it. Many anti-phishing systems also treat these domains as safe, which allows the email to reach the inbox without triggering warnings.

Understanding SPF, DKIM, and DMARC in This Context

To understand why these phishing emails work, it's important to look at how authentication mechanisms interact. **SPF** checks whether the sending IP is allowed to send email for a specific domain, but it doesn't verify the content of the message. **DKIM** adds a digital signature that ensures the message body and headers haven't been tampered with and ties them to a domain identity. **DMARC** then ties everything together — it ensures that the visible "From" address aligns with the domain that passed SPF or DKIM.

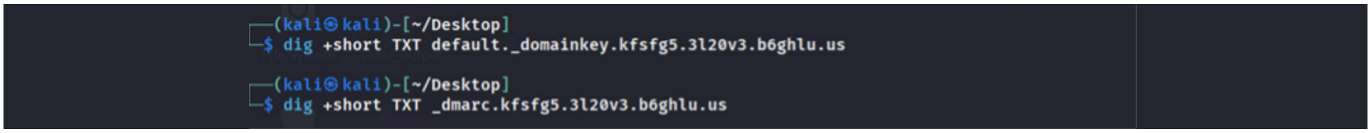
As we can see in the Figure 2, when SPF passes and DKIM fails, and if DMARC is either missing or set to "none," attackers gain an opening. They can send emails through servers authorized for a related domain, pass SPF, and still appear trustworthy. Without a strict DMARC policy instructing receivers to quarantine or reject mismatched messages, these spoofed messages are delivered successfully.



```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
       h=mime-version:subject:to:message-id:from:date:dkim-signature;
       bh=8CqnYcuzvdVLR7dP+4Jvqf2/P/YFDsnG75H1CJ8HAq4=;
       fh=SStKiyRW0AGdtzcZ2XfpqDxGcZMNqbEZkt8vB2x0UD8=;
       b=P0Y72rdfDKpgzNjeZ4N0SiYIW7vb9SrLjmJaLXDs7+VR5FVMyo3LQQBNKC9jgjZW7T
        Uz5/7xJW4BmYWuM2oqde9SuK0nZwq1vLa5Bucb1Bznpej0u/kLVlnwbd7iOtLj6ID9cv
        azJ9sKAw9M0P6E7Y3we9eVg2Ppt/xeHUFNPMK4fv76RcWkAoyeSJXSY0k8IXPDTrfEu2
        cHWnS0oGgkhkr4elo1IF/8yLjcTCUp8E82I19/ATPArfn9cwxc7LmP4GU2QkeQCyK6y0
        iPeK7FjmhdwrOZb+W4ZC2yyLTixagLTJzwgK9VvMk89bKWxNldeCTvB9LP3WY3QSH+Rh
        /0JA==;
       dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
      dkim=permerror (no key for signature) header.i=@kfsfg5.3l20v3.b6ghlu.us header.s=default
header.b=iy/iba4q;
      spf=pass (google.com: domain of return@febrile-cortex.practiceexam.com.taxpayering.nl
designates 91.109.23.149 as permitted sender) smtp.mailfrom=Return@febrile-
cortex.practiceexam.com.taxpayering.nl
Return-Path: <Return@febrile-cortex.practiceexam.com.taxpayering.nl>
Received: from divisitors.com (divisitors.com. [91.109.23.149])
       by mx.google.com with ESMTPS id 6a1803df08f44-
720ac2673b9si14669176d6.163.2025.09.03.04.21.39
       for ·              @gmail.com>
       (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
       Wed,              2025 04:21:40 -0700 (PDT)
Received-SPF: pass (google.com: domain of return@febrile-
cortex.practiceexam.com.taxpayering.nl designates 91.109.23.149 as permitted sender) client-
ip=91.109.23.149;
Authentication-Results: mx.google.com;
      dkim=permerror (no key for signature) header.i=@kfsfg5.3l20v3.b6ghlu.us header.s=default
header.b=iy7iba4q;
      spf=pass (google.com: domain of return@febrile-cortex.practiceexam.com.taxpayering.nl
designates 91.109.23.149 as permitted sender) smtp.mailfrom=Return@febrile-
cortex.practiceexam.com.taxpayering.nl
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=kfsfg5.3l20v3.b6ghlu.us;
```

Figure 2- Email header

Further DNS lookups returned no DKIM or DMARC records, confirming that DKIM signatures cannot be validated and that no DMARC policy is published to instruct receivers as shown in Figure 3.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig +short TXT default._domainkey.kfsfg5.3l20v3.b6ghlu.us

┌──(kali㉿kali)-[~/Desktop]
└─$ dig +short TXT _dmarc.kfsfg5.3l20v3.b6ghlu.us
```

Figure 3- dig output

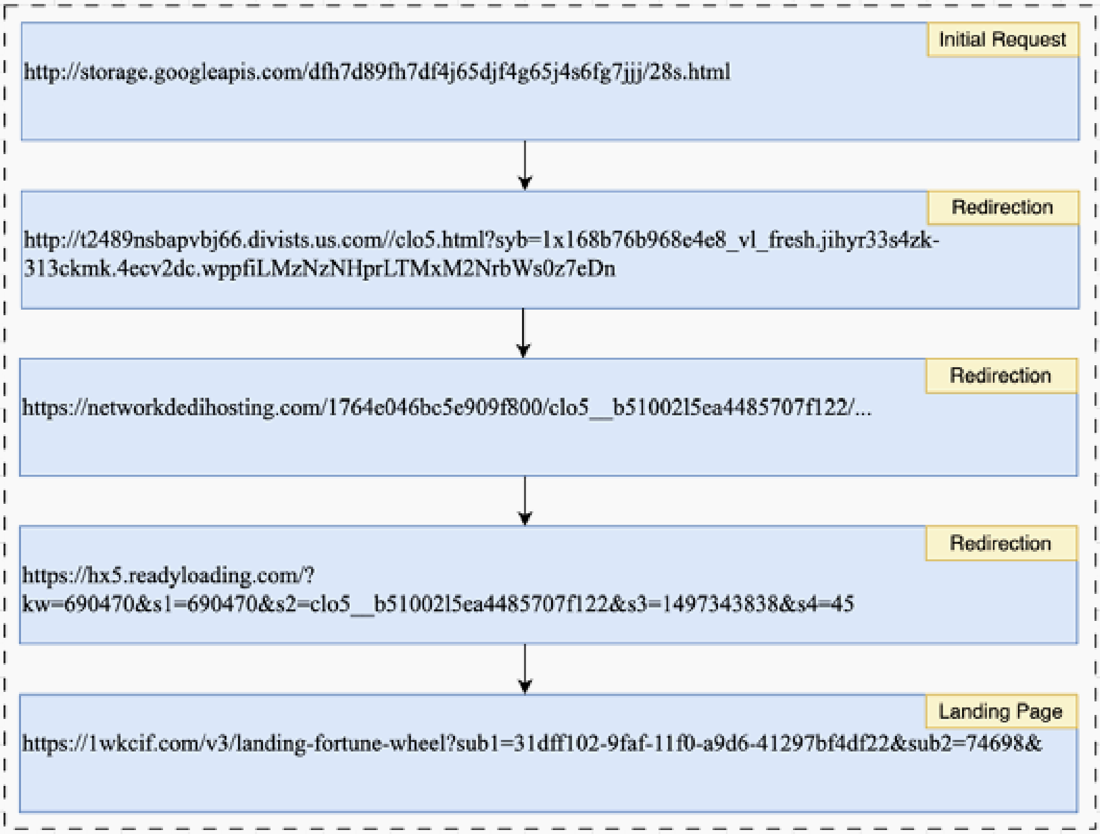
The Redirection Chain: From Cloud Storage to Scam

Once the user clicks the link, the deception sequence begins. The GCS-hosted page is usually a tiny HTML file with a short JavaScript snippet that reads encoded data from the URL fragment (after the #) and performs a client-side redirect. Because the redirect executes in the browser, static URL scanners and tools that only follow server-side redirects often miss the next stage. This makes the initial GCS object an ideal, low-effort redirector: it leverages Google's domain reputation while hiding the destination inside encoded fragments and JavaScript logic.

One observed example:

hxxp://storage.googleapis.com/dfh7d89fh7df4j65djf4g65j4s6fg7jjj/28s.html#/clo5.html?syb=1x168b76b968e4e8_vl_fresh.jihyr33s4zk-313ckmk.4ecv2dc.wppfiLMzNzNHprLTMxM2NrbWs0z7eDn

The full redirect chain, captured in our traffic logs and shown in Figure 4, begins with the GCS URL, passes through several intermediary domains, and ultimately leads to the final landing page.



http://storage.googleapis.com/dfh7d89fh7df4j65djf4g65j4s6fg7jjj/28s.html

http://t2489nsbapvbj66.divists.us.com//clo5.html?syb=1x168b76b968e4e8_vl_fresh.jihyr33s4zk-313ckmk.4ecv2dc.wppfiLMzNzNHprLTMxM2NrbWs0z7eDn

https://networkdedihosting.com/1764e046bc5e909f800/clo5__b5100215ea4485707f122/...

https://hx5.readyloading.com/?kw=690470&s1=690470&s2=clo5__b5100215ea4485707f122&s3=1497343838&s4=45

https://1wkcif.com/v3/landing-fortune-wheel?sub1=31dff102-9faf-11f0-a9d6-41297bf4df22&sub2=74698&

Figure 4- Redirection Chain

This redirection sequence often includes Bot detection mechanisms such as hCaptcha. The presense of a CAPTCHA service helps filter out automated analysis tools while maintaining a sense of authenticity for human users. After the CAPTCHA, users ae redirected to the final landing page, hxxps://1wkcif.com/v3/landing-fortune-wheel?sub1=31dff102-9faf-11f0-a9d6-41297bf4df2&sub2=74698". The page content varies by campaign-fake gift cards, prize draws, or adult content as shown in Figure 5.

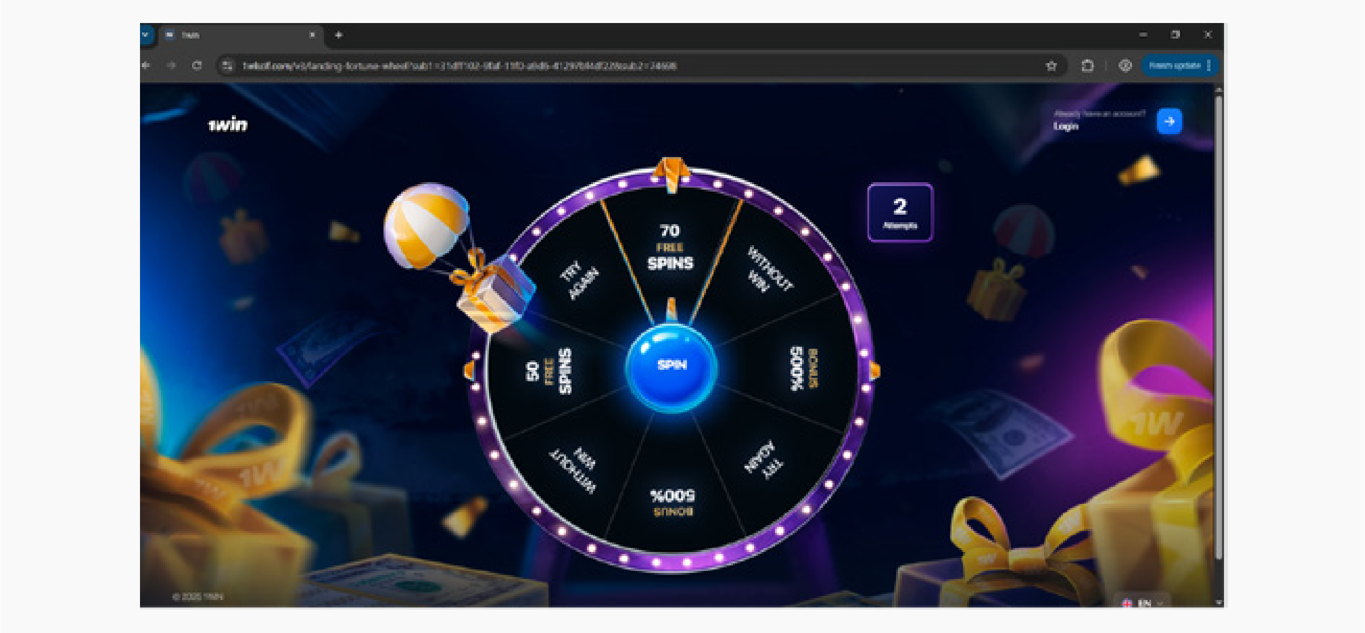
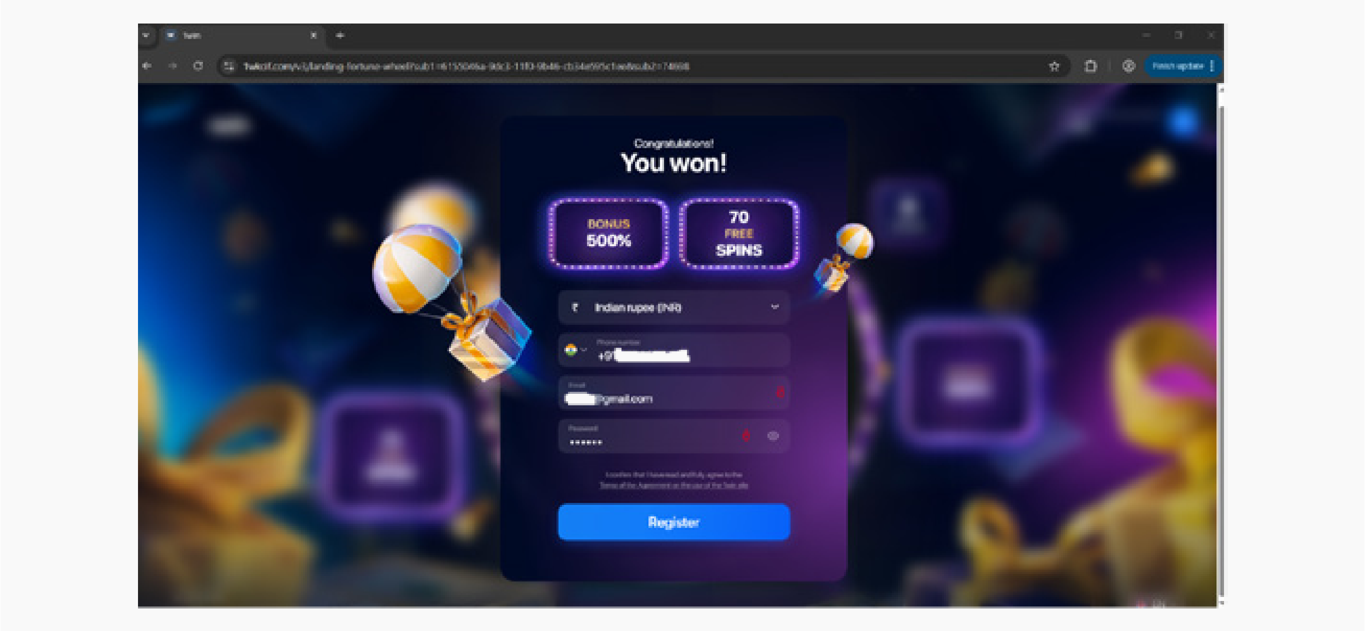


Figure 5- Landing Page - gambling/prize wheel

In one example, Users are redirected to a spin game, and after spinning, they are shown a message claiming they have won Bonus and are then sent to a registration page requesting their phone number, currency, email, and password to claim the prize as shown in Figure 6.



Indian rupee (INR)

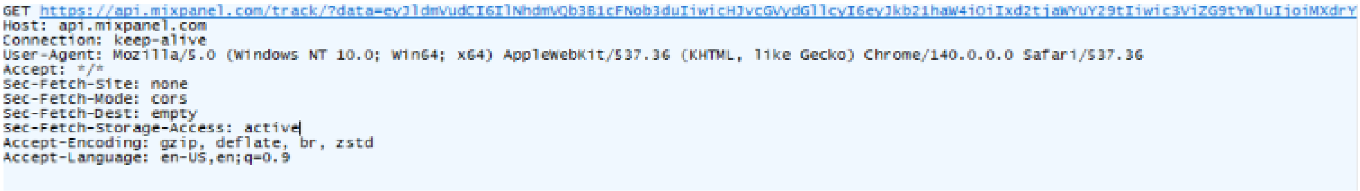
+9[redacted]

[redacted]@gmail.com

••••••

Figure 6- Registration Page

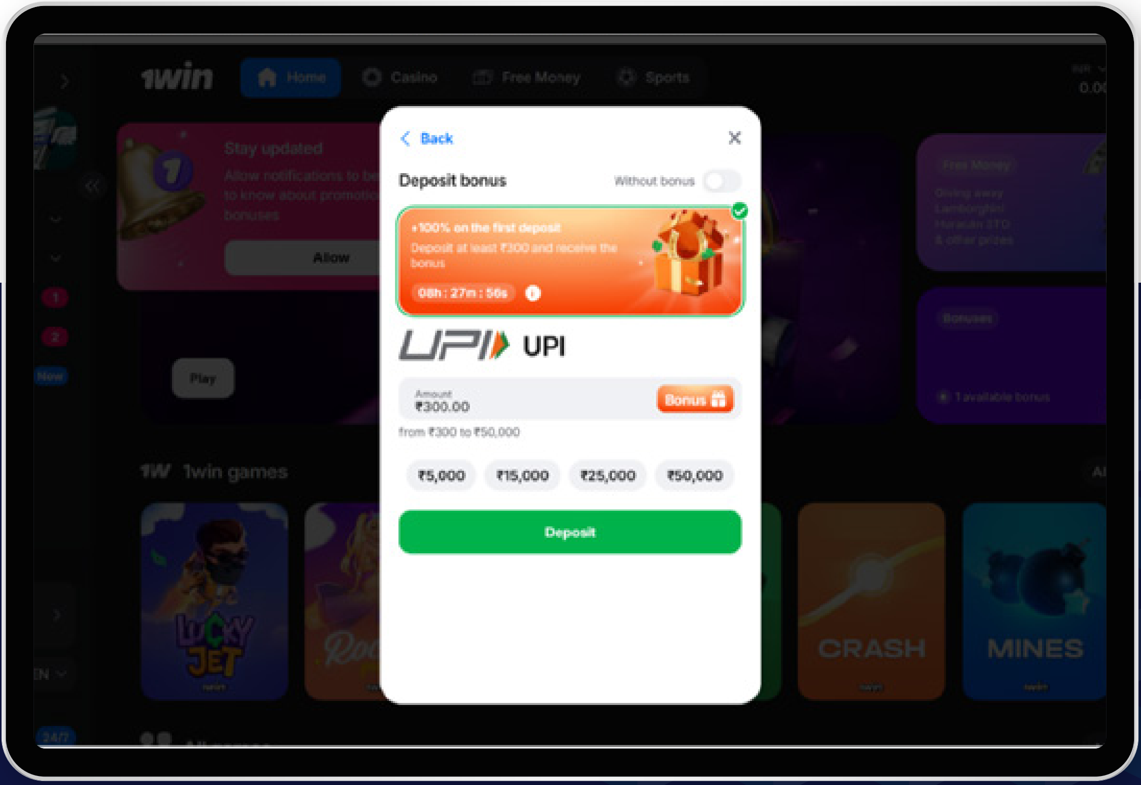
After users register on the landing page, detailed browser and platform information—including domain, subdomain, browser and OS details, extension/installation info, autofill settings, license type, and user registration status—is collected and sent from the user's side to Mixpanel, Google Analytics, and Amplitude—third-party analytics services that track user interactions and collect event data for analysis, as shown in Figure 7 .



```
GET https://api.mixpanel.com/track/?data=eyJldmVudCI6IlNhdmVQb3B1cFNob3duIiwicHJvcGVydGllcyI6eyJkb21haW4iOiIxd2tjaWYuY29tIiwic3ViZG9tYWluIjoiMXdrY
Host: api.mixpanel.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: */*
Sec-Fetch-Site: none
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Sec-Fetch-Storage-Access: active
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
```

Figure 7- Sending data to MixPanel

The user is now redirected to another page that prompts them to deposit money to claim the advertised bonus, as shown in the Figure 8. The flow from lure to spin game, registration, and deposit to claim a bonus is a classic scam designed to steal money and personal data. Requiring an upfront payment to claim a prize is a clear indicator of fraud. Users are pressured quickly from low-risk interaction to high-risk financial action.



Back

Deposit bonus

Without bonus

+100% on the first deposit

Deposit at least ₹300 and receive the bonus

08h : 27m : 56s

Amount
₹300.00

Bonus

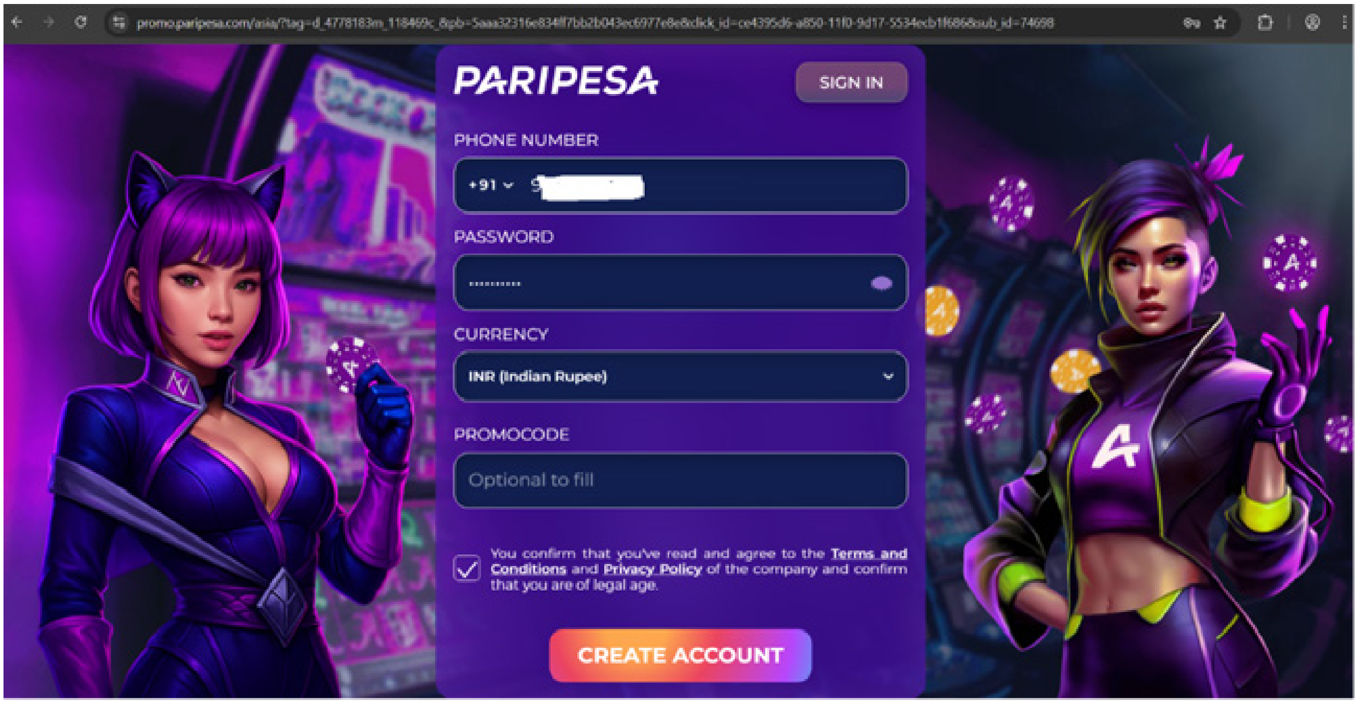
from ₹300 to ₹50,000

₹5,000 ₹15,000 ₹25,000 ₹50,000

Deposit

Figure 8- Money Deposit Option

Final landing URLs rotate frequently — the same GCS redirect can produce different pages as shown in Figure 9. Each variant ultimately funnels users into payment collection, profiling, and persistent logging to analytics endpoints.


promo.paripesa.com/asia/?tag=d_4778183m_118469c_&pb=5aaa32316e834ff7bb2b043ec6977e8e&click_id=ce4395d6-a850-11f0-9d17-5534ecb1f6868sub_id=74698

PARIPESA

PHONE NUMBER: +91 9[redacted]

PASSWORD: ••••••••••

CURRENCY: INR (Indian Rupee)

PROMOCODE: Optional to fill

☑ You confirm that you've read and agree to the **Terms and Conditions** and **Privacy Policy** of the company and confirm that you are of legal age.

Figure 9- Landing page

The Broader Implications

This type of scam goes beyond immediate financial loss. Users who engage with these pages risk providing personal information, such as credentials, phone numbers, and financial details, which can be misused or sold. The multi-stage flow, including redirected pages and repeated requests for deposits, makes it difficult for users to recognize the fraud until they have already lost money.

Repeated exposure to such scams can erode trust in legitimate promotions, online games, and cloud-hosted services. The collection of personal and financial information can also be used to target users with future scams. Overall, these scams exploit psychological pressure and misleading incentives, creating significant risk for individuals and highlighting the importance of vigilance and verification before providing sensitive information or sending money.

Conclusion

This scam illustrates how legitimate cloud services and analytics platforms can be manipulated to create convincing yet fraudulent user experiences. By chaining together trusted domains, CAPTCHA challenges, and polished interfaces, scammers effectively bypass both automated defenses and human skepticism. What begins as a harmless-looking email ends in the theft of personal and financial information — all under the guise of a reward or bonus.

To stay protected, users should remain cautious of any message that urges immediate action or requests payment to claim a prize. Organizations, on the other hand, must enforce strict DMARC policies, enhance link inspection mechanisms, and monitor for abuse of trusted platforms like Google Cloud Storage.

Ultimately, awareness and layered security remain the most effective defenses. Understanding how these scams exploit trust is the first step toward breaking their success cycle and preventing further victimization.

Unified SASE as a Shield Against Modern Web

Aryaka's Unified SASE framework neutralizes scams that exploit trusted cloud services and multi-stage redirection chains. DNS filtering blocks access to malicious redirection domains and fraudulent landing pages hosted on abused cloud infrastructure such as Google Cloud Storage (GCS). Secure Web Gateways inspect outbound HTTP and HTTPS traffic, preventing the submission of sensitive user data—including credentials and payment information—to unauthorized endpoints.

Next-generation firewalls enforce URL and application controls that stop browser-initiated redirects to suspicious gambling or payment sites. Integrated IDS/IPS engines detect anomalies such as rapid multi-domain redirects, analytics-based exfiltration, and scripted page instrumentation. Data Loss Prevention (DLP) policies further ensure that personal and financial information cannot leave the corporate environment through browser forms or HTTP POST requests.

Together, these layers of protection break the scam's sequence at multiple points—blocking malicious redirections, stopping data collection, and preventing fraudulent transactions before users are exposed. By continuously inspecting, correlating, and enforcing policy across every traffic flow, Aryaka's Unified SASE delivers proactive defense that safeguards users against evolving web-based scams and cloud abuse.

Appendices

Appendix A: Indicators of Compromise

IOC	Description
1wkcif.com	Scam landing page domain
154.197.121.1 91.109.23.149	Spam distribution IPs

Appendix B: Mapping MITRE ATT&CK® Matrix

Tactic	Technique	Technique Name
Initial Access	T1566.002	Phishing: Spearphishing Link
Initial Access	T1204.002	User Execution: Malicious Link
Collection	T1056	Input Capture: Web Portal Capture
Discovery	T1082	System Information Discovery
Exfiltration	T1567	Exfiltration Over Web Service

About Aryaka Networks

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit **www.aryaka.com**.

Experience Aryaka's Unified SASE as a Service

View Interactive Tour

aryaka

LEARN MORE | info@aryaka.com | +1.888.692.7925