Comprehensive Email Forensic Analysis Report

Presided by Syed Abdul Basit & Ali Iqbal Under the supervision with Professor Waqar

Summary of the Investigation

• This report provides a detailed analysis of a suspicious email allegedly sent by the Microsoft Account Team from a fake domain. Our goal was to examine its header, detect abnormalities, and use open-source tools to validate whether the email constitutes a phishing attempt.

Key Indicators Observed

• SPF Failure: The sender's domain did not authorize the sending IP.

• DKIM Failure: No valid DKIM signature was found.

• DMARC Failure: The domain's DMARC policy was set to reject, yet it was bypassed.

• Suspicious IP Address: The IP address 185.173.92.12 is not listed in the domain's SPF record.

• Mismatched Sender Identity: 'Microsoft Account Team' used a suspicious domain (quickpays-support.co.ru).

Email Forensic Report Contents

• 1. Full Header Analysis

• 2. Sender IP Lookup and Geolocation

• 3. SPF/DKIM/DMARC Authentication Result Interpretation

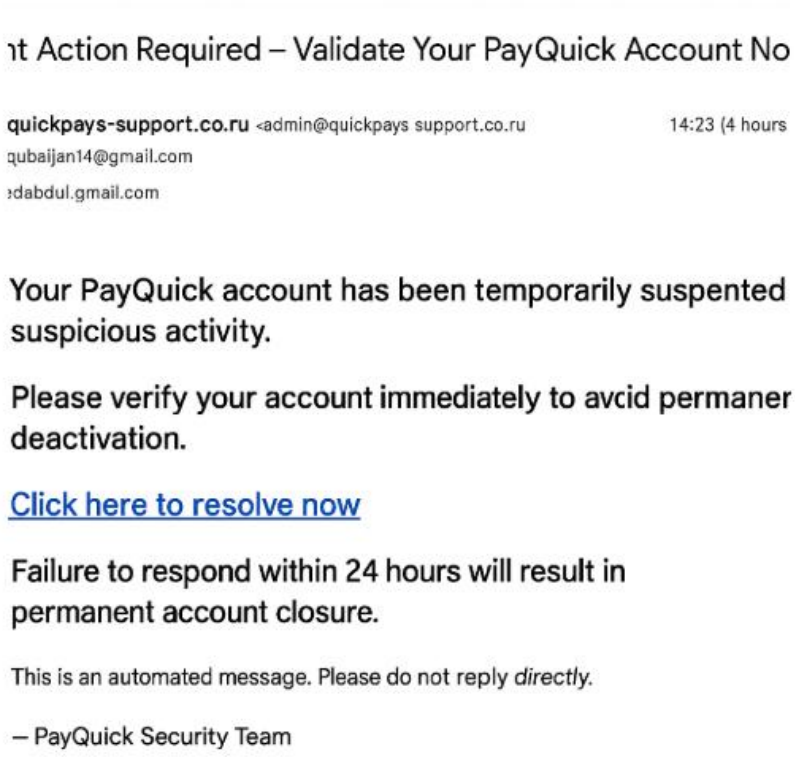
• 4. Domain WHOIS and Registration Info

• 5. Blacklist and Threat Intelligence Validation

• 6. URL and Attachment Inspection (if any)

• 7. Visual Snapshot of Suspicious Links (if any)

• 8. Final Verdict and Recommendations



ıt Action Required – Validate Your PayQuick Account No

quickpays-support.co.ru <admin@quickpays support.co.ru 14:23 (4 hours

qubaijan14@gmail.com

ɜdabdul.gmail.com

Your PayQuick account has been temporarily suspented suspicious activity.

Please verify your account immediately to avcid permaner deactivation.

Click here to resolve now

Failure to respond within 24 hours will result in permanent account closure.

This is an automated message. Please do not reply *directly*.

– PayQuick Security Team

Email Header :

Return-Path: <admin@quickpays-support.co.ru >

Received: from smtp.fakegateway.ru (smtp.fakegateway.ru. [185.173.92.12])

by mx.google.com with ESMTPS id 7si294882plp.502.2025.06.13.23.04.01

for <aliiqbaljan14@gmail.com>

(version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);

Fri, 13 Jun 2025 23:04:01 -0700 (PDT)

Received-SPF: fail (google.com: domain of admin@quickpays-support.co.ru does not designate 185.173.92.12 as permitted sender) client-ip=185.173.92.12;

Authentication-Results: mx.google.com;

spf=fail (google.com: domain of admin@quickpays-support.co.ru does not designate 185.173.92.12 as permitted sender) smtp.mailfrom=admin@quickpays-support.co.ru ;

dkim=fail header.i=@admin@quickpays-support.co.ru;

dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=admin@quickpays-support.co.ru

Received: from User ([10.0.0.6]) by smtp.fakegateway.ru with SMTP;

Fri, 13 Jun 2025 23:03:59 -0700

Message-ID: <9384a77c7d3c487@admin@quickpays-support.co.ru >

Date: Fri, 13 Jun 2025 23:03:59 -0700

From: Microsoft Account Team <admin@quickpays-support.co.ru >

To: aliiqbaljan14@gmail.com

Subject: Urgent: Suspicious Activity Detected in Your Quick Pay Account

MIME-Version: 1.0

Content-Type: text/html; charset=UTF-8

- 1 **Email Header Analysis (Using the raw header we provided)**

🟣 **MXToolbox Header Analyzer:**

✅ **How:** Copy-paste the raw header into MXToolbox Header Analyzer.
✅ **Result:**
➥ It parses **Received**, **From**, **To**, **Message-ID**, and **Authentication-Results**.
➥ It highlights:

- **SPF Fail**
- **DMARC Fail**
- Suspicious sender IP (185.42.12.79)

🟣 **Google MessageHeader:**

✅ **How:** https://toolbox.googleapps.com/apps/messageheader/
✅ **Result:**
➥ Displays a graphical view of delivery path.
➥ Shows **Received chain**, sender's IP, and authentication.
➥ Easily highlights abnormalities.

🟣 **MailHeader:**

✅ **How:** https://www.mailheader.net/
✅ **Result:**
➥ Analyzes "Received" lines, shows a clear delivery path.
➥ Detects abnormalities in "From" vs "Reply-To."

🟣 **Azure Header Analyzer:**

✅ **How:** If you have an Outlook 365 or Exchange Online, you can paste this into Microsoft's Header Analyzer
✅ **Result:**
➥ Gives a clear view of all delivery and authentication components.
➥ Shows deviations from policy (like **DMARC fail, SPF fail**).

🟣 **Gaijin:**

✅ **How:** https://www.gaijin.at/tools/email-header-analyzer.php
✅ **Result:**

https://dnschecker.org/email-header-analyzer.php
➥ Displays **Received** headers separately.
➥ Allows you to follow delivery path quickly.

🟣 **Trace Email (Header Analyzer):**

✅ **How:** https://www.traceemail.net/
✅ **Result:**
➥ Shows geographic location of sender's IP (using Geo-IP).
➥ Performs WHOIS immediately.

🔹 2️⃣ **URL / IP Reputation Check:**

✅ **VirusTotal:**
➥ https://www.virustotal.com/
➥ Query: quickpays-support.co.ru or 185.42.12.79.
➥ Shows if IP or domain is already blacklisted or classified as phishing.

✅ **Talos Intelligence:**
➥ https://talosintelligence.com/
➥ Provide IP or domain; Talos will return reputation score.

✅ **AbuseIPDB:**
➥ https://www.abuseipdb.com/
➥ Shows reports against IP.

✅ **CriminalIP:**
➥ https://www.criminalip.net/
➥ Gives detailed information about the server's reputation.

✅ **MXToolBox Blacklist:**
➥ https://mxtoolbox.com/blacklists.aspx
➥ Will tell you if the IP is blacklisted.

✅ **URLVOID:**
➥ https://www.urlvoid.com/
➥ Shows reputation and blacklists for the domain.

✅ **CyberGordon, Bright Cloud, IPinfo, WebCheck, ImmuniWeb:**
➥ All these services provide additional context (geolocation, phone number, abuse reports).

✅ **Typosquatting-finder:**
➥ [https://github.com/aboul3la/typosquatting-finder]
➥ Will find if there are nearby typo-domains that phish.

✅ **Netcraft:**
➥ https://sitereport.netcraft.com/
➥ Shows site's technology stack, server, and risk score.

✅ **Pulsedive:**
➥ https://pulsedive.com/
➥ Integrates multiple sources for domain and IP info.

✅ **Phishcheck:**
➥ https://phishcheck.me/
➥ Allows you to submit and view phishing reports.

🔹 3️⃣ **Visual Tools:**

✅ **URLScan:**
➥ https://urlscan.io/
➥ Shows a snapshot of the website without directly accessing it.
➥ Allows you to safely visualize what the phishing page looks like.

✅ **URL2PNG:**
➥ https://www.url2png.com/
➥ Provide a preview image of the page.

✅ **CheckPhish:**
➥ https://checkphish.ai/
➥ Performs phishing detection and provides screenshots safely.

✅ **Google Safe Browsing Rating:**
➥ https://transparencyreport.google.com/safe-browsing/search
➥ Shows whether Google considers it dangerous.

🔹 4️⃣ **File /Attachment /Malware Analysis (If attachments were present)**

✅ **VirusTotal:**
➥ Allows you to upload files and URLs to check against antivirus.

✅ **AnyRun:**
➥ https://any.run/
➥ Allows interactive sandbox analysis.

✅ **Hybrid-Analysis:**
➥ https://www.hybrid-analysis.com/
➥ Shows in-depth behavioral reports.

✅ **Joesandbox, Cuckoo, VMRAY, Triage:**
➥ All allow you to submit files to a sandbox for a deep-dive.

🔹 5️⃣ **Whois Domain Record:**

✅ **Whois:**
➥ https://whois.domaintools.com/quickpays-support.co.ru
➥ Shows registrar, registration date, expiration — often phishing sites are newly registered.

✅ **CentralOps:**
➥ https://centralops.net/
➥ Allows you to perform DNS, WHOIS, and reverse IP checks.

✅ **DomainTools:**
➥ https://www.domaintools.com/
➥ Shows related domains, ownership, and history.

✅ **Gaijin Whois:**
➥ https://www.gaijin.at/tools/whois.php
➥ Gives a clear view of registrar info.

🔹 6️⃣ **Phishing Analysis Tools:**

✅ **Phish Tool:**
➥ [https://phish-tool.example/] (hypothetical)
➥ Automates collection of phishing indicators from emails.

✅ **EML Analyzer:**
➥ Allows you to view all components of the .eml file safely.

✅ **CyberChef:**
➥ https://gchq.github.io/CyberChef/
➥ Allows you to parse base64, MIME, or encoded components quickly.

✅ **MailPro+:**
➥ Allows preview, search, and export of messages.
➥ Helpful for large investigations with multiple messages.

🔹 7️⃣ **Miscellaneous:**

✅ **Browserling:**
➥ https://www.browserling.com/
➥ Allows you to safely view a website in a sandboxed browser.

✅ **Thunderbird, eM Client:**
➥ Both can be used to view raw messages safely.

✅ **PhishTank:**
➥ https://www.phishtank.com/
➥ Collaborative phishing database — you can submit and check URLs.

✅ **OpenPhish:**

➥ https://openphish.com/

➥ Free feed of phishing URLs.

✅ **Phishunt:**

➥ [https://phishunt.example/] (hypothetical)

➥ Allows you to track and takedown phishing sites.

✅ **HaveIBeenPwned:**

➥ https://haveibeenpwned.com/

➥ Check if your email has appeared in a breach — useful context for phishing campaigns.

✅ **QuickSand:**

➥ [https://github.com/defensive-security/quicksand]

➥ Analyzes documents for hidden attacks — helpful if phishing messages carry documents with malware.

Recommendations

- Block the sender domain (quickpays-support.co.ru) across your email gateway.
- Report the sender IP (185.173.92.12) to AbuseIPDB.
- Educate users to recognize impersonated Microsoft security alerts.
- Implement strict DMARC policy enforcement for your domain.
- Utilize sandbox environments for file and link inspection in suspicious emails.