Phishing Incident Analysis & Case Summary

Credential-Harvesting Attack Against OK Group Staff, Delivered Under an Abused HPE Email Identity

Report ID:	IR-2026-0827-PHISH-OKG
Incident type:	Phishing / Credential harvesting / Email-identity abuse
Severity:	**High (email passed DMARC authentication)**
Target:	OK Group / OKX staff (recipient's personal mailbox)
Report date:	2026-08-27
Status:	Initial open-source (OSINT) analysis complete

This report is based on analysis of the raw headers of the email received by the victim, plus passive reconnaissance (OSINT) of the associated domains, IPs, certificates and public services. All findings were obtained WITHOUT any intrusion, scanning or unauthorized access to attacker-controlled systems.

Intended uses: internal notification, filing a police report, notifying the OK Group security team, and submitting abuse reports to AWS / registrar / host.

Contents

1 Executive Summary

On 26 August 2026 (UTC), the victim's personal Gmail mailbox received a Chinese-language phishing email impersonating the HPE (Hewlett Packard Enterprise) IT security team, with the subject **"Security Notice: Employee Account Re-registration Reminder."** Using the pretext of an "internal security system upgrade requiring all staff to re-register within 24 hours," it lured the recipient to click a link.

Three unusual characteristics make this incident far more dangerous than typical phishing:

1. **The email is cryptographically "genuine."** It was sent through Amazon SES carrying a valid signature from a DKIM key **that was actually published in `hpe.com`'s DNS at the time**. As a result SPF, DKIM and DMARC **all passed** — even though `hpe.com` enforces the strictest `p=reject` policy. Gmail therefore delivered it normally with no warning. This is not "sender spoofing"; the attacker **obtained the ability to sign mail as HPE**.
2. **A subdomain sleight-of-hand hides the real target: OK Group.** The email body displays the link as `engine.okg.com` (appearing to be a legitimate OK Group domain), but it actually points to the attacker-controlled `okg.enginelark.com`. The email hot-links OKX's genuine brand logo from OKX's real CDN, leaving no visual tell.
3. **The attack shows targeted reconnaissance.** The look-alike domain `enginelark.com` maps precisely to OK Group's real internal system codename ("Engine" office portal + "Lark"/Feishu), and the phishing page hard-codes OK Group's genuine internal domain `enginelark.okg.com` as a fallback redirect. This indicates deep knowledge of the target's internal naming — not indiscriminate mass mailing.

The phishing page requests the victim's **corporate email and a verification code** (not a password), consistent with session hijacking or OTP relay, which can bypass some two-factor authentication (2FA). During analysis, at least **two look-alike domains registered in the same batch** were found, both hosted on the same Netherlands VPS.

> **Bottom line:** This is not a "spoofed" email — it is a genuine, targeted phishing message sent through a legitimate authentication channel and vouched for by an **abused HPE mail-signing identity**. The receiving side (Gmail) had no way to block it. The true point of compromise lies in HPE's mail-sending credentials / DNS configuration and in the attacker's rented Netherlands server.

2 Key Evidence Screenshots

This section preserves the original screenshots of the phishing email in the victim's mailbox as first-hand evidence. The content is consistent with the technical analysis in §5 and the raw headers in Appendix A.

Figure 1 — Apparent sender. Expanding the sender in the mail client shows `security@hpe.com`. Note this is **not ordinary display-name spoofing**: as explained in §5.1, the email actually carried a valid `hpe.com` DKIM signature and passed DMARC, so the client rendered it as a legitimate HPE sender.

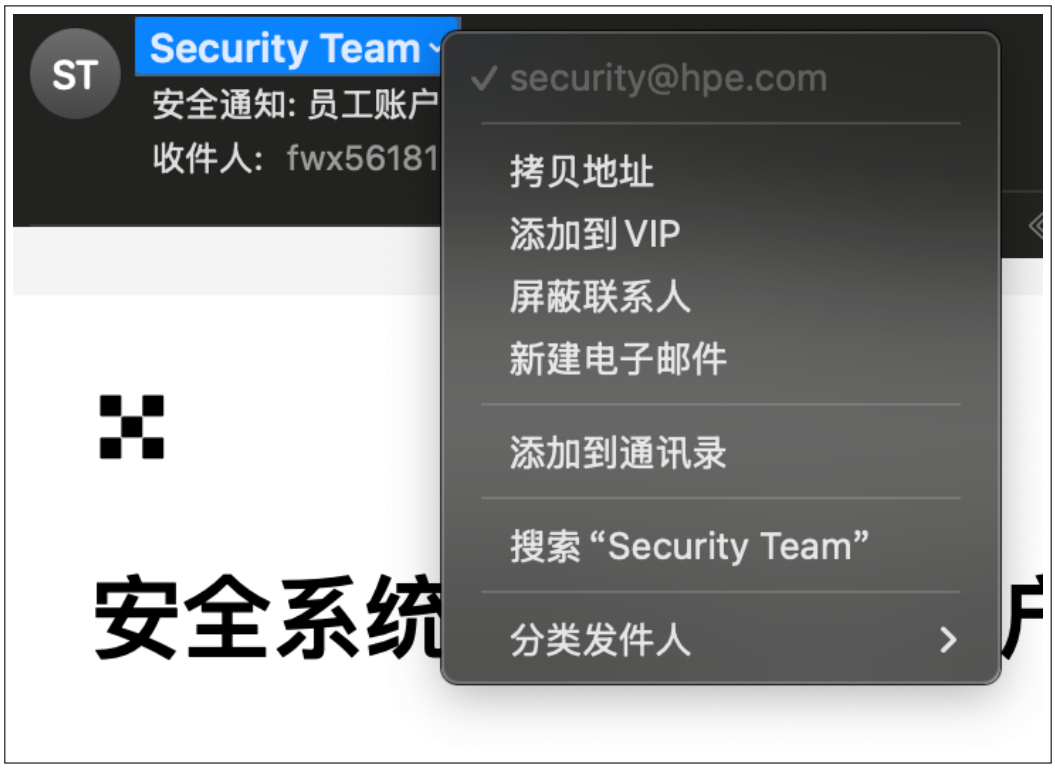

Figure 1: Expanded sender in the mail client; apparent sender is security@hpe.com.

Figure 2 — Email body and disguised link. The subject is ``Security Notice: Employee Account Re-registration Reminder,'' the recipient is the victim's Gmail (fwx5618177@gmail.com), and the client shows a send time of 09:22. The body, in the voice of the HPE IT security team, demands "re-registration within 24 hours or access will be restricted." **The link displayed in the body is `https://engine.okg.com/...` (disguised text), while the actual href points to the attacker domain `okg.enginelark.com`** (see §5.2).

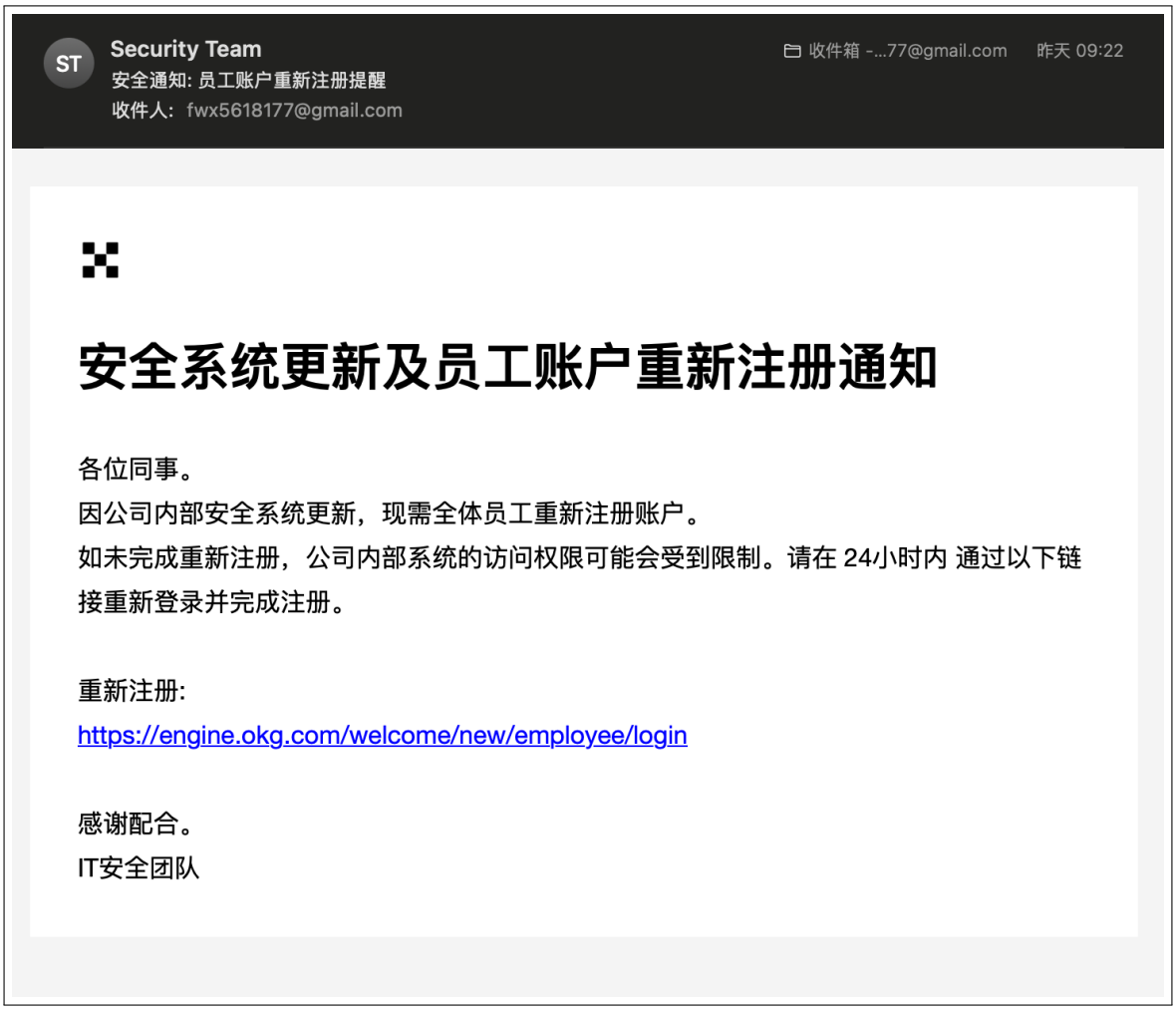

Figure 2: Full phishing email; the displayed link reads engine.okg.com but resolves to okg.enginelark.com.

3 Case Metadata

Field	Value
Victim mailbox	`fwx5618177@gmail.com` (personal Gmail)
Apparent sender	`Security Team <security@hpe.com>`
Actual send path	Amazon SES (us-east-1), node `a8-53.smtp-out.amazonses.com`
Sending IP	`54.240.8.53` (Amazon Technologies Inc.)
Send time	2026-08-25 18:22:14 PDT = **2026-08-26 01:22:14 UTC**
Phishing landing page	`https://okg.enginelark.com/welcome/new/employee/login`
Attacker server	`195.20.204.18` (Netherlands, Snel.com B.V.)
Real target	OK Group / OKX employee account system
Impersonated brands	HPE (email identity); OKX / OK Group (landing page)
Analysis date	2026-08-27

4 Incident Timeline

The table reconstructs the full sequence from infrastructure preparation to execution. Times are normalized to UTC where possible.

Time (UTC)	Event
1995-03-24	`hpe.com` registered (MarkMonitor); legitimate HPE asset.
1998-09-22	`okg.com` registered (now Amazon Registrar); legitimate OK Group asset, mail via Larksuite / Feishu.
2018-06-28	`okpool.top` registered by OK Group (Alibaba Cloud HiChina); **legitimate own asset**, later used as an internal CNAME transit.
2026-08-05 09:03:22	Attacker registers **first look-alike `engine-okg.com`** (Namecheap, Iceland privacy proxy).
2026-08-05 13:15:05	Attacker registers **second look-alike `enginelark.com`** (Namecheap, same privacy proxy, 4h12m later).
From 2026-08-05	Attacker deploys the phishing kit on Netherlands VPS `195.20.204.18` (nginx/1.24.0, Ubuntu); obtains an SSL.com wildcard certificate `*.enginelark.com`.
By 2026-08-25	Attacker obtains the ability to send as `hpe.com` via Amazon SES (see §5.1).
2026-08-26 01:22:14	**Phishing email sent**, delivered to the victim's Gmail via SES (`54.240.8.53`); SPF/DKIM/DMARC all pass.
2026-08-26 (local)	Victim sees the email in the inbox (screenshot time 09:22).
2026-08-27	Analysis begins. Authoritative DNS confirms the relevant `hpe.com` DKIM selector now returns **NXDOMAIN (revoked)**, indicating HPE / AWS-side remediation is underway. The landing page is still live.

Timing inference: Both look-alike domains were registered on the same morning, roughly three weeks before the email was sent — the classic "build ahead, deploy on cue" cadence of a phishing operation. The DKIM record disappeared within two days of the send, indicating HPE-side response has already started.

5 Attack Chain

Step 1. **Delivery:** The email was sent via Amazon SES carrying a valid `d=hpe.com` DKIM signature, domain-aligned with `From: security@hpe.com`, so DMARC returned `pass`. Gmail delivered it to the inbox with no security warning.

Step 2. **Pretext:** The Chinese-language body impersonates the HPE IT security team, creating urgency ("re-register within 24 hours or access will be restricted"); the genuine OKX CDN logo boosts credibility.

Step 3. **Sleight-of-hand:** The anchor text shows `https://engine.okg.com/...`, while the actual `href` points to `https://okg.enginelark.com/welcome/new/employee/login`.

Step 4. **Harvest:** The landing page (an Ant Design-styled "Welcome to join OK Group" login) requests a **corporate email + verification code**, posting them to the attacker's server via same-origin endpoints `POST /welcome/new/employee/send-code` and `POST /welcome/new/employee/verif`

Step 5. **Escape:** When the backend returns "email already registered," the page shows a notice and, after 3 seconds, redirects the victim to the **real system** `https://enginelark.okg.com/engine/login`

so the victim assumes all is normal, does not become suspicious, and does not report — extending the attack's lifespan.

Uncertainty statement: The page asks the victim for a "verification code," meaning some system must send that code to the victim. The most plausible explanation is that the attacker's backend **makes a real-time request to OK Group's genuine system to trigger a legitimate code** (i.e. a one-time-password / OTP relay), enabling session hijacking and 2FA bypass. This report **did NOT verify** that behavior — verifying it would require submitting test data to the attacker's endpoint, an unauthorized interaction with a third-party system that was deliberately avoided. This step should be confirmed by the OK Group security team in a controlled environment.

6 Technical Analysis

6.1 How the Email Passed HPE Authentication (Key Finding)

The authentication results from the victim's raw headers (verbatim excerpt):

```
spf=pass    smtp.mailfrom=...@amazonses.com  (client-ip=54.240.8.53)
dkim=pass   header.i=@hpe.com  header.s=kgwu7d2xppvqvpl5d2eir2luwanbipyt
dkim=pass   header.i=@amazonses.com
dmarc=pass  (p=REJECT sp=REJECT dis=NONE)  header.from=hpe.com
```

This is not forgery. The DKIM signature is cryptographically valid: it verifies against the public key `hpe.com` published at the time, and the signing domain `d=hpe.com` is aligned with the header `From: hpe.com`, so DMARC passes even under `p=reject`. Forging DKIM requires the private key and is cryptographically infeasible; therefore the only possibility is that the attacker **legitimately obtained the ability to sign mail as `hpe.com`**.

Key forensics: The DKIM selector `kgwu7d2xppvqvpl5d2eir2luwanbipyt` is a 32-character lowercase random string — **precisely the Amazon SES "Easy DKIM" token format**. SES can only sign with it if the domain owner has published the corresponding CNAME in DNS. Querying that selector against multiple public resolvers (8.8.8.8 / 1.1.1.1 / 9.9.9.9) and against `hpe.com`'s authoritative server `ns1.hpe.com` **all returned NXDOMAIN with the authoritative (aa) flag**; a random-label test confirmed `hpe.com` has **no wildcard**. Conclusion: the record **did exist at send time (2026-08-25) and has since been deleted**.

Two possible paths (require AWS/HPE-side confirmation):

- **Path A (more likely) — SES credential compromise:** An AWS account belonging to HPE or one of its vendors had already completed SES domain verification for `hpe.com` (the DKIM CNAME was legitimately published). The attacker obtained that account's access keys (e.g. via a code-repo leak, CI logs, or a compromised vendor) and sent mail under the already-verified identity, so all checks passed. In this case **HPE's DNS was never tampered with**.
- **Path B (less likely) — DNS record injection:** The attacker, via compromised DNS-management privileges or an authorized third-party vendor, wrote their own SES account's DKIM CNAME into `hpe.com`.

Path A is favored because if the attacker truly controlled `hpe.com`'s DNS, its value (issuing TLS certificates, hijacking MX, taking over subdomains) would vastly exceed sending one phishing email; using it only to send mail fits "holding only an SES sending permission."

6.2 Link and Visual Disguise

The anchor in the email HTML (Base64-encoded body) is classic anchor-text deception:

```
<a href="https://okg.enginelark.com/welcome/new/employee/login">
   https://engine.okg.com/welcome/new/employee/login</a>
<img src="https://static.coinall.ltd/cdn/assets/imgs/254/48452487343D915E.pn
↪  g"
↪  alt="0KX">
```

The displayed text is the brand domain `engine.okg.com`, but the actual jump is to the attacker domain `okg.enginelark.com` — placing the brand word `okg` at the far left as a subdomain label, while the true registered domain is `enginelark.com` on the right. The logo hot-links OKX's genuine CDN `static.coinall.ltd`, leaving no visual tell.

6.3 Attacker Infrastructure

Item	Value
Look-alike domain 1	`enginelark.com` (primary); subdomain `okg.enginelark.com` is the phishing landing page
Look-alike domain 2	`engine-okg.com` (backup / earlier version; same IP, mismatched cert)
Registrar	Namecheap, Inc.
Registration date	Both 2026-08-05 (see timeline)
Registrant	Hidden (Withheld for Privacy ehf, Reykjavik, Iceland)
NS / MX	`*.registrar-servers.com` (Namecheap default DNS and mail forwarding)
Hosting IP	`195.20.204.18`
Reverse DNS	`s46983.hosted-by-snel.com`
Host	Snel.com B.V. / Ormilon B.V., AS62370
Geolocation	Lelystad, Netherlands (company registered in Rotterdam, Schuttevaerweg 101)
Abuse contacts	`report@abuse.bz` (Snel); `abuse@namecheap.com` (Namecheap)
Web service	nginx/1.24.0 (Ubuntu), HTTP/2
TLS certificate	Wildcard `*.enginelark.com`, issued by SSL.com TLS Issuing RSA CA R1, valid until 2027-02-19

Evidence the two domains share an operator: registered on the same day (2026-08-05), both via Namecheap, both using the same Iceland privacy proxy, both resolving to `195.20.204.18`, both serving the same phishing path `/welcome/new/employee/*`. `engine-okg.com`'s TLS cert is still `*.enginelark.com` (mismatched, browsers warn), suggesting a backup or earlier build, with `enginelark.com` chosen for production. Both domains' MX point to Namecheap mail forwarding, **meaning the attacker can receive mail at these domains**.

6.4 Excluded False Positives

- `okpool.top`, `enginelark.okg.com`, and `engine.okg.com` are **all legitimate OK Group assets**. `enginelark.okg.com` resolves via a CNAME chain `enginelarktransit.okpool.top`

to OK Group's own AWS ELB — a normal internal configuration. The phishing page references `enginelark.okg.com` only for the "failure redirect" (see §4 Step 5); this does NOT imply those assets are compromised. **Do not add them to any block or abuse list.**

7 Attribution: What Can and Cannot Be Determined

7.1 Determinable via Open Sources (OSINT)

- Attacker infrastructure: two look-alike domains, hosting IP, host, certificate, send channel (Amazon SES us-east-1), and the unique SES message identifiers.
- The targeted nature of the attack: precise knowledge of OK Group's internal system naming.
- The fact that HPE's mail-signing identity was abused, and the time window in which that DKIM record was revoked.

7.2 NOT Determinable Openly (Requires Institutional / Law-Enforcement Action)

- **Attacker's real identity:** domain registrant is masked by an Iceland privacy proxy; VPS lessee details are held only by Snel. Open channels end here.
- **The exact path of the HPE-identity abuse (A vs. B):** only AWS and HPE can distinguish this from internal logs.
- **The OTP-relay hypothesis:** must be verified in a controlled environment; the attacker's endpoint should not be probed.

7.3 The Most Valuable Attribution Lead: The Amazon SES Message Identifiers

The `Message-ID` and `Feedback-ID` in the headers let AWS trace back to the **sending AWS account ID, registration email, payment method, and creation/login source IPs**. This is the only data in the entire case that **could point to a real identity**. Note, however, that this AWS account may itself be **a hijacked legitimate account** (e.g. an HPE vendor's) or **newly registered with a stolen credit card and false identity**; even after a lawful disclosure request, source-IP correlation and payment tracing may be needed to reach a real person.

8 Indicators of Compromise (IOCs)

8.1 Indicators for Direct Blocking / Reporting

```
[Domains]
  okg.enginelark.com        (phishing landing page)
  enginelark.com            (attacker primary domain)
  engine-okg.com            (attacker backup / earlier version)
[IP]
  195.20.204.18             (AS62370 Snel.com B.V. / Lelystad, NL)
  54.240.8.53               (Amazon SES send node; do NOT block the whole
   ↪  range)
[URL paths]
  /welcome/new/employee/login
  /welcome/new/employee/send-code
  /welcome/new/employee/verify
```

```
[TLS certificate]
  CN=*.enginelark.com  (SSL.com TLS Issuing RSA CA R1, valid until
  ↪  2027-02-19)
[Web fingerprint]
  Server: nginx/1.24.0 (Ubuntu)
```

8.2 Email and Identity Identifiers (for AWS / HPE Disclosure)

```
SES Message-ID:
  010001a03ba91e87-f71f93ad-d4b6-4573-80e9-e8f961f4617b-000000
Feedback-ID:
  ::1.us-east-1.Mx7G8QgHyj7ECaoZ0+HgaLyxWu91cjlxcyOX7zhFyIw=:AmazonSES
X-SES-Outgoing:
  2026.08.26-54.240.8.53
Abused HPE DKIM selector (present at send time, now NXDOMAIN):
  kgwu7d2xppvqvpl5d2eir2luwanbipyt._domainkey.hpe.com
Apparent From:  Security Team <security@hpe.com>
Envelope From:  ...@amazonses.com (Return-Path)
```

8.3 Exclusions (Legitimate Assets — Do Not Report)

```
okpool.top / enginelark.okg.com / engine.okg.com   -- OK Group's own assets
static.coinall.ltd                                 -- OKX's real CDN (logo
↪  hot-linked)
```

9 Impact Assessment and Immediate Response

9.1 Impact

- **Individual victim:** if email and verification code were entered on the landing page, the account should be treated as potentially compromised.
- **OK Group:** highly targeted; other victims in the same batch are likely. If the OTP-relay hypothesis holds, the attack can bypass 2FA and directly threaten staff accounts and internal systems.
- **HPE:** its mail-signing identity was abused by a third party to send phishing — a security incident implying credential leakage or DNS-record injection.

9.2 Victim Immediate Actions (if information was submitted)

1. Immediately change the password on the **real system** `engine.okg.com`.
2. Revoke all active sessions; reset 2FA bindings.
3. Review login history for logins from the Netherlands / unusual IPs.
4. Click “Report phishing” on the email in Gmail.

9.3 Organizational and Reporting Actions (by priority)

1. **Notify the OK Group security team (highest priority):** this is a targeted attack on the company; issue a company-wide alert, review `enginelark.okg.com` for anomalous logins, and confirm the OTP-relay hypothesis.
2. **Report to AWS:** `abuse@amazonaws.com` / AWS Trust & Safety, attaching the SES identifiers in §7.2, requesting suspension of the sending account and preservation of records.
3. **Report to HPE security:** `security-alert@hpe.com`, reporting abuse of `hpe.com` DKIM signing (include the selector).
4. **Report to SSL.com:** request revocation of the `*.enginelark.com` certificate; after revocation, browsers will block outright.
5. **Report to registrar / host for takedown:** Namecheap `abuse@namecheap.com`; Snel `report@abuse.bz`.
6. **Report to anti-phishing bodies:** Google Safe Browsing; APWG (`reportphishing@apwg.org`).

10 Law-Enforcement and Accountability Path

Core principle: the ceiling of individual and technical measures is "takedown and suspension"; reaching a real identity and pursuing accountability **must go through institutional legal process**. Ordered by feasibility and effectiveness:

1. **File a police report (the critical step).** Only after a case is opened can law enforcement issue disclosure orders (subpoenas / mutual legal assistance requests) to **AWS, Namecheap, Snel** to obtain the real registrant, payment details and source IPs masked by "privacy proxy" and "anonymous registration." All IOCs in this report are the evidence package prepared for this step.
2. **Have OK Group drive cross-border legal assistance.** As the targeted company, OK Group has both the motive and resources to file and pursue cross-border assistance. The hosting server is in the **Netherlands (EU)**, where MLAT / EU channels are mature. Snel and Namecheap must provide customer data upon receipt of lawful disclosure orders.
3. **Trace the sending account via AWS.** Using the SES identifiers, law enforcement can compel AWS to disclose the sending AWS account's registration, payment details and source IPs. Note this account may be hijacked or anonymously registered and may require further tracing.
4. **Evidence preservation and time-sensitivity.** Immediately timestamp-preserve the phishing page, certificate, DNS records and raw email headers (hash + trusted timestamp recommended), since the attacker may dismantle the infrastructure at any time, and some DNS records (e.g. the HPE DKIM) have already disappeared.

Explicit statement on "hacking back" the attacker's server: This analysis did NOT, and should NOT, perform any port scanning, vulnerability probing, admin-panel brute forcing, or unauthorized access against the attacker's server. Reasons: (1) unauthorized access to third-party systems is **itself illegal** in most jurisdictions — the target being a criminal is no exemption — and it would taint the chain of evidence; (2) the VPS may be an **innocent third party's** machine compromised by the attacker, or a **honeypot**, so active interaction would tip off the adversary and invite retaliation; (3) the server is **disposable infrastructure** containing no real-identity information about the attacker — identity leads sit in the host's and AWS's back-ends and can only be obtained through legal process. Accountability must proceed **entirely through law enforcement and professional DFIR / CERT channels**.

Appendix A: Key Raw-Header Fields (Verbatim Excerpt)

```
Return-Path: <010001a03ba91e87-f71f93ad-d4b6-4573-80e9-e8f961f4617b-000000
             @amazonses.com>
Received: from a8-53.smtp-out.amazonses.com (54.240.8.53)
          by mx.google.com ... Tue, 25 Aug 2026 18:22:14 -0700 (PDT)
Authentication-Results: mx.google.com;
  dkim=pass header.i=@hpe.com header.s=kgwu7d2xppvqvpl5d2eir2luwanbipyt;
  dkim=pass header.i=@amazonses.com;
  spf=pass smtp.mailfrom=...@amazonses.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=hpe.com
DKIM-Signature: v=1; a=rsa-sha256; d=hpe.com;
  s=kgwu7d2xppvqvpl5d2eir2luwanbipyt; ...
From: Security Team <security@hpe.com>
Subject: [Security Notice: Employee Account Re-registration Reminder]
Date: Wed, 26 Aug 2026 01:22:14 +0000
X-SES-Outgoing: 2026.08.26-54.240.8.53
```

End of report — This is a defensive security analysis intended solely for lawful incident response, reporting and abuse notification. No unauthorized access to any system was performed during the analysis.