STRATEGIC CRYPTO RESERVE · PHISHING & SCAM TAKEDOWN SERVICE

Takedown Case Report

Case SCR-TD-2026-1031-01 · Opened 31 Oct 2026, 13:25 PT · Reports sent 13:31 PT

CONFIRMED INVOICE FRAUD

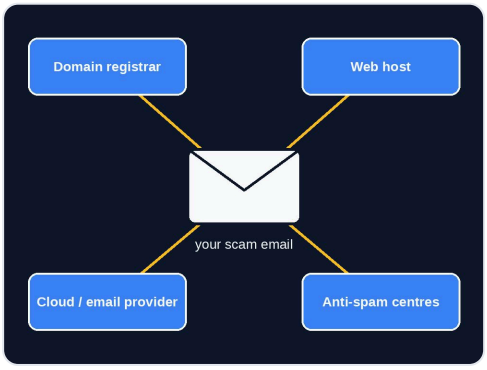
Sample report. This is a real case handled on 31 October 2026, published as a demo of what a client receives after buying a takedown. The client's identity and mailbox, the police file references and the names of the innocent third parties whose systems were abused have been redacted. Strategic Crypto Reserve is not affiliated with Intuit or QuickBooks.

$11,125.99*	6 min	9	3
amount the scammer asked the client to pay	from case opened to reports delivered	organisations notified (abuse desks, brand, regulators)	linked fraud emails from the same sender kit found

* The invoice shows "$11,125.99" with no currency; the e-Transfer request implies Canadian dollars.

1. Verdict in plain language

Do not pay this invoice. The email pretends to be a QuickBooks invoice from a real Toronto process-serving firm. That firm did not send it. A criminal sent it from a hijacked mail server, forged the firm's name, and set things up so that replies and payments go to the criminal instead.



Red flags we found

- The sender's own domain publishes a strict anti-spoofing record (SPF `-all`), and this message **fails** it. The firm's real mail goes through Microsoft 365. This one came from a rented cloud server.
- The **Reply-To** is a mailbox at an unrelated Malaysian company, not the firm.
- The "Preview" button opens `titan-invoice.surge.sh`, a free static-site host. Real QuickBooks invoices open on intuit.com.
- It was sent by a PHP script (`X-Mailer: PHP/8.3`), not by Intuit's mail system. It copies real Intuit logos and tracking links so it looks genuine.
- It is addressed to "Account Payables" with no name, invoice lines or matter number: a typical **fake-invoice / business-email-compromise** lure.

2. How the email reached the client

Attacker	Stolen login	Abused relay	Client inbox

PHP mail kit
`62.60.134.68`
HELO `[62.60.130.6]`
	Authenticated (ESMTPSA) submission to a third-party Postfix server	`mail.t••••••g.org`
		`206.189.181.33`
		DigitalOcean
			[redacted]
			31 Oct 2026
			13:19:29 PT

Header / evidence	Value	What it means
From (display)	`"[IMPERSONATED FIRM] LTD." <noreply@[firm-domain].ca>`	Forged. SPF fails.

Reply-To	`finance@o••••••••.asia`	Drop mailbox for victims' replies
Payment instruction	Interac e-Transfer to an address shown as the firm's	Funds diversion
Landing page	`https://titan-invoice.surge.sh`	Fake invoice "preview"
Relay queue ID	`DCF9C1146678`	Lets the server owner find the stolen account
Message-ID	`<c2d4e89b-…-0765897d836f@206.189.181.33>`	Generated by the kit, not by Intuit

3. History check: is this a one-off?

Before we write a single letter we search our archive of over two years of reported spam, plus our mail-gateway logs, by sender, domain, relay, IP range, reply-to, subject, template text and links. Here the attacker's fingerprint (HELO `[62.60.130.6]` + `X-Mailer: PHP/8.3`) matched **two earlier fraud emails**:

Date	Lure	Attacker IP	Hijacked relay
20 Oct 2026	"[Important] Liberian Gold Partnership" (advance-fee fraud, forged government sender)	`62.60.130.63`	Mail server in the US
24 Oct 2026	"Re: This is my last email" (extortion-style lure)	`62.60.134.82`	Web server in Australia
31 Oct 2026	Fake QuickBooks invoice, $11,125.99 (this case)	`62.60.134.68`	Cloud server (DigitalOcean)

Pattern: **one operator, a new stolen mail account each time.** That is why we report the attacker's network as well as each relay. We also found a June 2026 fake-invoice campaign on the same free host (surge.sh). It matches only by template, and we say so in our letters rather than overstate the link.

4. Takedown reports sent

Each organisation received a tailored letter written *on behalf of our client*, with the evidence above and the full original message attached in a forensic format (`message/rfc822`, headers intact).

Recipient	Request	Status
DigitalOcean Abuse	Customer's server relayed phishing through a compromised login. Reset it, review the login logs, stop the relay.	**Delivered**
Abused server's postmaster + abuse	Find the stolen account from queue ID DCF9C1146678, reset the password, purge the queue.	**Delivered**
Attacker's network (RIPE abuse contact for 62.60.130.0/24 and 62.60.134.0/24)	Terminate the customer running the kit; preserve the logs. All 3 samples attached.	**Delivered**
surge.sh Abuse	Take down `titan-invoice.surge.sh`; keep deployment logs.	**Delivered**
Intuit security (phishing desk)	Brand abuse of QuickBooks invoice template, logos and tracking links.	**Delivered**

The impersonated firm	Courtesy warning: your name is being forged; check the e-Transfer address and warn your clients.	Delivered
Reply-To company (postmaster, abuse)	Your finance mailbox is a scam drop; secure it.	Rejected (550)
APWG (Anti-Phishing Working Group)	Phishing intelligence feed used by browsers and security vendors.	Delivered
Canadian Spam Reporting Centre (CRTC/CASL)	Regulatory complaint under Canada's Anti-Spam Legislation.	Delivered
SpamCop	Full raw message for automated blocklisting of the sending IP.	Accepted

"Delivered" means the recipient's mail server accepted the report (SMTP 250), confirmed in our gateway log. The Reply-To company's server refuses its own postmaster@ and abuse@ addresses. We record that and do not write to the drop mailbox itself, so the criminal is not alerted.

5. Block list for your mail filter

Every client gets a ready-made block list for Gmail, Outlook or their IT provider. In this case the email reached our own mail gateway, so we also applied and tested these blocks ourselves:

Layer	What we blocked
Sender filter	Forged sender address, the Reply-To drop mailbox, and the whole abused relay domain (including subdomains)
Connection filter + firewall	Relay `206.189.181.33` and attacker IPs `62.60.130.6`, `62.60.130.63`, `62.60.134.68`, `62.60.134.82`
Content rules	A fingerprint rule on the kit's fixed HELO, so its next email is caught **even through a new hijacked server**, and a rule on the landing URL. Re-test score: 30.1 against a reject threshold of 10. The October 20 message is also caught.

Every block was tested with a simulated mail session before going live, and a legitimate address at the impersonated firm was checked to make sure it still gets through.

6. Excerpt from a report we sent

Hello DigitalOcean Abuse team,

Your droplet 206.189.181.33 relayed the phishing message below to our client's mail server. It was submitted through an authenticated (ESMTPSA) login, so a mailbox on that Postfix server has very likely been compromised and is being used by a phishing operator. Please have the customer reset the account, review their SASL logs for logins from 62.60.130.0/23 and 62.60.134.0/24, and stop the relay.

Message details
- Delivered: Sat, 31 Oct 2026 13:19:29 -0700
- From (spoofed): "[IMPERSONATED FIRM] LTD." (SPF -all FAILS from this relay)
- Relay: Postfix ESMTPSA, queue ID DCF9C1146678
- Submitted from: [62.60.134.68], HELO [62.60.130.6]
- Lure: fake QuickBooks invoice for $11,125.99; "Preview" links to https://titan-invoice.surge.sh
[history section, evidence and preservation request follow; the full original message is attached]

7. Timeline and follow-up

13:19 PT	Phishing email arrives in the client's inbox.
13:25 PT	Client forwards the .eml. Case opened: headers and body parsed, links and IPs looked up (WHOIS/RDAP, DNS, SPF).
13:27 PT	History search done: 3 linked emails from the same kit found.
13:29 PT	Blocks added and tested.
13:31 PT	All reports sent; delivery checked in the log; one bounce recorded.
Next 14 days	We watch for abuse-desk replies and answer any request for more evidence. We re-check the landing page (still online at 13:33 PT on 31 Oct 2026, pending surge.sh action) and send a follow-up if it is not removed.

What the client should do now

- Don't pay, reply, or click "Preview". If you owe this firm money, call them on a number you find yourself, not one from the email.
- If anyone on your team already sent an e-Transfer, call your bank right away and ask for a fraud recall. Then report it to the Canadian Anti-Fraud Centre (1-888-495-8501) and your local police.
- Tell your accounts-payable staff: invoices with a new payment method or a non-Intuit payment link get checked by phone before payment.

Got a phishing email, scam website or fake invoice?

Forward it to us and we do everything in this report for you: trace it, block it, and report it to every host, registrar, brand and regulator that can take it down.

C$49 one case

One phishing email or scam site, fully traced and reported.

C$29 / month

Up to 5 cases a month. Cancel any time.

Start here: **strategiccryptoreserve.ca/phishing-takedown-service.html**

Send your .eml file to **takedown@cryptoinvestor.ca** · Company line +1-778-557-2041

One-time case fee, or a monthly plan that renews each month until you cancel. All Terms of Service must be read and agreed: strategiccryptoreserve.ca/terms.html#takedown · Payments and refunds: terms.html#payments. We report abuse to the organisations able to act on it. We cannot guarantee that a third party removes content or prosecutes, and we never contact or threaten the scammer on your behalf.