2026 Mailbox Compromises: spam sent from NFE accounts

Incident report: spam sent from aaron.tushabe@nearlyfreeenergy.com (31 Mar – 1 Apr 2026)

*Prepared 20 Oct 2026 · read-only investigation (nothing was changed, deleted or sent) · **Status: open**, severity S2 (see the [severity matrix](#))*

Summary

The spam was **real, authenticated mail sent through NFE's own mail server**, not spoofing or backscatter. Someone had Aaron's **mailbox password** (the LDAP password shared by IMAP/SMTP, Roundcube webmail and Nextcloud). Several separate spam operators used it during a **~6-hour window, 31 Mar 2026 18:52 UTC → 1 Apr 01:11 UTC**:

- some logged in to **Roundcube webmail** (webmail.nearlyfreeenergy.com) and sent Bcc blasts of 99 recipients each;
- others used **SMTP AUTH** on smtp.nearlyfreeenergy.com:587/465 with bulk-mailing tools.

The bounces that came back on 1–9 April were delivery failures and retries for mail submitted in that window. **Nothing was sent after 01:11 UTC on 1 Apr.**

The password most likely came from a **leaked credential list ("combo list")**: the attackers' own tool messages say "PydroidCH SMTP Cracker EMAIL:PASS". The leak itself is still unexplained. Possible sources: an infostealer on a device, a phishing page, or the same password used on another site.

A **second, separate compromise** hit **dansturn.kimbowa@** from May to 3 Sep 2026. It used SMTP only, a different spam tool and German-language phishing/dating spam (see below). The common weakness: NFE's mail server accepts a bare password for SMTP submission, with no 2FA

and no per-user sending limits.

Evidence

Finding	Evidence
Sent through NFE's server, authenticated	Every returned original is DKIM-signed `d=nearlyfreeenergy.com s=mail` (only NFE's server holds that key), has envelope sender `aaron.tushabe@…`, and passed SPF/DKIM/DMARC at Gmail. Bounces come from NFE's own outbound relays (fi-relay / de-relay.federatedcomputer.com).
Password was harvested and tested by an SMTP checker	Messages from the account to attacker addresses: "You get a new smtp", "HIT ◫ smtp.nearlyfreeenergy.com", "SMTP Checker Test – PydroidCH SMTP Cracker EMAIL:PASS", plus "Jerry Rivera" (a host|port|user|pass line). They contain the **full old password in clear text**, with the login given as the full email address.
Roundcube webmail was used	"Loan Offer" (Samuel Braandon) and "US Department of the Treasury" (Danny Alba) carry Roundcube's fingerprint: `X-Sender`, `Mail-Reply-To`, `format=flowed`, md5 Message-IDs. 41 copies are in **Sent** (5–99 Bcc each, 3,965 recipients) and ~42 attacker drafts are in **Drafts** (31 Mar 19:24–00:16 UTC). Roundcube saves both automatically. Roundcube 1.7.x is publicly reachable at webmail.nearlyfreeenergy.com.
SMTP AUTH with a bulk mailer was also used	The "Emily Portney" campaigns ("I need your quick response", "Please get back to me") went one recipient per message, with Message-IDs in `YYYYMMDDhhmmss.HEX@domain` format, and were never saved to Sent.
Multiple operators	Different personas, reply-to addresses and sender timezones (−07:00, −04:00, +03:00, +13:00), and "hit" notices sent to five different attacker mailboxes. This fits a credential that was sold or shared.
Not a Nextcloud Mail send	The Nextcloud Mail outbox is not involved, and none of the originals have Nextcloud Mail headers.
No persistence left in mail settings	The active Sieve script only holds Aaron's three filing rules: no redirect, forward or vacation. No aliases.

Timeline (UTC)

Time	Event
31 Mar 18:52	First spam submitted ("From Patricia E. Harri…", "Patricia Bloomberg Foundation" persona)

Time	Event
18:54 → 22:04	"Loan Offer" Bcc blasts via Roundcube (~570 bounces from this campaign alone)
19:52	French "AR24 registered letter" phishing lure sent from the account
19:58 → 00:00	SMTP checker "hit" notices sent to attacker mailboxes (gmail/outlook/hotmail)
21:53 → 1 Apr 01:11	"Emily Portney" bulk-mailer campaign via SMTP AUTH (≈2,500 bounces)
~22:00–22:04	**Mail history before this point disappears** from INBOX, Sent, Trash, Archives and Archives.2025 (see Unknowns)
22:48	"Leads / databases for sale" spam ("Paul")
23:10 → 1 Apr 00:08	"US Treasury" Bcc blasts via Roundcube (40 × 99 recipients)
1 Apr 01:11	Last submission seen
1 Apr – 10 Apr	Bounces, delayed DSNs, Outlook retry failures (4.7.650) and auto-replies arrive. **No new sends.**

Volume: about **14,400 bounce notices** (2,145 in "Bounces April 2026", ~12,240 in Trash, plus some in Junk). Microsoft rejected mail from the relay IP 135.181.193.48 citing a **Spamhaus listing** , so this also hurt deliverability on Federated Computer's shared relay.

Still unknown

1. **How the password leaked.** It was long and random, which rules out guessing. That leaves an infostealer (passwords saved in a browser or mail client on a compromised device), a phishing page, or the same password used elsewhere and leaked there.
2. **Source IPs and first login.** NFE's MTA strips submission `Received` headers, so no client IP survives in the bounces. Only server logs can show this: Postfix `sasl_username`, Dovecot auth and Roundcube `userlogins` for 31 Mar 2026. Nextcloud's activity stream only goes back to 27 Apr 2026 and doesn't log logins anyway.
3. **Whether Nextcloud itself was accessed.** The same LDAP password logs into Nextcloud, and **Aaron is in the `admins` group**. No evidence either way survives in the activity stream.
4. **The missing mail history.** INBOX, Sent, Trash, Archives and Archives.2025 contain nothing older than ~22:00 UTC on 31 Mar. Sent's oldest item is spam. Drafts still has Aaron's own drafts back to April 2025. Mail could have been bulk-deleted mid-attack, e.g. to hide bounces. *Open question: did anyone purge these folders or move the mailbox?* If not, ask Federated Computer whether backups from before 31 Mar exist.
5. The app password **"cli" created by an administrator on 13 Oct 2026** should be confirmed as legitimate.

Recommendations (for Aaron to approve. None have been applied.)

Now

- Confirm the rotated password is **not reused anywhere** and that the old one is gone from every saved-password store. The old password appears in clear text in several bounces in Trash and "Bounces April 2026", so treat it as public.
- Delete the "You get a new smtp" / "HIT" / "SMTP Checker" / "Jerry Rivera" bounces that contain the old password.
- Run a malware/infostealer scan on every device that had the password saved (browser and mail client). Check aaron.tushabe@nearlyfreeenergy.com at haveibeenpwned.com.
- Review Nextcloud → Personal settings → Security → Devices & sessions. Revoke anything unrecognised and confirm the "cli" app password.
- Ask Federated Computer for Postfix/Dovecot/Roundcube logs for 31 Mar 2026 18:00–1 Apr 02:00 UTC (logs may already have rotated), and for any pre-31-Mar mailbox backup. Also ask whether 135.181.193.48 is still on Spamhaus lists.

Harden

- **Enable 2FA in Nextcloud** (TOTP), at least for every account in `admins`. Note this alone does **not** protect IMAP/SMTP/Roundcube, which still accept the bare LDAP password.
- **Protect Roundcube**: add a 2FA plugin (e.g. `twofactor_gauthenticator`) or put it behind SSO/VPN. Otherwise retire it in favour of Nextcloud Mail, and keep it on the latest release.
- **Outbound rate limits per authenticated user** on submission: Postfix `smtpd_client_message_rate_limit` / `smtpd_client_recipient_rate_limit`, or rspamd `ratelimit` keyed on `user`. Set Roundcube `max_recipients` (about 20) and `max_group_members`. Add an alert when one user sends more than N messages per hour.
- **fail2ban / rate-limiting on SASL auth failures** for SMTP, IMAP and Roundcube logins.
- **App-password hygiene**: give each client (phone mail app, CLI tools, Claude skills) its own named app password, revoke unused ones, and never save the main password in browsers.
- **DNS** (checked today): SPF is `-all` and covers the relays, but has duplicate entries (`de-relay` and `fi-relay` each listed twice). DKIM selector `mail` is present. DMARC is `p=quarantine; sp=none; pct=100` with reports to admin@. Proposed: tidy the SPF duplicates and move DMARC to `p=reject; sp=reject` after a few weeks of clean aggregate reports. This stops outright spoofing, but would **not** have stopped this incident, since the spam was legitimately signed.
- Check the DMARC aggregate reports at admin@nearlyfreeenergy.com for 31 Mar–1 Apr. They show volume per sending IP.

Second account: dansturn.kimbowa@nearlyfreeenergy.com (May – Sep 2026)

216 bounce notices on Dansturn's account (now in "Bounces 2026", Trash and INBOX) were analysed the same way.

This is also a stolen password used for authenticated sending, not spoofing. All 216 returned originals are DKIM-signed `d=nearlyfreeenergy.com` and have envelope sender `dansturn.kimbowa@…`. They went out through fi-relay, or directly from NFE's server IP 128.140.54.201.

But it looks like a different actor and tool from Aaron's incident:

	Aaron (Mar–Apr)	Dansturn (May–Sep)
Window	One ~6-hour burst (31 Mar 18:52 → 1 Apr 01:11 UTC)	Low-and-slow bursts: 5–6 May, 18 May, 7 Aug, 15–19 Aug, 26 Aug, 29 Aug → **3 Sep 19:25 UTC** (last seen)
Route	Roundcube webmail **and** SMTP AUTH	SMTP AUTH only. Nothing in Sent or Drafts, and Sent history is intact back to Jul 2025
Tooling	SMTP-checker "hit" notices; Roundcube; bulk mailer with `YYYYMMDDhhmmss.HEX` Message-IDs	Commercial spam mailer: `X-Felis-L` / `X-rpcampaign` / `List-ID` headers, random lowercase Message-IDs, no `Date` header (added downstream). No checker "hit" messages seen
Content	English advance-fee / loan / "Treasury" scams; reply-to Gmail accounts	**German phishing** posing as Deutsche Rentenversicherung ("Ihre Daten sind veraltet", May). **Dating-spam lures** with German personas ("Anna sent a hello…", Aug–Sep), linking to throwaway tracker domains (maileo.app, edgeunite.co.uk and dozens of hacked sites)
Targets	Hotmail/Outlook, Gmail, AU ISPs	web.de / T-Online / freenet (DE), Comcast, Outlook
Bounce volume	~14,400	216 (low because the mailer throttles; real volume unknown)

Conclusion: the entry point is the same *kind*: a valid mailbox password accepted by the LDAP-backed SMTP submission service, which has no 2FA and no per-user rate limit. But nothing links the two incidents to the same actor or the same leak. There is no sign of a server-wide compromise either: team@ and dismas.friday@ show no outbound bounce waves this year. Each password was

most likely leaked separately (infostealer, phishing or reuse) and then sold.

Dansturn-specific actions

- **Urgent: confirm Dansturn's password was changed after 3 Sep 2026.** If not, change it now and treat the account as still compromised. The bounces stopped on 8 Sep, but that may just be the attacker pausing.
- Scan Dansturn's devices for infostealers. Check for reuse of the password elsewhere.
- Include Dansturn's account in the log request to Federated Computer (SASL logins for `dansturn.kimbowa`, May–Sep 2026).
- Side note: T-Online rejects mail sent **directly** from 128.140.54.201 ("Dialup/transient IP not allowed"). Ask Federated Computer why some outbound mail bypasses the relays.

Indicators (attacker-controlled addresses)

Reply-To / hit recipients: `emily.portney37@gmail.com`, `j6919069@gmail.com`, `samuelbrandon430@gmail.com`, `patriciabloomberg.foundation@gmail.com`, `dannyalba@usa.com`, `beinspired4730@gmail.com`, `gas.c@outlook.com`, `stephenschwarman252525@hotmail.com`, `richard.lerbier@gmail.com`, `alugixuge234@gmail.com`.

Lessons for this book

These incidents shaped the Leaked Credentials Runbook, Accounts, 2FA and App Passwords and the Audit Logging Policy.

Revision #1
Created 2026-10-20 23:53:52 UTC by MCP Server
Updated 2026-10-21 00:02:18 UTC by MCP Server