Email Security and Phishing

Email Security and Phishing

Adapted from GitLab's Phishing Program and Email Security Standards.

Email is the most common way into an organisation: phishing pages steal passwords, attachments install malware, and fake invoices or "urgent" requests trick people into paying.

How to spot phishing

- **Urgency or fear:** "your mailbox will be deleted today", "invoice overdue", "account suspended".
- **Login links:** "verify your account", "storage full", "shared document". NFE systems never ask you to log in from an email link. Open nextcloud.nearlyfreeenergy.com yourself.
- **Mismatched sender:** a display name that says "Nextcloud Admin" but a strange address, or a Reply-To that differs from From.
- **Unexpected attachments:** `.html`, `.htm`, `.zip`, `.iso`, `.exe`, Office files asking to "enable content".
- **Money or gift-card requests,** even from a colleague's name. Confirm by phone or Talk.
- **Grant, loan and "funding" offers** that ask for fees or personal details.

What to do

You...	Do this
Got a suspicious email, didn't interact	Forward it **as an attachment** to the Security DRI or post in Talk, then move it to Junk
Clicked a link but entered nothing	Report it (S3). Close the tab. Run a malware scan
Entered your password, opened an attachment or replied	**Urgent:** change your password from a trusted device, then follow the Leaked Credentials Runbook
See bounces for mail you didn't send	**Urgent:** your account is probably sending spam. Report immediately

Domain protections (nearlyfreeenergy.com)

Checked October 2026:

- **SPF:** `-all` (strict), covering our server and the Federated Computer relays. Has some duplicate entries to tidy.
- **DKIM:** selector `mail`, published.
- **DMARC:** `p=quarantine; sp=none`, with reports to admin@. *Target:* `p=reject; sp=reject` once reports look clean.

These stop other people **forging** our domain. They don't stop someone who has a real NFE password: that mail is genuinely signed. So account protection (2FA, unique passwords, rate limits) matters most.

Training

Phishing awareness is part of onboarding. The Security DRI may run occasional practice phishing emails. If you report them, great; if you click, you'll get a short refresher, with no blame.

Revision #1
Created 2026-10-20 23:50:21 UTC by MCP Server
Updated 2026-10-21 00:02:11 UTC by MCP Server