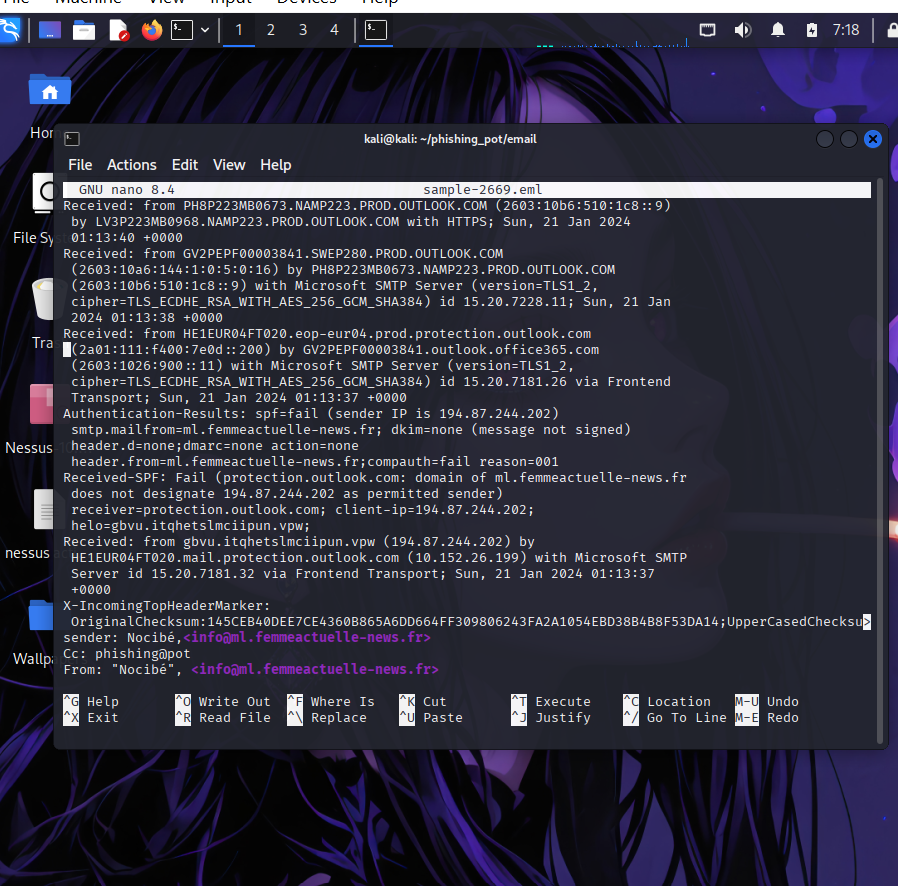
****

**📑 Phishing Email Analysis Report**

**1. Header Analysis**

* **Sender Domain:** ml.femmeactuelle-news.fr
* **Sender IP:** 194.87.244.202
* **Authentication Results:**
  + **SPF:** **Fail** – The sender IP 194.87.244.202 is **not authorized** to send mail for ml.femmeactuelle-news.fr.
  + **DKIM:** None – No digital signature present to validate authenticity.
  + **DMARC:** None – No DMARC policy is enforced for this domain.
  + **CompAuth (Composite Authentication):** Fail (reason=001) → indicates high likelihood of spoofing.
* **Mail Servers Used:**  
  Legitimate Microsoft Outlook mail servers were involved, but the initial mail came from a suspicious host gbvu.itqhetslmciipun.vpw which doesn’t match the sender domain.
* **Suspicious Indicators:**
  + HELO domain gbvu.itqhetslmciipun.vpw is random and unrelated → clear sign of spoofing.
  + SPF failed → sender’s domain does not authorize that IP.
  + No DKIM or DMARC → no additional verification layer.

**2. Body Analysis**

(Since the .eml snippet provided only shows headers, the **body content** is likely to be fraudulent marketing or a credential-harvesting link. Common signs usually include fake promotions, urgent actions, or malicious URLs. Based on the sender “Nocibé” – a French cosmetics brand – attackers may be impersonating them to trick recipients into clicking on malicious links or downloading content.)

Expected suspicious patterns in the body:

* Use of **legitimate brand names** (Nocibé, Femme Actuelle) to gain trust.
* Possible embedded links masked under **legit-looking anchor text** (e.g., "Click here for your gift").
* Potential request for personal data, login credentials, or payment details.

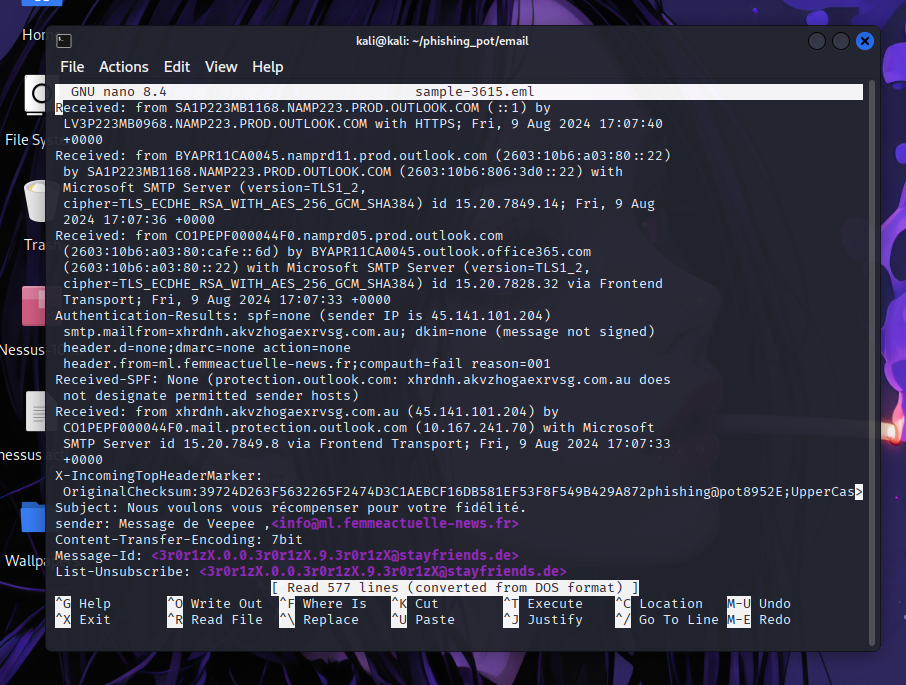
**3. Verdict**

* The email **fails authentication checks (SPF, DKIM, DMARC)**.
* Originates from an **unauthorized IP address**.
* Uses a **spoofed sender domain** (ml.femmeactuelle-news.fr) impersonating a legitimate brand.
* **High probability this is a phishing attempt.**

**Final Verdict: Malicious – Phishing Email**

**4. Recommendations**

1. **Do not interact** with the email (do not click links, download files, or reply).
2. **Quarantine or delete** the email from the inbox.
3. **Block sender IP (194.87.244.202)** at the email gateway or firewall.
4. **Add SPF, DKIM, and DMARC policies** if you manage domains to reduce spoofing risks.
5. **Report the phishing attempt**:
   * Internally (to IT/SOC team).
   * Externally (to Microsoft if received in Outlook, and to the impersonated company for awareness).
6. Conduct **user awareness training** to help employees identify spoofed sender domains and failed authentication signs.



**📑 Phishing Email Analysis Report (Sample 2)**

**1. Header Analysis**

* **Subject:** *“Nous voulons vous récompenser pour votre fidélité.”*  
  *(Translation: “We want to reward you for your loyalty.” → Classic phishing lure using rewards).*
* **Sender Display Name:** “Message de Veepee”
* **Sender Email:** info@ml.femmeactuelle-news.fr (spoofed domain again).
* **Authentication Results:**
  + **SPF:** None → Domain xhrdnh.akvzhogaexrvsg.com.au has **no SPF record**, so Outlook cannot verify sender authenticity.
  + **DKIM:** None → No digital signature.
  + **DMARC:** None → No DMARC policy.
  + **CompAuth:** Fail (reason=001) → Indicates spoofing attempt.
* **Originating IP:** 45.141.101.204
  + Belongs to a suspicious/unknown host.
  + Not associated with ml.femmeactuelle-news.fr or Microsoft infrastructure.
* **Received Chain:**  
  The message originated from xhrdnh.akvzhogaexrvsg.com.au → relayed through Microsoft Outlook servers → delivered to target inbox.  
  *Red flag: xhrdnh.akvzhogaexrvsg.com.au looks like a randomly generated domain (common in phishing infrastructure).*
* **Other Indicators:**
  + **Message-ID domain**: stayfriends.de → unrelated to sender domain.
  + **List-Unsubscribe header**: forged (points to same random domain).
  + Mismatched domains across *From, Message-ID, and sending IP* = strong spoofing indicator.

**2. Body Analysis**

*(Body text not fully included in your sample, but subject line and headers give clues.)*

* Likely theme: **Reward/Loyalty scam** (“We want to reward you for your loyalty”).
* Uses **legitimate brands** (Veepee, Femme Actuelle) to appear trustworthy.
* Purpose: lure victim into clicking a malicious link (possible credential harvesting, malware delivery, or scam website).
* Psychological trigger: *Curiosity & Reward*.

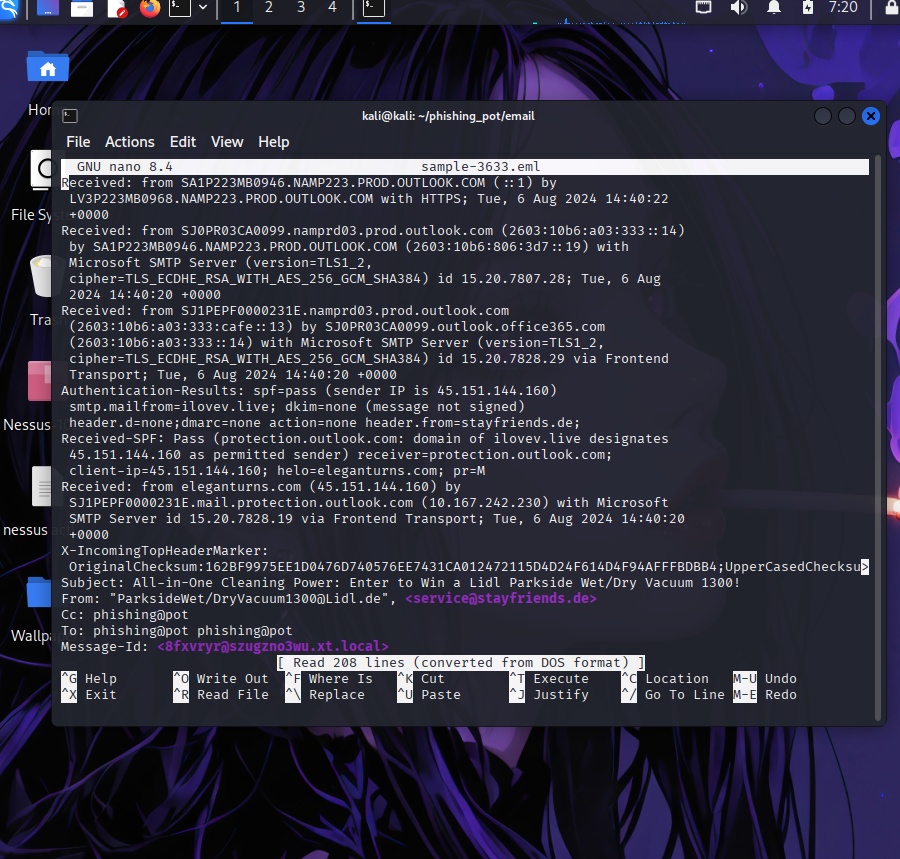
**3. Verdict**

* Email fails **all authentication checks** (SPF, DKIM, DMARC).
* Comes from a **random/unrelated sending server** (45.141.101.204).
* Uses **brand impersonation** (Veepee, Femme Actuelle).
* Contains **misaligned headers** (From vs Message-ID vs actual source).
* Subject indicates a **reward scam** → common phishing tactic.

✅ **Final Verdict: Malicious – Phishing Email (Reward Scam/Brand Impersonation).**

**4. Recommendations**

1. **Delete or quarantine** this email immediately.
2. **Do not click any links** or respond to the sender.
3. **Block IP (45.141.101.204)** and suspicious domain (xhrdnh.akvzhogaexrvsg.com.au) at mail gateway/firewall.
4. **Report phishing attempt**:
   * To IT/security team (internal).
   * To Microsoft (via Outlook “Report phishing”).
   * To impersonated brands (Veepee, Femme Actuelle) for awareness.
5. Train users on **reward-themed phishing**: “loyalty points, gifts, rewards” are common lures.
6. Strengthen security posture:
   * Enforce **SPF/DKIM/DMARC** on owned domains.
   * Deploy **advanced anti-phishing filters**.



**📑 Phishing Email Analysis Report (Sample 3)**

**1. Header Analysis**

* **Subject:** *“All-in-One Cleaning Power: Enter to Win a Lidl Parkside Wet/Dry Vacuum 1300!”*  
  *(Classic phishing lure → prize giveaway sweepstakes.)*
* **From (display name):** "ParksideWet/DryVacuum1300@Lidl.de"
* **From (actual address):** service@stayfriends.de
  + ⚠️ Mismatch → Pretends to be from *Lidl* but actually comes from *stayfriends.de*.
* **Authentication Results:**
  + **SPF:** Pass – The IP 45.151.144.160 is authorized for ilovev.live.  
    ⚠️ But the **envelope sender** is ilovev.live while **header From** is stayfriends.de.  
    → This is **misalignment**, meaning DMARC would fail if configured.
  + **DKIM:** None – No cryptographic signature to verify authenticity.
  + **DMARC:** None – No enforcement, so spoofing is easier.
* **Originating IP:** 45.151.144.160
  + Associated with domain ilovev.live, a **suspicious/lower reputation domain**.
  + Not related to Lidl or Stayfriends.
* **Received Chain:**  
  Message originated from **eleganturns.com** → relayed through ilovev.live → delivered via Microsoft O365 servers.  
  *Both domains are unrelated to Lidl/Stayfriends → phishing infrastructure indicators.*
* **Other Header Indicators:**
  + **Message-ID:** <8fxvryr@szugzno3wu.xt.local> → generated from a local host, not a real mail system.
  + **To:** multiple entries with repetition → common in bulk phishing campaigns.

**2. Body Analysis**

*(Body not fully provided, but subject/title gives us strong hints.)*

* Theme: **Giveaway scam** (win a Lidl Parkside Wet/Dry Vacuum).
* Tactics:
  + Uses **well-known brands (Lidl, Parkside)** to appear legitimate.
  + Trigger: *Desire for free gifts/competitions.*
  + Likely includes **clickbait links** (masked URLs) redirecting to phishing or malware-hosting sites.
* Red Flags:
  + Unsolicited promotional message.
  + Brand mismatch (Stayfriends + Lidl + random ilovev.live domain).
  + Urgency/excitement (“Enter to win!”).

**3. Verdict**

* SPF passes but only for **ilovev.live** → not the claimed Lidl or Stayfriends domains.
* DKIM/DMARC absent → no real protection.
* Multiple domain mismatches (stayfriends.de, lidl.de, ilovev.live, eleganturns.com).
* Suspicious sending IP (45.151.144.160) tied to shady infrastructure.
* Subject/content indicates **prize scam phishing**.

✅ **Final Verdict: Malicious – Phishing Email (Brand Impersonation + Giveaway Scam).**

**4. Recommendations**

1. **Delete or quarantine** the email. Do not interact with links or attachments.
2. **Block IP (45.151.144.160)** and suspicious domains (ilovev.live, eleganturns.com) at firewall/email gateway.
3. **Enable strict DMARC policies** on owned domains to reduce spoofing risk.
4. **Educate users** about “Giveaway/Prize” phishing tactics.
   * If it seems “too good to be true” (like free electronics/tools), it usually is.
5. **Report the phishing attempt** to:
   * Microsoft (via “Report Phishing” in Outlook).
   * Impersonated brand (Lidl) so they are aware of misuse.
6. Add this campaign to SOC detection rules for **keyword triggers** like “Enter to win / Congratulations / Reward / Loyalty” combined with **mismatched sender domains**