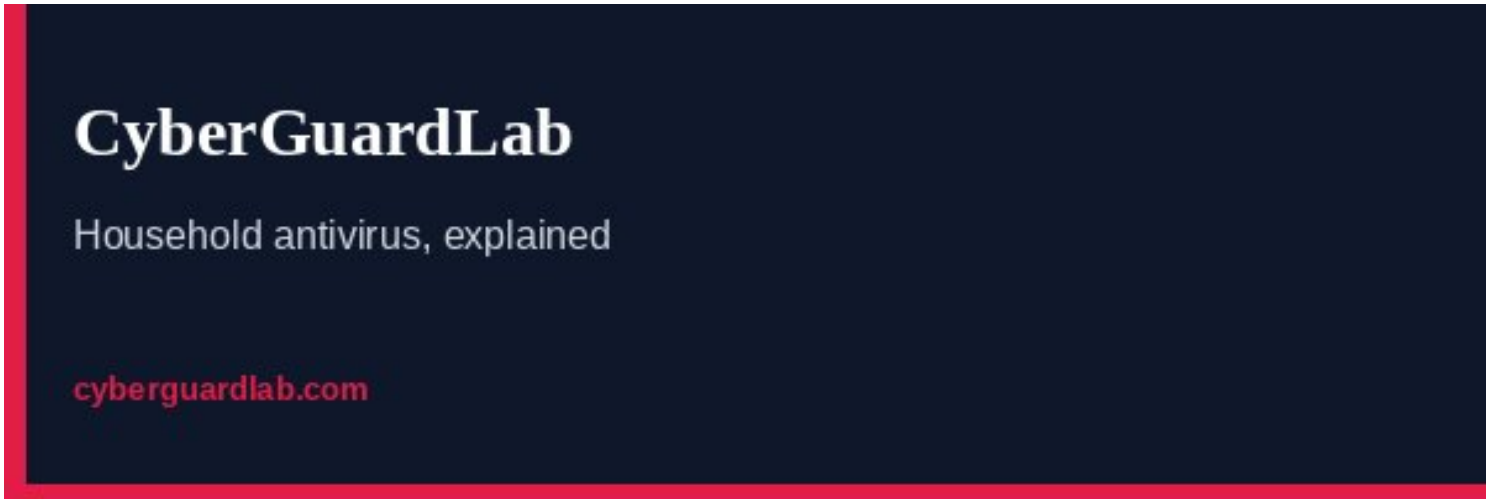
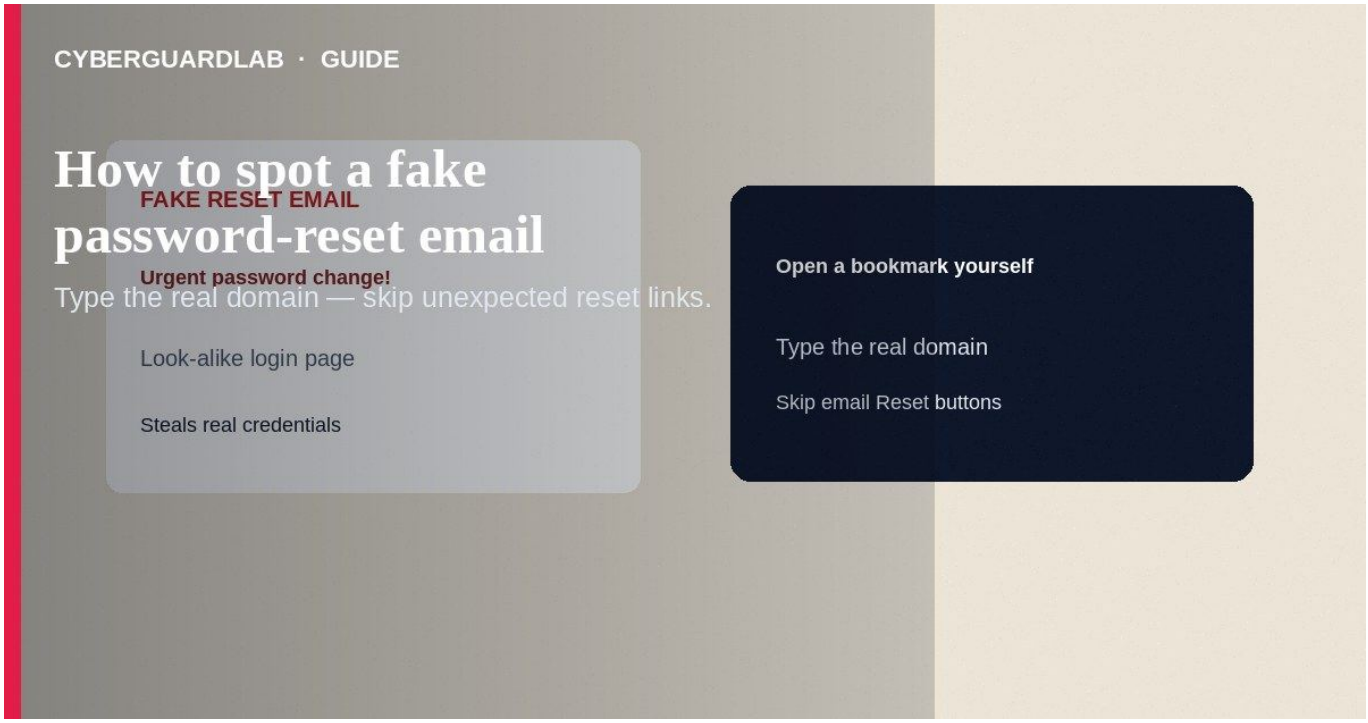


How to spot a fake password-reset email

https://cyberguardlab.com/blog/fake-password-reset-email

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A fake password-reset email pretends to be Google, Apple, Microsoft, your bank, payroll, or a store-warning that someone tried to change your password-so you click a look-alike link and type your real credentials. Do not use links inside unexpected reset mail. Open a bookmark or type the real domain, then check security settings yourself. This scam-spot guide is email/SMS reset phishing-not password manager vault alerts, not browser push scareware, and not passkey enrollment steps.

1. What this scam looks like

Subject lines include "Unusual sign-in," "Reset your password now," "Your mailbox is full-verify," or "Payroll password expires tonight." The From name shows the brand, but the real address is a free mailbox or a domain with extra characters. Links go to `micros0ft-login...` style hosts. Some attach HTML files; others move you to WhatsApp "IT support."

Related cues overlap how to spot a phishing email. SMS variants ("Apple ID locked") follow the same rule: no codes to strangers.

Help-desk impostors call while a reset email is on your screen and ask you to read the code aloud. Hang up. Real IT will not ask you to relay MFA codes to prove identity over an unexpected call.

2. Legitimate vs scam cues

Cue | Likely legitimate | Likely scam

You started it | You clicked "Forgot password" minutes ago | Cold reset you did not request

Link target | Exact brand domain you typed/bookmarked | Look-alike host or unexpected redirect

Tone | Calm, limited detail | Threaten lockout, arrest, or payroll stoppage

Codes | Code only when you are mid-reset on the real site | Caller/email asks you to read back a code

Attachments | Rare for resets | HTML/DOC "reset form" attachment

3. What to do if you get one

* Do not click the reset button in the email. Do not open attachments.
* Navigate yourself to the real site/app and review recent security activity.
* If you did not request a reset but the real site shows one pending, secure the account (change password from a clean device, revoke sessions, enable MFA/passkeys).
* Report phishing via the provider's "Report phishing" tool; delete the message.
* If you already typed a password on a fake page: change it on the real site immediately; change any reused passwords; enable MFA.
* Scan the device with Norton or Bitdefender; keep one primary product (TotalAV, McAfee, Avast).
* For identity-heavy accounts, use IdentityTheft.gov checklists when needed.

4. What to do if you get one

* Do not click the reset button in the email. Do not open attachments.
* Navigate yourself to the real site/app and review recent security activity.
* If you did not request a reset but the real site shows one pending, secure the account (change password from a clean device, revoke sessions, enable MFA/passkeys).
* Report phishing via the provider's "Report phishing" tool; delete the message.
* If you already typed a password on a fake page: change it on the real site immediately; change any reused passwords; enable MFA.
* Scan the device with Norton or Bitdefender; keep one primary product (TotalAV, McAfee, Avast).
* For identity-heavy accounts, use IdentityTheft.gov checklists when needed.

FAQ

I requested a reset-how do I know the email is real?

Prefer opening the site from a bookmark. Hover/long-press links cautiously; when unsure, ignore the mail and restart reset from the typed URL.

How is this different from a vault breach alert?

Vault alerts appear inside your password manager's UI/monitoring. Fake reset mail is unsolicited email designed to harvest passwords.

Will a passkey stop this?

Passkeys reduce password typing on real sites, which shrinks phishing success-but you must still ignore fake pages that ask for old passwords or codes.

Microsoft/Google said "you got a reset you didn't request."

That can be a real notice of someone else's attempt. Still open security settings yourself-do not use the email's button if anything looks off.

The email has my full name and last login city-is it real?

Not necessarily. Breaches and prior phishing give scammers personal details. Still open security settings yourself instead of using the message's button.

If you still want a paid suite

Avoiding how to spot a fake password-reset email does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* FTC: How to recognize and avoid phishing scams
* CISA: Recognize and report phishing
* Microsoft: Protect yourself from phishing
* Google Account Help: Password reset issues

Also read

* How to spot a phishing email
* How to recover from a password manager vault breach alert
* How to spot a malicious browser push notification scam
* How to set up a password manager for a US household
* How to spot a fake Google Play billing phishing email