

TraceMyEmail Scan Report

Generated 07 July 2026

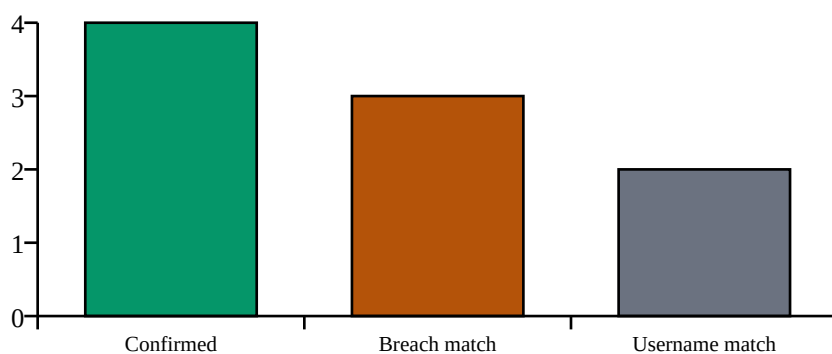
Scan ID: **sample-00000000-0000-0000-0000-000000000000**

This report is generated from a verified email address you provided. The email address itself is never included in this document, only the Scan ID above, which identifies this report without identifying you.

Executive Summary

Category	Services found
Forums	3
Other	1
Productivity	3
Social	2

Source breakdown



Risk summary

6 service(s) -- including any already marked Confirmed below -- were found in a breach that exposed email addresses and potentially password data. These are the highest priority to secure.

Full Results

Forums

Service	Source	Detection method	Breach date	Where exposed
GitHub	Confirmed	Self-reported	--	--
Reddit	Username match	Public profile match	--	--
Medium	Username match	Public profile match	--	--

Other

Service	Source	Detection method	Breach date	Where exposed
MyFitnessPal	Breach match	Data breach	2018-02-01	MyFitnessPal

Productivity

Service	Source	Detection method	Breach date	Where exposed
Adobe Creative Cloud	Confirmed	Data breach	2013-10-04	Adobe
Dropbox	Confirmed	Data breach	2012-07-01	Dropbox
Canva	Breach match	Data breach	2019-05-24	Canva

Social

Service	Source	Detection method	Breach date	Where exposed
LinkedIn	Confirmed	Data breach	2016-05-18	LinkedIn
Tumblr	Breach match	Data breach	2013-02-28	Tumblr

What "Source" means

Source	What it means
Confirmed	You've confirmed this is your account.
Breach match	Your email address was found in a documented data breach for this service.
Username match	A public profile using a likely username for your email was found on this service.

Actions to consider

Service	Actions	
	Change password	Delete account
Adobe Creative Cloud	https://account.adobe.com/security	https://helpx.adobe.com/manage-account/using/cancel-creative-cloud-subscription.html
Dropbox	https://www.dropbox.com/account/security	https://help.dropbox.com/
LinkedIn	https://www.linkedin.com/psettings/change-password	https://www.linkedin.com/help/linkedin/answer/a1339724
GitHub	https://github.com/settings/admin	https://docs.github.com/en/account-and-profile/setting-up-and-managing-your-personal-account-on-github/managing-your-personal-account/deleting-your-personal-account
Canva	https://www.canva.com/account/security	https://www.canva.com/help/delete-account/
MyFitnessPal	--	--
Tumblr	https://www.tumblr.com/settings/account	https://www.tumblr.com/settings/account
Medium	https://medium.com/me/settings/security	https://help.medium.com/hc/en-us/articles/360034750933
Reddit	https://www.reddit.com/settings/account	https://support.reddithelp.com/hc/en-us/articles/360043513151

Other actions to consider

1. Use a password manager

Reusing a password across services means one breach can unlock all of them. A password manager (e.g. 1Password, Bitwarden, or your browser's built-in one) generates and stores a unique password per service, so a single breach exposes one account.

2. Privacy improvement steps

- Turn on two-factor authentication where possible for every account.
- Change the password on any account linked to a breach that exposed passwords, even if you no longer use it.
- Delete accounts you no longer use -- an account that doesn't exist can't be breached again.
- Use a unique, random password per service going forward.
- Check back periodically -- new breaches surface for email addresses that have been in circulation for years.