Flotek group

Powered by
BREACH MONITOR

— CREDENTIAL EXPOSURE REPORT —

YOUR DATA WAS FOUND ON THE DARK WEB

Our scan has identified compromised credentials linked to your organisation. This report details what was found, what it means, and the steps your team needs to take **immediately**.

DOMAIN SCANNED	EXPOSURES FOUND	SOURCE TYPE	REPORT GENERATED
example.com	5	Dark Web Forum	09/04/2026

Last Seen	Asset / Domain	Email Address	Username	Name	Password	Database	Found In
Dec 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••024 Hidden	url login pass12-12	CRACKED.SH
Oct 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••e99 Hidden	combolist-q3-2025	DARKFORUM.ONION
Aug 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••23! Hidden	breach-dump-aug25	PASTE SITE
Jun 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••327 Hidden	leaked-db-2025	PASTE SITE
Mar 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••023 Hidden	combolist-q1-2025	BREACH-DB
Jan 2025	example.com	demo@gmail.com	demo-user	demo-user	•••••••ede Hidden	old-breach-jan25	BREACH-DB

This report does **not** display password data. Enabling Breach Monitor's automated monitoring unlocks full credential visibility, including exposed passwords, helping identify password reuse and minor variations created over time.

UNLOCK FULL PASSWORD VISIBILITY

To view **exposed passwords** and full breach details, you will need Breach Monitor. Running regular dark web scans is essential because data is exposed when the websites and services people use suffer breaches that you often hear about in the news. Once data is available online, reused or slightly modified passwords become a **real risk.** Breach Monitor alerts you **when your data appears online**, allowing your IT team to act quickly.

GET BREACH MONITOR

03 - RESPONSE

WHAT YOU NEED TO DO NOW

STEP ONE

CHECK IF IT'S A COMMON PASSWORD

URGENT

If the exposed password is something simple like **Password1!** or your company name, it is likely in use by others too and actively targeted. Replace it immediately with a long, unique passphrase of at **least 14 characters.**

STEP TWO

RESET THE PASSWORD AND REVOKE ALL SESSIONS

URGENT

Changing the password is not enough on its own. **Revoke all active sessions** on the affected account so anyone already logged in — including a potential attacker — is immediately signed out. Most platforms offer a **"sign out everywhere"** option in security settings.

STEP THREE

RESET IT EVERYWHERE ELSE YOU USED IT

URGENT

If that password was used on any other service — even once — treat those accounts as **compromised** too. Attackers run automated tools that try **stolen credentials** against hundreds of platforms within minutes. Change every account that shared that password.

STEP FOUR

ENABLE TWO-FACTOR AUTHENTICATION

IMPORTANT

Once the password is reset, immediately **enable 2FA** on the account if not already active. Even if the new password is later exposed in another breach, 2FA means an attacker still cannot access the account without a second form of verification.

STEP FIVE

CHECK FOR SUSPICIOUS ACTIVITY

IMPORTANT

Review the account's login history, sent emails, connected apps and any **recent changes** to account settings. Look for logins from **unfamiliar locations or devices.** If anything looks unusual, contact your IT team immediately — do not wait.

STEP SIX

USE A PASSWORD MANAGER GOING FORWARD

RECOMMENDED

The root cause of most **credential breaches** causing wider damage is password reuse. A password manager generates and stores a **unique, complex password** for every single account — so one breach can never cascade into many. This is the single most impactful security habit you can build.