

# Google Workspace Under Login Attack: What to Do

*A one-page playbook for small and mid-size organizations*

Failed logins are normal background noise on the internet. The real question is whether any are succeeding, and whether your accounts are protected if one does.

## Step 1: Check if anything got in

Sign in to [admin.google.com](https://admin.google.com) and go to Reporting > Audit and investigation > Login audit log. Filter for successful logins in the last 30 days. Look for logins from countries no one works in, unfamiliar IP addresses, or dormant accounts.

If you find a suspicious successful login, suspend the account, reset the password, sign out all sessions, and check the user's Gmail for new forwarding rules or filters.

## Step 2: Audit your 2FA coverage

Go to Reporting > User reports > Security. This shows you who has 2-Step Authentication (2FA) turned on and who does not. Immediately add 2FA to all accounts without it.

## Step 3: Close the biggest gaps, in order

- **Enforce 2-Step Authentication for everyone.** This single change does more than everything else combined. Set a deadline 2 to 4 weeks out, communicate it clearly, and help the few people who need help enrolling. Path: Security > Authentication > 2-Step Verification.
- **Disable app-specific passwords.** These bypass 2FA. Once legacy protocols are off, almost nothing legitimate needs them. Path: Security > Authentication > Less secure apps and app passwords.
- **Give admins hardware security keys.** SMS and authenticator codes can still be phished. Hardware keys (YubiKey, Titan) cannot. Budget about \$50 per admin for two keys, primary and backup.
- **Review which outside apps have access to your data.** Path: Security > Access and data control > API controls. Revoke anything unfamiliar or unused for 90+ days.

## Step 4: Turn on alerts so you find out faster next time

Path: Security > Alert center > Settings. Enable alerts for suspicious logins, leaked passwords, and changed email settings. Route them to an inbox or channel someone actually reads.

**If you do only one thing: enforce 2-Step Verification for everyone.** *It is the single highest-impact change you can make.*

---

Revision #1

Created 14 May 2026 02:22:27 by Josh

Updated 14 May 2026 02:26:42 by Josh