Reset every user's password after a security event

A credential leak — a breach at a vendor, a phishing wave, a stolen laptop — makes every password in the office suspect. Rotate them all. Pipeline doesn't have a one-click bulk reset, but the per-user path is short and the full rotation goes faster than it sounds.

Introduction

A reused or phished password only protects you until someone else has it. After any event that might have exposed credentials, the right move is to invalidate them. The way to do that in Pipeline is to send every user a reset link from *Manage Users*. Each user clicks the link, sets a fresh password, and the old credentials stop working.

There's no shortcut, but it goes faster than it sounds — about five minutes for ~120 users. While you're at it, this is a good moment to turn on *Two-Factor Authentication* if you don't have it on already. That makes the *next* leaked password useless.

Why this stops a credential leak cold

A leaked password is only dangerous as long as it still works. Once every user has reset, the leaked credentials are dead — and the attacker has nothing to use them on. The five minutes you spend walking *Manage Users* buy you a clean account.

1. Audit your active user list

Open *Manage Users* and skim the active roster. Deactivate anyone who shouldn't have access — former agents, expired logins, role changes that haven't been cleaned up. Resetting passwords on profiles that should be gone is wasted work.

Learn how → *Users*

2. Send a password reset email to each active user

For every user on the list, click the gear icon next to their name and pick [Reset Password]. Pipeline emails them a reset link. Tell them the email is coming so it doesn't get ignored.

If a profile is inactive and you see a *"D'oh!"* error, activate it first (gear icon → [Activate User]), reset, then deactivate again if needed.

3. Turn on Two-Factor Authentication

If your office doesn't already require 2FA, this is the time. Go to *Admin / Settings* → *Feature Settings* → **Require Two-Factor Authentication** → save. Every sign-in now needs a one-time code along with the password.

Learn how → *Two-Factor Authentication*

4. Tell your team what to do

Send a short note to everyone: *"We've reset every Pipeline password as a precaution. You'll get a reset email from* ***help@paperlesspipeline.com*** *— click the link, set a new password, and from now on you'll also enter a security code from your email when you sign in."*

5. Ask support for a login report (optional)

If you suspect credentials were actually used, write to support from your master admin email and request a login report covering the relevant date range. The report shows timestamp, IP address, and the email used for each sign-in — enough to confirm what happened.