Was a user's Pipeline account used to send unauthorized emails?

Bounce-backs from Pipeline messages you didn't send. Reports of spam from your address. The first instinct is *"we've been hacked"* — and the fix is straightforward.

Reason

Someone got hold of the user's Pipeline credentials and signed in long enough to send messages from their profile. The Pipeline platform itself stays intact. The breach is at the credential level. Once the credentials are reset and 2FA is on, the account is locked back down.

Solution

Act in this order:

- **Change the affected user's Pipeline password.** The user can update it from *My Info*, or an admin can issue a reset.
- **Change the user's external email password too** — especially if it's the same as the Pipeline one.
- **Turn on Two-Factor Authentication for the office** under *Admin / Settings → Feature Settings*. A stolen password alone won't get past 2FA.
- **Contact support.** We can delete the unauthorized messages from the account (with admin approval), notify affected recipients, and pull a login report so you can see exactly what happened.

If you store passwords in a browser or document, move them into a password manager so the same credentials can't leak the same way again.