Re-secure a compromised account

When you suspect a user's account has been accessed by someone who shouldn't have it, this is the sequence that locks it back down and gives you a clear picture of what happened.

Introduction

Most *"is my account hacked"* worries trace back to leaked credentials — a password reused on a site that got breached, a stolen device, a phishing email someone clicked. Pipeline itself stays intact. The breach is at the credential level, and the fix is at the credential level too.

This use case walks the full sequence: change what's leaked, turn on the extra barrier, ask support for the audit trail, and clean up the damage. Run it in order. The password reset comes first because everything after it builds on a clean credential.

Why this gets you back to clean

You're not just changing a password. You're closing every door someone could use to get back in, and giving yourself the evidence to know what got touched. By the end, the account has fresh credentials, an extra sign-in barrier, a documented login history, and any unauthorized activity cleaned up.

1. Reset the affected user's Pipeline password

The user updates their password from *My Info*. If they're locked out, they can reset it from the login page.

Learn how → *Password Reset*

2. Reset the user's external email password

If the email account itself was the breach point — or even if you're not sure — change that password too. Pipeline's 2FA codes go to that inbox, so the email account is part of your security boundary.

3. Turn on Two-Factor Authentication for the office

With 2FA on, a stolen Pipeline password alone won't get anyone in. Every user enters a one-time code emailed to their login address.

Learn how → *Two-Factor Authentication*

4. Ask support for a login report

Write to support from your master admin email and request a recent login history for the account. The report includes timestamp, IP address, and the email used for each sign-in — enough to confirm what got accessed and from where.

5. Clean up any unauthorized activity

If unauthorized messages were sent, support can delete them from the account (with admin approval) and alert affected recipients. Check the user's *Notes & Sent Emails* tab on any transactions they touched to confirm nothing else was changed.