Compromised account: the protocol

The 5 recovery steps, in the right order — print before you need them.

THE 5 STEPS, IN ORDER

1. **Email first, always**
   It's the master key: whoever controls it resets everything else. Start there, even if another account seems affected.

2. **Password changed AND sessions signed out**
   Changing the password isn't enough: use “Sign out of all devices” in the security settings.

3. **Recovery options and rules inspected**
   Backup email, phone: yours? Forwarding rules and filters: empty or known list — that's where the attacker settles in.

4. **2FA on, linked accounts handled**
   Two-factor authentication on the recovered account, then password changed everywhere the same one served.

5. **Notify who needs to know**
   Bank (block the card), contacts if messages went out in your name, report according to your situation.

Have I been leaked? — 5 minutes

1. haveibeenpwned.com: enter your email address, read the listed breaches.
2. Any leaked password still in use anywhere: change it everywhere, now.
3. Turn on your manager's breach alerts (Bitwarden: Reports) — automatic from then on.

You can't react to what you don't know.

The 3-2-1 backup — the last line of defense

Two copies besides the original: trusted cloud + external drive unplugged outside backups.
Test a restore once a year — a backup never tested is a hope.
Report: UK Action Fraud · US ic3.gov · FR cybermalveillance.gouv.fr · ES 017 · BG cybercrime.bg