

Small business IT | Medium | 2 min read

What to do after a suspected breach in a small business

Finding out that an account may have been taken over, or that data may have leaked, is stressful. Calm, quick steps limit the harm. This is general information, not legal advice.

First hour: contain it

1. **Tell the person in charge** straight away, and do not blame anyone. Speed matters more than fault.
2. Disconnect affected computers from the network and Wi-Fi. Do not switch them off yet if you suspect ransomware, unless advised.
3. Change passwords on affected accounts from a different, clean device, and turn on two-step sign-in.
4. Sign out of all sessions where the service allows it.
5. Contact your bank at once if money or payment details are involved.

Next: find out what happened

- Write down what you saw, when, and who noticed it.
- Note which accounts, devices and data might be affected.
- Keep emails and screenshots as evidence.
- Check for odd forwarding rules in email, which attackers often add.

Recover safely

- Restore from a **clean backup** taken before the problem, after the cause is removed.
- Update and scan all devices.
- Tell customers or suppliers if they might receive scam messages from your account.

Personal data and reporting

If personal data was lost, stolen or exposed, UK GDPR has rules. You must decide whether it must be reported to the **ICO**, and this generally has to be done within 72 hours of becoming aware of it, where it is a risk to people. Check the ICO's website, which has a self-assessment and a reporting line. You can also report cyber crime through Action Fraud (in England, Wales and Northern Ireland) or Police Scotland.

Afterwards

Keep a record of what happened and what you changed, and review how it got in.

When to get more help

Call for help early if you suspect ransomware, large data loss, fraud against your bank, or if you cannot tell how far the problem has spread.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.