LESSON 05 OF 05 · 7 MIN · ESSENTIAL

# The first hour after “uh oh”

What to do in the first sixty minutes of a suspected incident, and the mistakes that make it worse.

## The first hour sets the cost

Most of the financial damage in a small business incident happens in the first hour: more money is transferred, more devices are infected, more evidence is destroyed. The response doesn't need to be sophisticated. It needs to be fast and in the right order.

Basic sequence: stop the spread, call the right people, preserve evidence, communicate deliberately.

## Stop, call, preserve

01 **Disconnect** affected devices from Wi-Fi and the network. Don't power them off, memory can hold evidence.

02 **Call the incident lead** and the deputy. Record the time.

03 **If money moved, call the bank's fraud line immediately.** Recall chances fall by the hour.

04 **Call your insurer** before engaging your own forensics, if the policy requires it.

05 **Preserve** emails, logs and devices. Don't tidy up, rebuild or delete.

06 **Agree the message** to staff, customers and suppliers before anyone posts.

## One page is enough

You don't need a 40-page policy. You need one page with names, numbers and the first-hour steps, printed and available offline in case email and file storage are down. Rehearse it once a year with the people named.

The most common failure isn't a missing tool. It's nobody knowing who decides.

> **DON'T TIDY UP**
>
> Deleting the phishing email, rebuilding the laptop or resetting every password can destroy the evidence needed to find the entry point, and to support an insurance claim.

### Key takeaways

- ✓ Disconnect affected devices; don't power them off.
- ✓ Call the bank immediately if money has moved.
- ✓ Preserve evidence before recovering or rebuilding.
- ✓ A one-page plan with named people beats a long policy.