FREE GUIDE

Before You Touch Anything: The First-Hour Incident Checklist

If something just happened (a ransomware note, a taken-over email account, money that moved), take a breath. This page is the first hour, in plain English. Read the do-not-touch list first, then do the three actions in order.

The most expensive mistakes in a security incident usually happen in the first hour, made by smart people moving fast with good intentions. Wiping the laptop, deleting the weird emails, turning it off and on again: each one can destroy the evidence you'll need for insurance, for regulators, or to find out what actually happened. Here is the first hour, in plain English.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

This page works best on paper. Download the PDF above, print it now, and pin it up where you'd be standing when something goes wrong. An incident is a bad time to depend on the machine that may be the problem.

First, the do-not-touch list

Before anything else, here's what *not* to do, because each of these feels helpful and each one can make things worse:

- **Don't wipe or reinstall anything.** The infected machine is also the evidence. Insurance, investigators, and regulators may all need it as-is.
- **Don't delete the suspicious emails.** They're how you (or someone you hire) will trace what happened and who else got one.
- **Don't power machines off** unless they're actively encrypting files in front of you. Powering off destroys what's in memory; disconnecting from the network usually achieves what you want instead.
- **Don't log into important accounts from a machine you suspect.** If it's compromised, you've just handed over another password.
- **Don't announce anything publicly yet.** What you say early gets quoted later: to customers, insurers, and regulators. Say it once, accurately, when you know more.

The first three actions

1. Disconnect, don't destroy. Take the affected machine off the network: unplug the cable, turn off Wi-Fi. That stops most spread while preserving everything for later.

2. Start a log. A note on your phone is fine: what you noticed, when, what you've done since, each with a time. An honest timeline is worth real money with insurers and saves hours with anyone who helps you. Memory will not do this for you. The first hour blurs fast.

3. Change passwords from a clean device. From a machine you trust (a phone on mobile data counts), change the passwords that matter most (email first, since email resets everything else) and turn on two-step login wherever it's missing.

Who to call, in order

Your IT person or provider, if you have one. Your cyber-insurance carrier's hotline, if you have a policy. Calling early is often a policy requirement, and they'll usually provide a response team. Then, depending on what's involved: your bank (if money moved), and counsel (if personal data may be exposed).

Know which clocks may already be running

Some incidents start regulatory timers the moment you become aware of them. If personal data of people in Europe may be involved, a 72-hour reporting clock may apply. If you sell to bigger customers, your contracts may require notifying them within a set window. You don't need to resolve these in hour one. You need to know they exist, write down when you became aware, and not make them worse.

The honest summary

Disconnect instead of destroying, write everything down, change what matters from a clean device, call the people whose job it is to help, and respect the clocks. That's the first hour. Everything after that goes better because of it.

Where to go from here

This checklist is the first page of a longer playbook. If something is happening right now, the free First 4 Hours triage asks a few questions and returns a priority sequence and a do-not-touch list tailored to your situation, entirely in your browser; your answers never leave your device: sylvanassurance.com/free/first-4-hours/

When you want the rest written down before you need it (hour-by-hour runbooks, communication templates for customers, staff, insurers, and regulators, and the reporting clocks laid out in advance), the First 4 Hours toolkit is that playbook, from $49, one-time, with a 30-day money-back guarantee: sylvanassurance.com/first-4-hours

One conditional pointer: if personal data of people in the European Union may be involved, a separate 72-hour reporting clock can apply under the General Data Protection Regulation (GDPR). The GDPR Breach Response toolkit covers those first 72 hours: sylvanassurance.com/gdpr-breach-response

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-first-4-hours

guarantee security or prevent any particular breach. Responsibility for your business's security remains with you.