First 30 minutes after a security incident

For small teams with no security staff. Print it and keep it by the phone.

Minutes 0 to 5: stop and call

- ☐ **Don't wipe, reinstall or switch anything off.** Leave it as it is for now.
- ☐ **Phone, don't email,** your IT provider and whoever runs the response. If someone is in your email, they can read it. CISA advises out-of-band contact, such as phone calls [1].
- ☐ **Start a written log:** the time, what was noticed, by whom. Add a line for every step after this.

Minutes 5 to 15: contain

- ☐ **Unplug the network cable or turn off Wi-Fi** on any computer that looks affected. Power it down only if you can't disconnect it, since that loses evidence [1].
- ☐ **Many machines affected?** Take the whole network offline at the router or switch [1].
- ☐ **Password typed into a fake page?** Change it now from a different, clean device, and sign that account out everywhere [2][3].
- ☐ **Money may have moved?** Call your bank now and ask for a recall of the funds. The FBI's IC3 says time is of the essence. Then file at ic3.gov [4].

Minutes 15 to 30: get help and decide

- ☐ **Call your cyber insurer's claims line** if you have a policy, before you hire anyone. Note the claim number.
- ☐ **Tell staff only what they need,** in person or by phone: "Don't use X until we say so. Don't open emails about this. Don't post about it."
- ☐ **Keep suspicious emails.** Move them to a folder rather than deleting them.
- ☐ **Report it:** CISA at cisa.gov/report or 1-844-729-2472, and the FBI at ic3.gov [1].
- ☐ **Customer or staff personal data involved?** Talk to a lawyer about notification rules before you tell anyone outside. They vary by state [5].

Don't

- – Pay a ransom or reply to an attacker before talking to your insurer, a lawyer and law enforcement. The U.S. Treasury strongly discourages ransom payments [6].
- – Post about it publicly, or guess at causes in writing.

Sources: [1] CISA, #StopRansomware Guide, cisa.gov/stopransomware/ransomware-guide · [2] Microsoft, Respond to a compromised email account in Microsoft 365, learn.microsoft.com · [3] Google Workspace Admin Help, Identify and secure compromised accounts, support.google.com/a/answer/2984349 · [4] FBI IC3, PSA I-091124-PSA, ic3.gov/PSA/2024/PSA240911 · [5] FTC, Data Breach Response: A Guide for Business, ftc.gov · [6] U.S. Treasury OFAC, ransomware advisory, Sept. 21, 2021. General guidance, not legal or insurance advice. Checked November 16, 2026.

The full **Incident Response Kit** ($29) has step-by-step playbooks for ransomware, a hacked mailbox, a lost laptop and a vendor breach notice, plus a contact sheet and decision log: circuits.fit/services/incident-response-kit.html