

The first response to an IT incident

Help your team act calmly, contact the right people and preserve useful information when something looks wrong.

4 min read | Reviewed 15 October 2026

BEFORE YOU START

Keep the agreed incident contact and escalation route available outside your work account. Your organisation's incident plan takes priority over this general checklist.

01 Stop and contact the response owner

Stop the affected activity. Use a known telephone number or another trusted channel to contact IT promptly. If your work account may be affected, use an alternative agreed channel.

Explain the symptoms, when they started and whether you clicked, entered details or approved a prompt. Describe observations rather than guessing the cause; early reporting helps the responder decide what to do.

02 Contain only within the agreed plan

For a suspected infected device, follow your incident plan or IT instructions about disconnecting its network connection. Do not disconnect shared infrastructure, safety systems or other people's equipment yourself.

Avoid restarting, wiping or running cleanup tools while awaiting instructions because evidence may be lost. If you cannot isolate an actively affected device, seek urgent IT direction on the safest next step.

03 Keep a clear incident record

Record times, the device name, error messages and actions already taken. Preserve originals as IT directs. Do not forward suspicious files broadly or post confidential screenshots into a group chat.

Agree who coordinates business updates and recovery decisions. Refer potential data exposure, insurer requirements and notification decisions to the authorised business lead and appropriate advisers.

Your practical checklist

The first response to an IT incident

- ☐ Affected activity stopped and IT contacted
- ☐ Trusted communication channel used
- ☐ Symptoms and timeline recorded
- ☐ Containment follows the agreed plan
- ☐ Evidence retained without unnecessary sharing
- ☐ Incident owner, reference and next update agreed

Record the next action

Time noticed / affected device or service / symptoms

Contacted person / incident reference / actions taken

Next update time and responsible owner

This is an initial reporting aid, not a forensic or recovery procedure. Where safety is involved, follow the site's emergency arrangements and authorised response team.

OFFICIAL SOURCES & FURTHER READING

CISA and partners: [StopRansomware guide \(2023\)](#)

NIST: [Cybersecurity Framework small business guide](#)

Links open the official source. Web edition: compurep.co.za/guides/incident-first-response