CICADA | RESOURCES

LESSON 04 OF 04 · 8 MIN · ESSENTIAL

When ransomware arrives

The first hour, the mistakes to avoid, and why paying is rarely the end of it.

What it looks like

Files renamed or won't open, a note on the desktop, shared drives unavailable, printers printing demands. Sometimes the first sign is slower: files missing, a strange login, antivirus disabled. Assume it can spread until proven otherwise.

First hour

01 **Disconnect** affected devices from Wi-Fi and the network. Don't power them off.

02 **Tell the incident lead** and the deputy. Record times and actions.

03 **Call the insurer's incident line** before engaging your own forensics, if the policy requires it.

04 **Preserve evidence**: notes, emails, screenshots, devices.

05 **Don't restore yet.** Find out how they got in, or you may restore into an active intrusion.

06 **Report** to the relevant authority and, if personal data is involved, the regulator.

Recovery and payment

Recover from a known-good backup, rebuild where needed, and close the entry point: stolen credentials, exposed remote access, an unpatched service. Change passwords and revoke sessions from a clean device.

Paying funds crime, doesn't guarantee recovery, and may breach insurance conditions or sanctions. Decide with your insurer and a specialist, not under pressure from the note.

DON'T RESTORE BLIND

Restoring before you understand the entry point can give the attacker a fresh, unencrypted copy of your data. Contain, investigate, then recover.

Key takeaways

- ✓ Disconnect, don't power off, and tell the lead.
- ✓ Call the insurer early and preserve evidence.
- ✓ Find the entry point before restoring.
- ✓ Payment is a decision for you, your insurer and specialists.