dacros

A FREE DACROS CARD

The first hour of a cyber incident

A ransom note, a hacked mailbox, money sent to the wrong account, or systems behaving strangely. This card is for the first hour: one person in charge, the damage contained, everything written down, and the right people told. Print it now: in an incident, the computer you would read it on may be the problem.

EDITION
Edition 1 · November 2026

FOR
Whoever would be in charge if something went wrong

ONLINE
dacros.com/resources/cyber-incident-first-hour

One person in charge

- [ ] **One person leads and decides,** and everyone else reports to them. In practice the head of the business normally leads [1].
- [ ] **Set a calm tone.** Do not rush to judgement or to blame: attackers may try to increase the pressure on you [1].
- [ ] **Do not reply to the attacker, pay or agree to anything** before you have taken advice.

Contain it

- [ ] **Decide whether to disconnect or shut down.** Disconnecting a device from the network can stop an attacker issuing commands, limit the spread and keep evidence. Shutting it down may halt activity, but can lose evidence [1]. Ask your IT support first if you can.
- [ ] **For a hacked account,** from a device you trust: change the password, sign out of every device, check the mailbox's forwarding rules and filters, and turn on two-step verification [2].
- [ ] **If money has gone,** tell your bank straight away [2].
- [ ] **If email or chat may be compromised,** talk about the incident by phone or another channel you trust [1].

Write it down

- [ ] **Start a log now:** what was found and when, each decision, who made it and why, and the actions agreed and how far each has got. Use one clock for every time [1].
- [ ] **Keep the evidence.** Do not delete messages, files or logs, even the attacker's.

Check the backups

- [ ] Find out when the last backup was taken, whether it is available, and whether the attacker could have reached it [1]. Do not connect a backup to a device that may be affected.

Tell the right people

- [ ] **Your IT support,** or an NCSC-assured cyber incident response provider [1].
- [ ] **Your insurer,** if you have cyber insurance: check what the policy asks of you, and when [1].
- [ ] **Report it.** In England and Wales, if you have lost money or been hacked through a scam, report it to Report Fraud, online or on 0300 123 2040; in Scotland, to Police Scotland [3]. GOV.UK's service at gov.uk/report-cyber says who else you need to tell [4].
- [ ] **The ICO, if personal data is involved.** If the breach is likely to put people's rights and freedoms at risk, tell the ICO as soon as possible and, where feasible, within 72 hours of becoming aware of it. If the risk to people is high, tell them too, without undue delay [5, 6].
- [ ] **The NCSC.** Reporting to the NCSC brings guidance and support, but it does not meet any legal duty to report elsewhere [1].

Fill this in now

WHO	NAME AND NUMBER
Leads and decides	
Keeps the log	
IT support	
Bank, from the card or statement	
Insurer and policy number	
Solicitor	

Sources

[1] NCSC, Recovering from a highly disruptive cyber attack: 1, Immediate activities, published 28 July 2026, reviewed 1 October 2026, checked 10 November 2026 · ncsc.gov.uk

[2] NCSC, Hacked accounts, checked 10 November 2026 · ncsc.gov.uk/section/respond-recover/hacked-accounts

[3] GOV.UK, Report a scam, phishing or fraud, checked 10 November 2026 · gov.uk/report-suspicious-emails-websites-phishing

[4] GOV.UK, Where to report a cyber incident, checked 10 November 2026 · gov.uk/report-cyber

[5] ICO, Report a personal data breach, updated 28 May 2025, checked 10 November 2026 · ico.org.uk/for-organisations/report-a-breach/personal-data-breach

[6] UK GDPR, Article 33, Notification of a personal data breach, checked 10 November 2026 · legislation.gov.uk/eur/2016/679/article/33