DSPT
Better Security.
Better Care.

Digital
Care Hub

How to spot a cyber attack

Checklist for care staff

A cyber incident happens when someone who should not have access to your IT systems gets access or attempts to get access.

It could be a malicious attack by a hacker who might infect a computer with a virus or block access to information unless a ransom is paid. Or it could be other incidents (such as damage from fire or theft).

As a care provider, you've got very sensitive data about people – so you must keep it safe.

This checklist will help you to consider if a cyber incident might be taking place.

It you think something suspicious is happening, contact your organisation's data protection lead.

They will have a plan in place to manage cyber incidents.

Take a note of who you need to contact on the back of this leaflet and keep this close to hand – maybe on your notice board or beside your computer.

Produced by Better Security, Better Care - the official, free support programme on data protection for adult social care. Find out more about cyber security.

.

digitalcarehub.co.uk/cyber-security

Signs of a cyber incident

Are any of these things happening?
It could be a sign that a cyber incident is taking place.

- Your device is **running unusually slowly**, rebooting by itself, frequently closes programs or apps you are using, or opens those you are not.
- You have **pop-up boxes** from programmes or apps you don't recognise, asking you to do unexpected things.
- You are **locked out** of your IT systems or accounts or are unable to access your documents.
- You receive messages **demanding a ransom** for the release of encrypted or unavailable files.
- Someone you know tells you that they've **received unexpected emails** from you, advertising unlikely products, or perhaps asking for money or other actions that you don't recognise.
- There are logins or **attempted logins** from strange locations or at unusual times.
- There have been **changes to your security settings** that you didn't make.
- Your internet **searches are redirected** to strange sites.
- You receive requests for **unauthorised payments**.

What to do

If any of these things are happening, you should:

1. **Not click on, open or respond** to anything that looks suspicious.
2. Leave your computer or device **switched on.**
3. **Disconnect it from the internet.**
4. **Report it** to the person responsible for data protection within your organisation.

Data protection lead

Who to contact in your organisation

Name	
Email	
Telephone	