Cyber security: what you need to know and do

Department for Education

Your responsibilities

Everyone in your school should understand how and why to:

- recognise threats like phishing and ransomware
- create strong passwords
- only used approved software and services
- follow cyber security policies
- raise any concerns

Make sure you know who needs to be involved in a cyber attack response, and their responsibilities.

There's information on our website about who does what, and how to include that in your plan.

> We followed our crisis management policy, but you need to make sure you know how you would react. For example, if an incident were to occur on Christmas day - what would you do?

-Educational trust chief executive

Scan to visit the hub.

How we can help

The Department for Education cyber security hub has information to help you with everything mentioned here.

Visit our website to find:

- support to help you make sure you're prepared for an attack
- guidance on how to respond to specific incidents
- printable posters to raise cyber security awareness
- recommended schemes and initiatives to increase your security

Facts and figures

6 out of 10 secondary schools had a cyber attack or breach in the past 12 months

fewer than 40% of schools have a cyber incident response plan

under a quarter of schools use multi-factor authentication (MFA) on their supported cloud services - MFA is one of the simplest protections

23% of incidents were caused by poor data protection practices