Cyber security: what you need to know and do

Department for Education

Your responsibilities

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

Everyone in your school should understand how and why to:

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

How the hub can help your school

We have information on how to:

- **increase your security through schemes and initiatives**
- **be prepared for an attack**
- **understand how to respond to specific incidents**
- **raise cyber security awareness in your school**
- **build your cyber response 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?**
>
> - Academy Trust CEO

- fewer than 40% of schools have a cyber incident response plan
- 6 out of 10 secondary schools had a cyber attack or breach in the past 12 months
- under a quarter of schools use multi-factor authentication (MFA) on their supported cloud services
- 23% of incidents were caused by poor data protection practices

Scan to visit the hub

https://cyber-security-hub.education.gov.uk

Sources

Official Statistics, Cyber security breaches survey 2025: education institutions findings (19 June 2025), Secure Schools, "The State of School Cybersecurity 2025", Information Commissioner's Office, "Insider threat of students leading to increasing number of cyber attacks in schools" (11 September 2025)