safe & smart
By EveryChildOnline

Hacking & Cybercrime: Understand the risks. Protect your child.

What parents need to know

Young people are curious. They enjoy solving problems, exploring systems, and learning new skills, especially when it comes to technology. But without proper guidance, this curiosity can sometimes lead them into risky or illegal online behaviour.

Hacking isn't always a dramatic event like in films. It can be something as simple as trying to guess a password, helping someone install a remote access tool, or using a program to bypass restrictions in a game or app. These actions, even if they feel small, can break the law.

What is considered hacking under UK law?

Under the UK's Computer Misuse Act 1990, it is illegal to access or interfere with computers, systems, or data without permission. **That includes:**

- **Logging into someone else's account without their consent**
- **Installing software to monitor, change, or damage a system**
- **Using or sharing tools that can steal information or bypass security**
- **Helping others carry out these actions**

! Even if no harm was intended, it can still be a criminal offence.

Why children and teens might get involved

Most young people don't set out to cause harm. Often, it begins with curiosity or the desire to test their skills. **Common reasons include:**

- **Wanting to understand how systems work**
- **Solving technical challenges or puzzles**
- **Impressing friends or online communities**
- **Learning outside school or formal settings**
- **Being encouraged by others in online forums or group chats**

! Without support, these early actions can lead to serious consequences.

safe & smart
By EveryChildOnline

What could happen if a child crosses the line

The law takes digital crime seriously, even if the person involved is under 18. **Consequences may include:**

- A police investigation and possible court appearance
- Devices being taken away for evidence
- A criminal record
- Expulsion from school or university
- Being banned from certain countries or job roles
- Long-term damage to trust and reputation

! For example, logging into someone's account without permission can lead to up to two years in prison. Damaging or tampering with systems can carry sentences of up to ten years.

What your child can do instead

The good news is that the same technical skills used in hacking can be turned into positive opportunities. Young people who enjoy problem-solving and tech challenges can build fantastic careers in cybersecurity and software development.

Safe and legal ways to build digital skills include:

- Online coding platforms and courses
- School tech clubs and coding competitions
- Ethical hacking challenges like capture-the-flag events
- Bug bounty programmes where people report security flaws and get paid
- Volunteering with our digital inclusion or online safety projects

! With encouragement and guidance, curiosity can become a real strength.

If your child has already crossed a line

If your child has been involved in something they shouldn't have online:

- Ask them to stop straight away and not share the tool or software again
- Don't delete anything without advice, this could make things worse
- Encourage them to speak to a trusted adult or teacher
- Be honest if questioned. Admitting the mistake early can reduce the consequences
- Seek legal advice if needed, especially if police are involved

! Acting quickly and responsibly can help prevent a serious outcome.