Malware and Device infections

safe & smart
By EveryChildOnline

Malware, short for "malicious software", is a common threat to children and teens online. It often hides in games, fake apps, links, or attachments sent through group chats, emails, or social media.

Once it's on the device, it can:

- Spy on your child's activity
- Steal sensitive information
- Cause long-term system damage
- Open the door to more dangerous threats

Signs of infection

- Slow or crashing devices
- Sudden battery drain or increased data usage
- Unrecognised apps or pop-ups
- Passwords not working or unknown logins
- Antivirus has been disabled or removed

How to protect your child

- Talk about safe downloading habits, stick to official stores and trusted websites
- Help them enable automatic updates
- Turn on built-in device protection and antivirus software
- Encourage regular backups of schoolwork, photos, and other important files
- Help them remove unused apps

What to do if malware is suspected

- Disconnect the device from the internet
- Run a full antivirus scan
- Delete suspicious files or apps
- Back up safe data, then factory reset the device if needed
- Change passwords using another clean device

What parents need to know

Online threats don't always knock loudly, sometimes they sneak in through curiosity, shortcuts, or bore-dom. Teach your child that every click is a choice, one that could open a door to danger or help keep it

01268 554074 everychildonline.co.uk