Ransomware: A Real Threat to Your Child's Digital World

safe & smart
By EveryChildOnline

What is ransomware?

Ransomware is a dangerous form of malware that locks a device or encrypts files, then demands payment (often in cryptocurrency) to restore access. Children and teens are increasingly at risk through gaming, social media, or casual browsing.

How it spreads:

- Through phishing emails with malicious attachments
- Hidden in fake game mods, apps, or pirated software
- Exploiting vulnerabilities in outdated devices
- Embedded in sketchy websites

Signs your child may have been hit:

- Their files suddenly won't open
- A full-screen message demands money
- A countdown timer or urgent threat is shown
- They panic, try to hide what happened, or ask for money unexpectedly

How to reduce risk at home:

- Through phishing emails with malicious attachments
- Hidden in fake game mods, apps, or pirated software
- Exploiting vulnerabilities in outdated devices
- Embedded in sketchy websites

Never allow pirated software or cracked games, these are a major source of malware

What to do if ransomware hits:

1. **Do NOT pay the ransom – recovery isn't guaranteed, and it supports criminal activity**
2. **Disconnect the device from the internet immediately**
3. **Scan with trusted antivirus or anti-malware tools**
4. **Try to recover files from a clean backup**
5. **Report it at *Action Fraud* or call *0300 123 2040***

01268 554074 everychildonline.co.uk