

Ransomware

What is ransomware?

Ransomware is a type of malicious software that locks your files or device and demands money to unlock them. The catch? Even if you pay, you might never get your stuff back.

How does ransomware get in?

- A dodgy link in a message or email
- Downloading apps or cracked games from unknown websites
- Using pirated software
- Not updating your apps or device

Signs you've been hit:

- ➔ Your files suddenly have weird names like locked or encrypted
- ➔ A full-screen message appears demanding payment
- ➔ There's a countdown or warning message
- ➔ Your device is frozen

How to avoid it:

1. Back up your files to the cloud or a separate drive
2. Keep your software and apps updated
3. Don't click unless you're 100% sure it's safe
4. Use antivirus software with ransomware protection
5. **Never download pirated games or apps**

Remember

Backing up your stuff and knowing what to avoid can protect you from losing everything.

What to do if it happens:

Do **not** pay – it encourages crime and doesn't guarantee your files back

1. Disconnect from the internet
2. Run antivirus or anti-malware tools
3. Restore from a clean backup
4. Tell a trusted adult or report it

Need help? Visit our resource hub or speak to a trusted adult

