What is a computer virus?

KS3 KS4 Ages 11-16 ⏰ 3 min read

A computer virus is a piece of malicious software — code written with the specific intention of doing something harmful to your computer, your files, or your data. Like a biological virus, it can copy itself and spread to other computers.

How does it work?

A virus hides inside something that looks harmless — an email attachment, a dodgy download, a fake software update. When you open or run it, the virus code executes. Depending on what it's designed to do, it might delete files, encrypt your data and demand ransom, steal your passwords, or use your computer to attack other systems — all while trying to stay hidden.

A virus is like a spy who gets into your house by pretending to be a delivery driver. Once they're inside, they copy your house key, pass a copy to their friends, and help themselves to whatever you've got. The "pretending to be a delivery driver" part is why computer viruses almost always rely on tricking you into running them.

Types of malicious software

Virus — attaches itself to legitimate files and spreads when those files are shared.

Trojan — disguised as useful software. Doesn't spread on its own, but does damage once you've installed it.

Ransomware — encrypts all your files and demands payment for the key to unlock them. Hospitals and schools have been paralysed by these attacks.

Spyware — sits quietly on your device logging what you type, watching what sites you visit, stealing passwords and card details.

Worm — spreads itself automatically across networks without needing you to open anything.

How do you stay safe?

Keep your software updated — most successful attacks exploit old, unpatched security holes. Don't open attachments you weren't expecting. Don't install software from random websites. Use a reputable antivirus programme. And be sceptical: if something seems too urgent or too good to be true, it almost certainly is.