safe & smart
By EveryChildOnline

Social Engineering

What is social engineering?

This is when someone tries to trick you into giving them access to your information or systems. It is not just about stealing money, it is about making you give them control without realising.

How social engineering works

- They pretend to be someone helpful, like tech support
- They tell you your device is infected and ask you to install something
- They drop a USB stick hoping you will plug it in
- They fake job offers or requests to reset login details
- They might even fake voices to sound like your teacher or parent

What to watch out for

- People asking for your passwords or codes
- Someone asking you to download or install something you did not ask for
- Messages that feel too urgent or stressful
- USB sticks you find lying around
- Someone acting like a friend or expert but pushing you to act fast

How to protect yourself

- Double check if someone asks for login info or passwords
- Never install remote access tools unless you started it yourself
- Do not plug in random USB sticks
- Use multi-factor authentication and never share your codes
- If something feels off, ask someone before doing anything

If you believe someone is trying to access your information do the following:

1. Disconnect from the internet
2. Tell a trusted adult or tech support
3. Write down what happened and who contacted you
4. Run a virus scan
5. Change your passwords

Social engineering is about trust. If something does not feel right, slow down and check. It is always better to be safe than sorry.

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