safe & smart
By EveryChildOnline

# Social Engineering: The cybercrime you don't see coming

## What is Social Engineering?

Unlike typical scams, this isn't just about stealing money, it's about convincing your child to give away control of their system or digital accounts. **It's how many major cyberattacks start, with a human mistake.**

## Need help? Visit our resource hub or support services

## Other support services

Childline – *0800 1111* – ***childline.org.uk***
The Mix – ***themix.org.uk***
Ditch the Label – ***ditchthelabel.org***
Report Harmful Content – ***reportharmfulcontent.com***

safe & smart
By EveryChildOnline

## What children are targeted with:

**Fake tech support**
"Your device has malware - click here to fix it..."

**Dropped USB attacks**
Left outside schools, cafés, or libraries. Curious children plug them in.

**Impersonation of teachers, schools, or relatives**
Deepfake voice notes and convincing emails create urgency.

**Job offers or club invites**
Used to get children to install software or hand over login access.

## How to Spot the Signs

- Sudden changes in behaviour around tech
- They mention downloading tools for someone else
- Use of USB sticks from unknown places
- They say someone "helpful" contacted them
- New "friends" asking for remote access or login help

## What to Say to Your Child

- *"Always check before installing anything."*
- *"It's okay to pause and question anything that feels wrong."*
- *"If someone's rushing you or pressuring you, stop and speak to me."*

## How to Spot the Signs

1. **Disconnect from the internet immediately**
2. **Run a virus scan**
3. **Change any passwords stored or used**
4. **Report the issue via Action Fraud or school IT staff**
5. **Be calm, early action matters most**

*"The biggest vulnerability in any system isn't the software, it's trust. Stay curious but stay cautious."*


01268 554074 everychildonline.co.uk