safe & smart
By EveryChildOnline

Phishing scams and your child

Phishing scams are increasingly targeting children and teens, not just adults. These scams come as texts, emails, DMs, or pop-ups and often look like they're from banks, delivery companies, or even their friends.

What to watch out for:

- Messages that trigger panic: "Your account will be blocked unless…"
- Messages asking for login details, money, or personal info
- Links to fake sites that look very real
- DMs from 'friends' asking for help or gift cards

Why young people are vulnerable:

- They're used to clicking quickly
- They want to help if it looks like a friend is in trouble
- They don't always know what phishing looks like
- They may be too embarrassed to ask for help

What parents should do:

Be present online - Ask about messages they receive
Explain how scams work - Even if it seems obvious
Teach them to pause - No one should ever rush to click or pay
Help them secure their accounts - Strong passwords, 2FA
Encourage open conversations - Reassure them they won't be blamed for mistakes

If you think your child has been phished:

1. **Don't panic or shame them**
2. **Help them change passwords and check account activity**
3. **Report the scam via *phishing.gov.uk* or to their app provider**
4. **Contact your bank if any payment was made**

Phishing isn't just an adult issue anymore. Stay alert. Stay involved.

01268 554074 everychildonline.co.uk