

CyberAware UK — Scam Awareness Kit for Schools

Free resource for UK secondary schools. KS3–KS5.

BULLY SAYS

"Scammers don't take holidays — and neither do I. Every student armed with knowledge is one less victim. Share the kit. Spread the word."

Stay sharp. Stay safe.

15 Scams Your Students Need to Know

1. **Phishing** — Fake emails pretending to be your bank, HMRC, or delivery companies
2. **Smishing** — Fake text messages with malicious links (Royal Mail, DPD, Evri)
3. **Vishing** — Phone calls from fake "bank fraud teams" asking you to move money
4. **QR Code Scams** — Fake QR stickers on parking meters and restaurant tables
5. **AI Voice Cloning** — Criminals clone voices from 3 seconds of social media audio
6. **Romance Scams** — Fake profiles on dating apps asking for money
7. **Investment Fraud** — Too-good-to-be-true crypto and stock tips (it's a rug pull)
8. **Shopping Scams** — Fake websites selling items that never arrive
9. **Tech Support Scams** — Pop-ups saying "your computer has a virus" with a phone number
10. **SIM Swap** — Fraudster convinces your mobile provider to transfer your number
11. **CEO Fraud** — Fake email from "the headteacher" asking for urgent payment
12. **Social Media Giveaways** — Fake competitions that steal your personal data
13. **Job Scams** — "Earn £500 a week from home" — it's a money laundering front
14. **Fake Tutor Scams** — Paid tutoring services that take your money and disappear
15. **Exam Board Scams** — Fake emails offering "GCSE grade changes" for a fee

Classroom Discussion Questions

- Why do scammers target young people on social media specifically?
- What makes a phishing email convincing? List three red flags.
- If a friend sent you a message asking for money, how would you verify it's really them?
- Why is "it won't happen to me" a dangerous attitude online?
- What should you do if a classmate shares a "get rich quick" opportunity?

Quiz: Can You Spot the Scam?

Q1: You get a text saying "Your Royal Mail parcel is on hold. Click here to reschedule delivery." What do you do?

Correct: Delete it. Royal Mail doesn't send texts about parcels being on hold.
Click the link to check — it looks official.

Q2: Someone on Instagram offers you £200 a day for "simple data entry work." All you need to do is open a bank account for them. What do you do?

Correct: Report and block. This is money laundering. It's illegal.
Take the job — it seems like easy money.

Q3: You get a call from "your bank's fraud team" saying there's suspicious activity on your account.

They ask for your PIN to verify. What do you do?

Correct: Hang up. Your bank will NEVER ask for your PIN. Call the number on the back of your card. Give them the PIN so they can stop the fraud.

Classroom Poster Ideas

- **"Think Before You Click"** — A poster showing the anatomy of a phishing email with red flags highlighted
- **"The 5-Minute Rule"** — If a message pressures you to act fast, stop for 5 minutes and think
- **"Scammers Wear Masks"** — People online aren't always who they say they are
- **"Your Data Is Worth Gold"** — Why criminals want your name, address, and school details

Teacher's Quick Guide

Suggested lesson plan (45 minutes):

1. **5 min** — Ask: "Has anyone in this room been targeted by a scam?" (most will say yes)
2. **10 min** — Walk through the 15 scams above. Focus on the 5 that affect young people most.
3. **10 min** — Quiz. Students vote on each scenario before revealing the correct answer.
4. **10 min** — Group discussion: "What would you do if..." (pick 2–3 scenarios)
5. **10 min** — Each student writes down ONE thing they'll do differently online from today.

Emergency Contacts

- **Action Fraud** — 0300 123 2040 — Report any scam
- **Crimestoppers** — 0800 555 111 — Anonymous reporting
- **Childline** — 0800 1111 — Support if you've been targeted
- **Your Bank** — Call the number on the back of your card

WE FEAR NO ONE

CyberAware UK — Protecting UK families from scams. Free resources for schools.

cyberawareuk.co.uk/school-kit