// E-SAFETY FACT SHEET

Spot the Phish: Scams Aimed at Young People

The lures, the tells, and what to do when you've already clicked
for Students, Teachers, and Parents

Phishing is the attempt to trick someone into handing over information — a password, a code, a card number — or into clicking something harmful. It is the most common way accounts are stolen, and young people are targeted with lures built specifically for them: free game currency, exclusive drops, giveaway wins, and messages that appear to come from friends.

Phishing does not defeat technology. It defeats attention. Every scam below works by creating urgency so the target acts before they think.

This sheet covers the lures used against young people, a simple checklist for spotting them, what to do after a click, and where to report.

In this document:

1 Know the lures

A. Free Currency, Skins, and Generators

“Free V-Bucks”, “free Robux”, “free primogems”, unlocked skins, rare items — promoted through videos, comments, and DMs. The site asks for a game login to “deliver” the reward, or runs a fake “human verification” step that harvests details. No legitimate platform gives away paid currency through a third-party site. Ever.

B. Messages from Hijacked Friend Accounts

The most effective lure of all, because it arrives from a real friend. Classic openers: *“is this you in this video?”*, *“vote for me in this contest”*, *“can you help me with something quick”*. The link leads to a fake login page. Anyone who enters their details becomes the next account used to spread it. If a message from a friend is oddly worded or unusually urgent, verify through another channel before clicking.

C. Account Suspension and Verification Warnings

A message claims the account will be deleted, has been reported, or must be “verified” within 24 hours. The countdown is the whole trick — panic suppresses checking. Real platforms do not resolve account problems through DMs or links in text messages, and they do not ask for your password or 2FA code.

D. Giveaways, Influencer Impersonation, and Bots

Fake accounts copy a well-known creator’s name and picture, then reply to comments announcing a win. Collecting the “prize” requires a small fee, a card number, a gift-card code, or a login. Look for the near-miss username, the account created last month, and the fact that they messaged first.

E. Marketplace, Ticket, and Trading Scams

Concert tickets, sneakers, consoles, and in-game items sold below market value, with pressure to pay by gift card, crypto, or a friends-and-family transfer — methods chosen precisely because they cannot be reversed. In game-item trading, a “middleman” offers to hold both sides and disappears with everything.

F. School Portals, Homework Help, and Fake Job Offers

Older students get targeted with fake school-login pages, fake scholarship and grant offers, and “easy remote job” messages. Some job scams are money-laundering recruitment: the “job” is receiving and forwarding money, which is a crime even for someone who didn’t know. Legitimate employers never ask a new hire to move funds or buy gift cards.

G. AI Has Removed the Old Tells

Bad spelling and clumsy grammar are no longer reliable warning signs. Generative AI writes fluent, personalised messages at scale, clones voices from a few seconds of audio, and produces convincing fake images and video. Judge the **request**, not the polish: what is this message asking me to do, and why now?

2 What can you do?

The S.T.O.P. check — four questions before you click

S — SENDER	Do I actually know them, and does this look like how they normally write? Is the username a near-miss of a real one?
T — TONE	Am I being rushed, scared, or excited? Urgency is the tool. Real organisations give you time.
O — OFFER	Is something free, exclusive, or too good to be true? Free paid-currency does not exist.
P — PAYLOAD	What is it asking for — a password, a 2FA code, a card, a gift-card number, a download? Any of those is a stop signal.

For students

- **Never enter a password on a page you reached from a link.** Open the app or type the address yourself. This single habit defeats most phishing.
- **Nobody legitimate ever needs your 2FA code.** If someone asks for it — friend, moderator, “support” — the account asking has been taken over.
- Verify odd messages from friends through a **different channel**. Text them, or ask in person.
- Treat requests for **gift-card numbers, crypto, or friends-and-family payments** as automatic scams. Those methods exist because they can’t be undone.
- Don’t download “mods”, cheats, or generators from links — that’s how account-stealing malware arrives.
- Slow down. Nothing legitimate is ruined by waiting ten minutes to check with an adult — and if you did click, tell someone straight away. You’re not in trouble, and speed limits the damage.

For parents & caregivers

- Agree a **family code word** for urgent requests. AI voice cloning makes “it’s me, I need money now” calls convincing; a code word doesn’t care how good the voice is.
- Remove stored cards from app and game stores, and require authentication for every purchase.
- Talk about the scams you receive yourself. Normalising “I nearly fell for this one” makes it safe for a child to admit the same.
- React to a click with problem-solving, not punishment. Fear of losing the device is the main reason young people stay silent.

For teachers & schools

- Run **spot-the-phish exercises** with real examples. Recognition is a trained skill, not a warning to remember.
- Teach students to check where a link actually goes — long-press on mobile, hover on desktop — and to read domains right to left.
- Make sure students know the school will never ask for credentials by email or DM, give them one clear place to report suspicious messages, and frame it as career practice: recognising social engineering is core to analyst and incident responder work.

Practise it free. PhishFinder at gamingforlearning.com trains phishing and social-engineering detection — no login, no download, works on school networks.

→

3 Resources and where to report

If you already clicked or entered details

STEP 01	Change that password immediately from a different, trusted device — and change it anywhere else it was reused.
STEP 02	Turn on 2FA, then sign out all other sessions on the affected account.
STEP 03	Check for changes the attacker made: new recovery emails or phone numbers, mail forwarding rules, connected apps.
STEP 04	If card or bank details were entered, contact the bank now and ask about blocking or reissuing the card. If a file was downloaded, disconnect from the network and run a full security scan before logging back in.
STEP 05	Warn friends — the account will likely have been used to message them — and report it using the links below.

- **Report fraud to the FTC:** reportfraud.ftc.gov · consumer guidance at consumer.ftc.gov
- **FBI Internet Crime Complaint Center (IC3)** — report online crime and financial loss: ic3.gov
- **Forward phishing emails** to the Anti-Phishing Working Group: reportphishing@apwg.org · forward scam texts to 7726 (SPAM)
- **IdentityTheft.gov** — step-by-step federal recovery plans: identitytheft.gov
- **CISA Secure Our World** — plain-language phishing guidance: cisa.gov/secure-our-world
- **In-app reporting** — every major platform lets you report a phishing DM or impersonation account.

If a scam turned into pressure or threats — particularly involving images of a minor — stop replying, don't pay, keep everything, and tell a trusted adult. Report to the NCMEC CyberTipline at report.cybertip.org or call 1-800-843-5678.

// Red flags in any message

- A deadline, countdown, or threat of account deletion
- A link to a login page you didn't go looking for
- Any request for a password, 2FA code, or "verification" code
- Payment by gift card, crypto, or friends-and-family transfer
- Free paid-currency, skins, or "you've won" from an account you don't follow
- A near-miss username, a brand-new account, or a friend messaging in a way that doesn't sound like them

One test covers nearly all of it: **did this arrive uninvited, and does it want me to act fast?** If yes, verify it somewhere else first.