

// E-SAFETY FACT SHEET

Staying Safe While Gaming

Voice chat, strangers, scams, and settings –
what actually goes wrong online
for Students, Teachers, and Parents

Online gaming is one of the best things about being young and online: it is social, creative, competitive, and for a lot of students it is the first place they meet people outside their school. It is also, increasingly, where the risks are — because it combines strangers, voice chat, real money, and an audience of young people, all in one place.

The goal is not to stop young people gaming. It is to make sure they can spot the small number of situations in a game that are not really about the game.

This sheet covers what actually goes wrong in online games, what students, parents, and teachers can do about it, and where to get help.

In this document:

- 01 Know the risks
- 02 What can you do?
- 03 Resources and where to get help

1 Know the risks

A. Talking to Strangers Is the Default

In most multiplayer games, teammates are strangers by design — matchmaking puts young players alongside adults with no age separation, and voice chat opens automatically. Over weeks of playing together, a stranger stops feeling like one. That familiarity is not evidence of safety; it is exactly what someone with bad intentions is building.

B. Grooming Patterns in Games

Offenders use games because they offer trust, privacy, and leverage. The pattern is recognisable: unusual generosity (gifted skins, currency, carrying a player through content), heavy flattery and attention, then a push to move the conversation somewhere more private — a direct message, Discord, Snapchat, or an encrypted app. From there come requests for personal details, photos, or secrecy. **Any request to keep an online friendship hidden from parents is a red flag, without exception.** Gifts are sometimes framed as debts later: *“I spent money on you, so you owe me.”* No young person owes anything for an in-game gift.

C. Account Theft, Trading, and Currency Scams

Game accounts have real value, which makes them targets. Common routes: fake “free currency” generator sites, phishing DMs offering rare items, fake trading middlemen who take both sides, and “let me log in and boost your rank” offers. Downloading cheats or unofficial mods from links is a leading way account-stealing malware reaches a device — the file usually does what it promised *and* steals credentials.

D. Money: Purchases, Loot Boxes, and Pressure

Free-to-play games make money through in-game purchases, and the mechanics are professionally designed to encourage spending: limited-time offers, battle passes, and randomised rewards. Saved payment cards mean large sums can accumulate without an adult noticing until the statement arrives. Social pressure to have current skins adds a real cost that has nothing to do with playing well.

E. Harassment, Toxicity, and Doxxing

Competitive games can be hostile places: abuse over voice chat, targeted pile-ons, exclusion, and stream-sniping. It can escalate to **doxxing** — publishing someone’s real name, school, or address — and in extreme cases to **swatting**, a false emergency call that sends armed police to a real home. Both start with small pieces of leaked personal information.

F. Oversharing Without Realising

Gamertags reused across platforms link accounts together. Streams and clips reveal school uniforms, house interiors, neighbourhood landmarks, and routines. A profile bio with a real name, age, and town gives a stranger everything they need to seem to already know you.

2 What can **you** do?

For students

- ▶ **Keep it in the game.** If someone you only know from a game wants to move to DMs, Discord, or Snapchat, that's the moment to slow down — not because everyone is dangerous, but because that's where the safeguards end.
- ▶ **Nothing personal in your gamertag or bio** — no real name, age, school, or town. Use a different handle from your other accounts.
- ▶ **Secrecy is the red flag.** Anyone who asks you not to tell your parents about them is telling you something important about themselves.
- ▶ **Gifts are not debts.** You never owe photos, information, or anything else for skins or currency.
- ▶ Unique password plus 2FA on every game account — and never share a login, even with a real-life friend or a teammate.
- ▶ No generators, no cheats, no unofficial mods from links. Free currency doesn't exist; malware does.
- ▶ Use mute, block, and report freely. They work, they're instant, and using them isn't overreacting.
- ▶ Watch what's behind you and around you when streaming or sharing clips.
- ▶ If something goes wrong — a scam, a creepy message, a photo you regret — **screenshot it, stop replying, and tell a trusted adult.** You will not be in trouble, and it is never too late.

For parents & caregivers

- ▶ **Know the games.** Ask to be shown what they play and who they play with. Interest earns access; interrogation closes it.
- ▶ Set up **platform family controls** together — every major console and store has them, covering chat, friend requests, spending, and screen time.
- ▶ **Turn off voice chat with strangers** for younger children, or limit chat to confirmed friends.
- ▶ Remove saved payment cards, or require a password for every purchase. Check statements.
- ▶ Keep gaming in shared spaces where possible, and devices out of bedrooms overnight.
- ▶ Ask "who did you play with?" as routinely as you'd ask about school friends. New in-game friends you've never heard of are worth a gentle follow-up.
- ▶ If something has happened, **lead with support.** Confiscating the console is the fastest way to guarantee you never hear about the next thing.

For teachers & schools

- ▶ Include gaming explicitly in e-safety teaching. Students often don't connect "online safety" lessons with the place they actually spend their time.
- ▶ Teach the grooming pattern as a **pattern** — generosity, flattery, privacy, secrecy — rather than a description of a stereotypical stranger.
- ▶ Make reporting routes obvious and low-friction, and treat game-based harassment as seriously as anything happening in a corridor.
- ▶ Follow your school's safeguarding and mandatory-reporting procedures for any disclosure. When in doubt, escalate.

Career link. Anti-cheat, account security, and platform trust & safety are real cybersecurity jobs — the people who catch scammers and protect players do this professionally. Explore the roles at getintocyberjobs.com and practise the skills free at gamingforlearning.com.

3 Resources and where to get help

If a stranger in a game has crossed a line

STEP 01	Stop replying. Don't negotiate, don't threaten, don't pay. Engagement is what the situation runs on.
STEP 02	Keep the evidence. Screenshot messages, usernames, and profiles before blocking — blocking can hide the history.
STEP 03	Block and report in-platform, on every service where the contact happened.
STEP 04	Tell a trusted adult. A young person who sent something they regret is a victim, not a wrongdoer, and needs support rather than blame.
STEP 05	Report it. NCMEC CyberTipline: report.cybertip.org or 1-800-843-5678. If there is immediate danger, call 911.

- ▶ **NCMEC CyberTipline** — report online exploitation of a child; reports are reviewed and routed to law enforcement: report.cybertip.org
- ▶ **24-hour hotline** for children and families: 1-800-THE-LOST (1-800-843-5678)
- ▶ **Take It Down** — helps minors anonymously request removal of explicit images of themselves: takeitdown.ncmec.org
- ▶ **ESRB** — game age ratings and content descriptors, plus parental-control setup guides for every major platform: esrb.org
- ▶ **Common Sense Media** — independent reviews of games and apps by age: commonsensemedia.org
- ▶ **FTC** — report scams and unauthorised charges: reportfraud.ftc.gov
- ▶ **988 Suicide & Crisis Lifeline** — free, confidential support 24/7: call or text [988](https://988lifeline.org)

// Warning signs to watch for

- ▶ A new online “friend” no one has met, especially an older or unusually generous one
- ▶ Unexplained skins, currency, gift cards, or in-game items
- ▶ Secrecy about who they play with, or switching screens when adults approach
- ▶ Distress, anger, or withdrawal after playing
- ▶ Moving conversations off the game to private or disappearing-message apps
- ▶ Unexpected charges, or a game account that suddenly won't log in
- ▶ Reluctance to play a game they previously loved

Changes in behaviour can have many causes. Whatever the reason, check in on red flags — and make gaming a normal part of the ‘check-in’ conversation, not a separate interrogation.

getintocyberjobs.com · A free resource for K-12 students and teachers across the US.

This fact sheet is for general educational purposes and does not replace your school's safeguarding or mandatory-reporting procedures. If a child is in immediate danger, call 911. To report online exploitation of a child, contact the NCMEC CyberTipline at report.cybertip.org or 1-800-843-5678.