Be scam smart

Protecting neurodivergent children from scams in online games

Contents

Learn about scams your child might come across in the games they play online and how you can prevent them from coming to harm.

Neurodivergent children are at greater risk of scams

Research shows that neurodivergent children typically spend more time playing online games than their neurotypical counterparts.

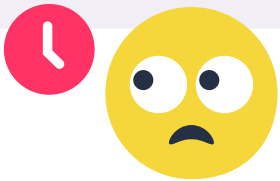
Coupled with other risk factors such as communication differences and increased impulse or hyperfocus behaviours, neurodivergent children are often at greater risk of becoming victims of scams.

Risk factors

Increased screen time

Many neurodivergent children can become deeply absorbed in activities they enjoy, such as online games. This focus can result in them not noticing how much time has passed. While being immersed in a game can be positive, spending longer on a platform also increases the chances of encountering scams.

Tip: Explore video game and console screen time controls to help manage this.



Communication differences

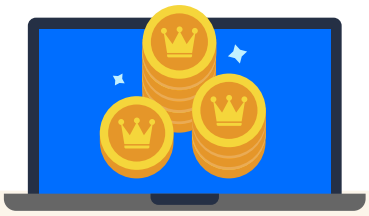
Some neurodivergent young people can be naturally open and trusting, which can be a real strength in many contexts. However, this can sometimes make them more vulnerable to people online who may not have good intentions. For example, if a young person takes what others say at face value or assumes honesty, they may be more at risk of being targeted by scammers.

Tip: Talk regularly about what positive and harmful behaviour looks like.

Spontaneity and quick decisions

Young people who act with spontaneity often bring energy, creativity and fresh ideas. Online, though, this can also mean they might agree to a trade or make a choice without pausing to consider the possible risks.

Tip: Create a Stop-Think-Act routine to help your child think before acting online.



Preference for concrete concepts

For those who connect most easily with hands-on, tangible experiences, digital items and virtual currency can feel less clear. Because these can't be physically touched or seen, it may be harder for neurodivergent young people to recognise how actions in online spaces can have real-world effects.

Tip: Try to compare items and experiences online to similar items or experiences offline.

Types of scams in online games

Not every scam in an online game is financial, especially if your child doesn't have access to money. Explore a range of scams below to familiarise yourself with potential risks.

Trust trades

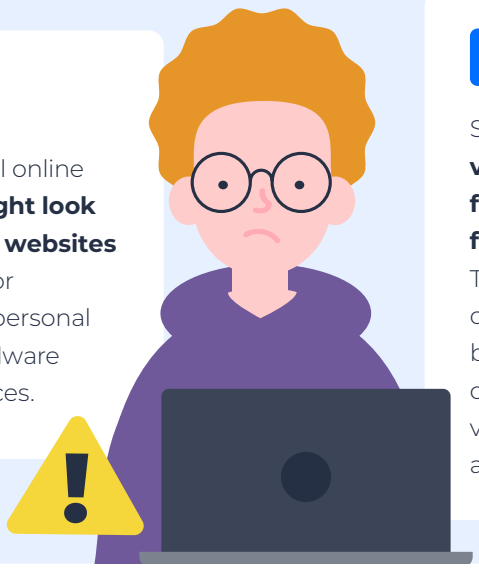
In a trust trade scam, **the scammer first builds a sense of friendship or reliability** before persuading someone to hand over valuable items. Children who are eager to connect with others, who may be more isolated or have a smaller friendship network, or who naturally take people at their word, can be particularly at risk of this type of scam.

Fake giveaways

These scams target children's accounts. **By promising free in-game currency, rare items or other prizes,** they can get children to share their login details or other personal information.

Phishing

A common scam across all online spaces, **in games this might look like sharing fake links or websites** claiming to offer rewards or benefits. This can lead to personal details being stolen or malware and viruses infecting devices.



Account takeovers

Similar to trust trade scams, **victims first develop a friendship or some other form of trust with the scammer.** The scammer then claims they can help them get a certain item, beat a level, get free in-game currency or something else. The victim shares their login details and ends up losing their account.

5 tips to protect your child from scams in games

Popular games that children play have community standards that every user must follow. These rules generally do not permit behaviours related to scamming.

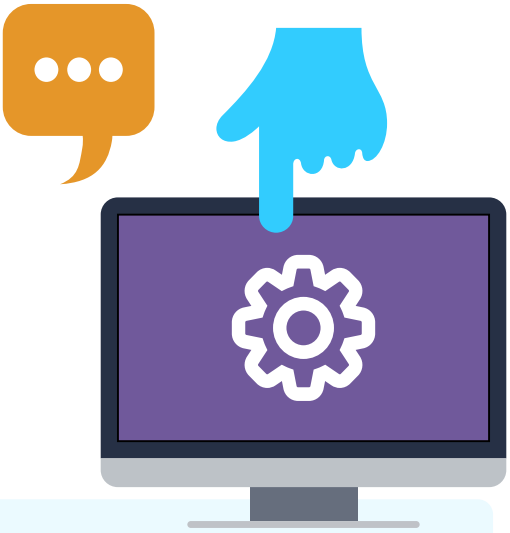
The platform will work to suspend or remove any user who breaks these rules. However, this doesn't mean your child won't come across fraudsters in their games. So, it's important to take active steps to keep them safe.

1 Review blocking and reporting tools

With your child, find where the blocking and reporting tools are. Do this outside of a game such as when reviewing their Friends list as well as during a game, so they know where to find those tools if they need them.

2 Talk about when to use those tools

Focus on the situations they could find themselves in such as a good friend they've made asking to trade a rare item or gain access to their account. **Remind them that it's better for them to use the tools too much than not at all,** and that the people they block or report won't know they've done it.



3 Use built-in parental controls

Popular games and platforms have built-in parental controls that you can use to restrict who your child can talk to. **Make sure you clearly explain the reasons for using these controls, especially with older children.** You can also encourage them to use similar safety tools on their own account by showing them how.

4

Agree on clear boundaries

As a family, create a set of rules when it comes to communicating with others and managing money in online games. This could include who they can add as a Friend, what kinds of games they can play and the steps they need to take when trading or buying an item such as telling you first.

Write the boundaries and display them in your home to serve as a repeated reminder. You can even review them before your child starts a session in their favourite game to help them remember the actions they should take.

5

Talk about their experiences

Create a routine around talking to your child about their experiences within their game. This could be daily, a couple times per week or some other schedule that works for your family. **Ask them what games they're playing, what they like about them, who they play them with,** if they've blocked or reported anyone and if they dealt with anything scary or confusing.

Use these regular chats as an opportunity to remind them of how and when to use reporting tools, what safe communication looks like and what steps they should take to stay safe, based on the boundaries you created together.

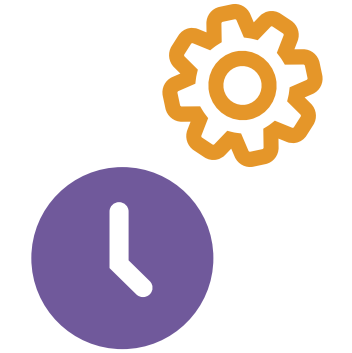
Regular check-ins can help you stay on top of potential risks and reinforce your child's attention to their safety online.

Extra steps for securing accounts

Many neurodivergent children understand online security basics but might require support when it comes to managing the practical steps to stay safe, such as remembering multiple logins or completing multi-step processes.

Turning these into simple routines and practising together can make online safety feel easier and more manageable.

- **Encourage strong, unique passwords** for each gaming account. A family password manager can take the pressure off remembering them all.
- **Switch on two-step verification** or multi-factor authentication wherever possible. Practise logging in together a few times so it becomes familiar.
- Remind children **never to share login details**, even with friends. Agreeing on a safe phrase can give them confidence to say "no."
- **Check that recovery emails** and phone numbers are up to date, so you can quickly get back into accounts if needed. Get more tips with our guide

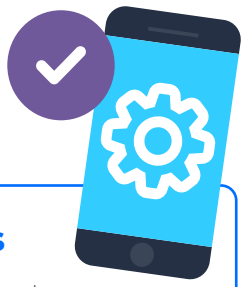


Advice for families new to online gaming

Starting with the right routines can reduce risk and anxiety later.

- **Set up accounts together.** Walk through privacy settings, parental controls and passwords step by step.
- **Play alongside your child** at first so you both understand how the platform works.
- **Review safety tools** before they face problems - prevention is easier than repair.
- **Establish spending rules early.** Visual reminders or written agreements work especially well for neurodivergent children.
- **Keep routines consistent.** Neurodivergent children may find changes stressful, so reviewing safety steps before each play session can help.

Quick checklist: Protecting your child from scams in games



Set up safely

- [ ] Create accounts together.
- [ ] Use strong, unique passwords.
- [ ] Turn on two-step verification.
- [ ] Check privacy and parental control settings.
- [ ] Practise account logins together until familiar.

Agree on boundaries

- [ ] Write down family rules (friends, trades, spending).
- [ ] Display rules somewhere visible.
- [ ] Use visual reminders (posters, contracts, checklists).
- [ ] Stick to consistent routines before and after gaming.

Practise using safety tools

- [ ] Show how to block and report users.
- [ ] Role-play common scam situations.
- [ ] Reassure them blocking/reporting is safe.
- [ ] Repeat safety steps regularly to build confidence.

Keep communication open

- [ ] Schedule regular check-ins (daily or weekly).
- [ ] Ask: What game did you play? Who with? Did anything feel confusing or worrying?
- [ ] Provide simple scripts they can use:
  - "I don't share my password."
  - "I'll ask my parent first."

Tips to protect children from scams on Roblox

- **Familiarise yourself with Roblox's Community Standards:** Learn what kind of behaviour around cheating and scams isn't allowed on the Roblox platform to better understand what should be reported. Visit the Community Standards here.
- **Create a parent account:** This lets you set parental controls on your child's account to manage who they interact with, which can prevent strangers from contacting your child to try and scam them. See Roblox's parent's guide here.
- **Show children where to block and report:** With your child, explore how they can block and report users or experiences that might be trying to scam them or others. Find step-by-step guidance here.
- **Review your child's Connections:** Check who is on your child's Connections list and set boundaries around them adding new people. This can help you prevent strangers from gaining Connections-level access to your child.

internet matters.org

Supported by:

ROBLOX