

Helping children recognize fake giveaways and online scams



Why fake giveaways appeal to children

Fake giveaways work because they borrow the language of legitimate rewards. A child might see a message promising free game currency, a new phone, a gift card, concert tickets, or exclusive merchandise. The message may appear in a game chat, a short video comment, a direct message, a pop-up, or an email that looks official. To an adult, the offer may look obviously unrealistic. To a child, it may feel like a lucky opportunity that could disappear if they wait.

This vulnerability is developmental, not a character flaw. Children and adolescents are still building inhibitory control, future-oriented thinking, and social risk assessment. Dopamine-driven reward anticipation can make a bright, urgent offer feel compelling before the child has time to evaluate it. Scammers exploit that normal neurodevelopment by adding countdown timers, fake winner lists, celebrity images, or messages that say only a few people have been selected.

Supportive teaching starts by separating the child from the scam. Instead of saying, "You should have known," try, "That message was designed to trick people quickly. Let's slow it down together." This preserves trust and helps the child's prefrontal "pause and evaluate" skills strengthen over time.

Red flags children can practice spotting

Children learn best when warning signs are concrete and repeated in everyday language. A useful family phrase is: "Real prizes do not need secrets, pressure, or unsafe information." This gives children a simple mental screen before they click.

Too good to be true: The offer promises expensive prizes, free in-game currency, or rare items for almost no effort.

Urgency: The message says the child must act immediately, before a timer runs out, or before a parent can check.

Unknown contact: The sender is someone the child does not know, a look-alike account, or a person claiming to represent a brand, creator, or game.

Suspicious links: The link looks misspelled, shortened, odd, or different from the usual official website or app store.

Requests for money: The message asks for a "small fee," gift card code, shipping charge, deposit, or payment to unlock the prize.

Requests for personal details: The form asks for a full name, address, school, phone number, passwords, account recovery codes, or images.

Downloads: The prize requires installing an unknown app, file, browser extension, or game modification.

Role-play can help. Show children example scenarios and ask, "What feels exciting here? What feels suspicious?" Naming both the attraction and the warning sign teaches emotional literacy and digital literacy for children at the same time.

Personal information, payments, and downloads

Children may not understand why a scammer wants information that seems ordinary. Explain that small pieces of data can be combined. A name, school, location, birthday, username, and photo can become a digital profile.

Protecting children's personal information online is partly about preventing account takeover, identity misuse, targeted grooming, bullying, and financial harm.

Payment requests deserve special attention. Some scams ask for gift card codes

because they are difficult to reverse. Others ask for a parent's card details, a game platform login, or access to a digital wallet. Children should know that winning a real prize should not require paying first, sharing a password, or sending a code from a text message. A one-time passcode is like a temporary key; if someone asks for it, the safest answer is no.

Downloads are another risk. A fake prize may install malware, spyware, or a browser extension that captures information. Use child-friendly language: "Some files pretend to be presents but behave like tiny spies or locks inside the device." Keep the tone calm. The goal is not to create hypervigilance, but to build a practical association: unknown download plus reward promise equals ask an adult first.

A check-first routine that preserves trust

A check-first rule works best when it is predictable and shame-free. Children should know exactly when to pause: before entering personal details, clicking a prize link, downloading a file, joining a private chat to claim a reward, sending a code, or using family payment information. Frame this as a safety routine, not a punishment.

For younger children, the rule can be simple: "If the internet offers you a prize, ask first." For older children and teens, involve them in the reasoning: "Scammers use urgency because they do not want your thinking brain to catch up." This respects their growing autonomy while still setting a clear boundary.

Families can also use practical safeguards. Keep privacy settings tight, limit who can contact the child, review in-app purchase controls, and use parental controls where appropriate. These tools support online safety for children, but they do not replace conversation. Children still need to practice recognizing manipulation, especially when scams arrive through friends, chats, or social platforms that filters may not catch.

It also helps to connect this topic with online stranger safety. A scammer may seem friendly, flattering, or familiar. Teach children that kindness from an unknown person does not create an obligation to reply, prove themselves, keep a secret, or move to a private chat.

What to do after a click or message

If a child clicks a suspicious link or shares information, respond quickly and calmly. The first adult reaction becomes part of the child's learning. Panic, blame, or confiscating the device as the only response may make the child hide the next incident. A better opening is, "Thank you for telling me. We can fix many things faster when we know early."

Next, gather facts without interrogating. Ask what was clicked, what information was entered, whether anything was downloaded, whether money or codes were shared, and whether the child is still receiving messages. Take screenshots if possible, but do not ask the child to keep interacting with the scammer. Report or block the account through the platform, game, or app.

Change affected passwords from a clean device, enable multifactor authentication when available, and check for unusual account activity. If payment information, gift card codes, or banking details were shared, contact the relevant financial institution or payment provider. If a device may have downloaded malware, run trusted security tools or seek technical help.

When the incident involves threats, sexual coercion, requests for images, persistent contact, or fear for the child's safety, escalate promptly to appropriate platform reporting systems, local authorities, child protection resources, or professional guidance. If the child develops marked anxiety, insomnia, appetite changes, headaches, abdominal pain, avoidance, panic symptoms, or self-harm thoughts after the incident, consult a pediatrician, child psychologist, or other qualified healthcare professional.

Emotional safety and child wellbeing

Scams often create shame. A child may think, "I was stupid," "I caused trouble," or "My parent will be angry." Shame increases secrecy, while connection increases disclosure. Tell children directly that many intelligent adults are tricked by scams too. The scam is the problem; the child's honesty is the protective factor.

Some children need extra support because of developmental stage, impulsivity, anxiety, social vulnerability, neurodivergence, learning differences, or a

strong wish to belong. Scams may also use coercive peer pressure: "Everyone is doing it," "Don't tell your parents," or "You'll miss out if you don't join now." These dynamics can be especially powerful for tweens and teens whose peer approval systems are highly active.

After an incident, watch for changes in sleep, mood, concentration, school avoidance, irritability, or somatic symptoms such as stomachaches and headaches. These signs do not automatically mean a psychiatric disorder is present, but they suggest the child's nervous system may be under stress. Gentle routines, device boundaries before bed, reassurance, and problem-solving can help. If distress is persistent, severe, or associated with safety concerns, healthcare professionals can assess the child's needs and recommend evidence-informed support.

Digital resilience grows through repeated, low-shame practice. Review examples together, praise pauses as much as correct answers, and keep the door open: "If something online ever feels weird, exciting, scary, or secret, you can bring it to me."