

Teaching children how to respond to unexpected phone calls or messages



Why unexpected contact can be difficult for children

Children are still developing executive functions such as inhibitory control, risk assessment, and delayed gratification. A message that promises a reward, claims that an account will be closed, or says that a loved one is in trouble can overwhelm these skills. Adolescents may also feel pressure to respond quickly because of peer expectations, social media norms, or fear of missing out.

Some children have additional communication or learning needs, limited literacy, attention difficulties, or heightened anxiety. They may interpret language literally, have trouble identifying an implied threat, or find it difficult to explain what happened afterward. This is not a failure of judgment or character. It means the safety plan should use clear language, visual reminders, repetition, and role-play.

Begin with reassurance: unexpected contact is not the child's fault, and they will not be punished for seeking help. Explain that adults can make mistakes too, so the rule is not to identify a bad person; it is to use a safe process whenever contact is unexpected or asks for something unusual.

Teach the pause, protect, check, and tell routine

A short sequence is easier to remember than a long list of rules. Practise four steps: pause, protect, check, and tell.

Pause: Do not answer, reply, click, download, forward, or call back simply because the sender requests immediate action. Put the device down and take a breath.

Protect: Do not share a full name, address, school, location, schedule, passwords, verification codes, financial information, photographs, or information about another person. Do not send money or allow remote access to a device.

Check: Show the contact to a parent, caregiver, teacher, or another trusted adult. If the message claims to be from a bank, school, delivery service, relative, or friend, verify it through a known phone number or an established app rather than using details supplied in the unexpected message.

Tell: Report what happened, even if the child already replied or clicked something. Early disclosure allows an adult to change passwords, contact the relevant organization, preserve evidence, or seek further help.

Use concrete reminders such as, "Urgency is a reason to slow down." A legitimate contact can usually tolerate a pause while the child checks with an adult. Children should understand that blocking or reporting is appropriate after an adult has helped assess the situation.

Give children practical words for phone calls

Children do not need to debate with an unfamiliar caller. A brief, nonrevealing response is safer than answering questions to be polite. Teach them not to confirm that they are home alone, identify family members, describe routines, or disclose where they are.

"I cannot help with that. Please speak to my parent or caregiver."

"The person you are calling is not available. I cannot give out information."

"I do not take messages from people I do not know. Goodbye."

"I need to check with an adult before I answer."

If a child answers a landline or a device shared by the household, they can

write down the caller's name, organization, telephone number, and reason for calling without promising a return call. They should not be persuaded to keep the call secret or move to another communication platform. If the caller becomes threatening, sexualized, manipulative, or frightening, the child can hang up immediately and tell a trusted adult.

Role-play should include ordinary mistakes, such as a wrong number, as well as higher-risk scenarios. Praise the child for ending the call and seeking help rather than focusing on whether they used perfect wording. A child who is non-speaking or uses assistive communication can have a preprogrammed message, visual card, or agreed button sequence for "I need an adult."

Give children practical words for texts and direct messages

Messages can look convincing because scammers or unknown contacts copy logos, names, writing styles, and familiar profile images. Explain that a displayed name is not proof of identity. A compromised account may send an unusual request even when the contact appears to be a friend or relative.

Teach children to look for warning signals: an urgent demand, a request for secrecy, an offer that seems unusually attractive, pressure to move the conversation elsewhere, threats of punishment, requests for intimate images, or demands for passwords, payment, gift cards, or security codes. One warning signal is enough to stop and ask for help; children do not need to prove that a message is fraudulent.

They should not click links, open attachments, scan unfamiliar codes, download files, or reply with personal or financial information. Instead, they can take a screenshot if safe to do so, leave the conversation, and show the original message to an adult. Do not encourage a child to "test" the sender, confront them, or continue chatting to collect evidence.

If a child has already shared information, reassure them that disclosure is the correct next step. The adult can help secure accounts, contact a service provider, report the message, and consider whether additional support is needed. Preserve relevant messages rather than deleting them immediately, unless retaining them could further endanger the child.

Build device settings and family routines around the skill

Teaching is more effective when the technology supports the rule. Review privacy settings together and use age-appropriate parental controls, spam filtering, contact restrictions, and blocking or reporting functions. The exact options vary by device, operating system, messaging service, and local law, so caregivers should check current manufacturer or service guidance.

Agree on which contacts are expected, how a child can identify approved adults, and where suspicious messages should be shown. A family code word can help verify an unusual request involving travel, collection from school, money, or an urgent change of plan. The code word should be shared only with the child's trusted adults and changed if confidentiality is lost.

Establish a no-blame reporting routine. For example, the child can place the phone in a designated location or say a neutral phrase such as, "I need a safety check." Adults should respond first with calm questions: "What happened?" "What did the person ask you to do?" and "What information, if any, was shared?" Avoid shaming, sudden interrogation, or removing the phone as an automatic response, because fear of losing access can discourage future disclosure.

Revisit the plan periodically. New apps, school transitions, travel, family separation, and changes in independence can create new situations. Include age-appropriate child personal safety skills and broader online boundaries rather than treating phone safety as a one-time lesson.

Practise without creating unnecessary fear

Short, predictable practice sessions are usually more useful than frightening stories. Begin by telling the child exactly what will happen: an adult will pretend to send a message, the child will practise pausing, and no real account will be contacted. Use several examples so the child learns the principle rather than memorizing one visual pattern.

Start with low-stakes situations, such as a wrong number or a message asking for a link to be opened. Progress to an apparent friend asking for secrecy, a caller asking whether the child is alone, or a message claiming that a package

or account needs immediate attention. After each rehearsal, ask what clues they noticed and which trusted adult they would contact.

Keep the language developmentally appropriate. Younger children may need a picture-based flowchart, while older children can discuss impersonation, privacy settings, account security, and social engineering. Neurodivergent children may benefit from explicit scripts, predictable alternatives, and extra processing time. Do not use real threats, impersonate a frightening person, or repeatedly test the child without consent.

Connect the routine with Teaching kids emergency response so the child knows that an unexpected communication about immediate danger is handled differently from an ordinary suspicious message. In a genuine emergency, the child should follow the household and local emergency plan, contact emergency services when appropriate, and involve a nearby trusted adult.

What to do when a contact is concerning

Respond promptly and calmly if a child receives repeated unwanted contact, sexual content, threats, extortion, requests for intimate images, attempts to arrange an in-person meeting, or messages suggesting self-harm or harm to someone else. Move the child to a safe adult-supervised setting and avoid replying to the sender. If there is an immediate risk of physical harm, contact local emergency services or the relevant safeguarding authority.

Document the date, time, platform, sender information, and what was requested when doing so is safe. Save screenshots or messages in a secure location, but do not forward sexual images of a minor. Reporting pathways may include the platform, school safeguarding staff, a telecommunications provider, law enforcement, or a child-protection service, depending on the circumstances and jurisdiction.

Monitor the child's emotional state without assuming a diagnosis. Sleep disruption, avoidance, somatic complaints, changes in school participation, or persistent fear may warrant discussion with a pediatrician or qualified mental health professional. A clinician can help assess distress and recommend appropriate support; caregivers should not attempt to diagnose or treat the child based on one incident.

Most importantly, reinforce that the child did the right thing by telling someone. Safety is strengthened when children know that adults will help them solve the problem, even when a mistake has already occurred.