What to do when a child clicks a suspicious link

Start with calm and stop further action

The first few minutes matter, but they do not need to be perfect. Sit beside the child, lower the emotional temperature, and say something simple such as, I am glad you told me; we can handle this together. Children often hide online mistakes when they expect punishment, and secrecy gives scammers more time to extract passwords, money, images, or personal details.

Ask the child not to click anything else, reply, call a number shown on the screen, install an app, scan a code, or type any more information. If a page is open, close the tab or app. If pop-ups keep appearing, disconnect the device from Wi-Fi or mobile data and restart it. If the suspicious link opened inside a game, social media app, or messaging platform, stop using that app until you have reviewed the account.

Ask what happened in chronological order.
Identify whether the child entered a password, code, address, school name, payment information, or photo.
Keep the original message if it is safe to do so.
Do not shame the child for being curious or trusting.

A calm pause also models digital triage: stop, think, check, and involve a trusted adult before the situation escalates.

Secure the device without erasing useful clues

A suspicious link may lead only to a fake login page, but it can also trigger unwanted downloads, browser notifications, malicious extensions, or ransomware attempts. Before deleting everything, take a quick screenshot or note the sender, platform, date, visible web address, and what the child remembers clicking. This information may help a school, bank, platform safety team, or cybercrime reporting service.

Next, close the page or app. If the browser or app freezes, restart the device. Avoid approving new downloads, permission requests, calendar subscriptions, device management profiles, or security warnings that pressure immediate action. On a phone or tablet, check recently installed apps and remove anything the child does not recognize or that appeared immediately after the click. On a computer, run reputable security software and make sure the operating system, browser, and antivirus definitions are updated.

Also review browser settings. Remove unfamiliar extensions, clear suspicious site permissions, and turn off notifications from unknown websites. If ransomware messages appear, files become inaccessible, or the screen demands payment, do not pay quickly or negotiate through the message. Disconnect the device from the network and contact a qualified IT professional, the device manufacturer support channel, or an appropriate cyber incident service. Backups are valuable here, but restoring from backup should be done carefully so that compromised files or settings are not simply reintroduced.

Protect accounts, identity, and payment information

The next priority is deciding what information may have been exposed. If the child typed a username and password, change that password from a clean, trusted device, not from the possibly affected device until it has been checked. If the same password was reused elsewhere, change it on every account where it appears. A password manager can help families create unique, strong passwords without expecting children to memorize complex strings.

Turn on multi-factor authentication for email, school portals, gaming accounts, social media, cloud storage, and payment-linked services. Explain to the child that a verification code is like a house key: even if someone sounds friendly, urgent, or official, the code should not be shared. Review account recovery email addresses, phone numbers, and logged-in devices. Sign out of unknown sessions and revoke access for unfamiliar apps or connected services.

If payment information, gift card numbers, banking details, government identification, or a home address may have been submitted, contact the relevant institution promptly. Ask about monitoring, card replacement, transaction disputes, or identity-protection steps. For a child account, check privacy settings for child accounts, friend lists, direct messaging permissions, public profile information, and location sharing. If the suspicious link came through a known friend's account, that friend may be compromised too; notify their caregiver or the school without blaming either child.

Support the child emotionally and assess wellbeing

A phishing incident is not only a technical event. Children may feel embarrassed, frightened, or responsible for family stress. Some scammers deliberately use coercive language, secrecy, countdown timers, fake authority, or threats. In younger children, stress may show as clinginess, irritability, sleep disturbance, headaches, abdominal pain, avoidance of devices, or sudden fear of school or friends. Older children may minimize the incident because they worry about losing access to a game, phone, or social group.

Use developmentally appropriate internet safety language. For a younger child, say that some online messages pretend to be safe but are trying to trick people. For an older child, discuss phishing, social engineering, credential theft, ransomware, and impersonation. Keep the conversation brief at first, then return to it later when everyone is calmer.

If the message involved sexual content, requests for images, blackmail, stalking, self-harm threats, or pressure to keep secrets, treat it as a safeguarding concern, not ordinary mischief. Preserve evidence, stop contact, and involve appropriate adults or authorities. If the child appears acutely distressed, expresses self-harm thoughts, cannot sleep, has panic symptoms, or develops persistent somatic complaints, consult a pediatrician, mental health

professional, or emergency service according to the level of risk. Do not try to manage serious psychological distress alone.

Report the incident and involve the right adults

Reporting can reduce harm for your child and for other children who may receive the same message. The right route depends on where the link appeared and what happened afterward. Report suspicious emails to the email provider, suspicious messages to the platform, and school-related messages to the school or district technology team. If a school account, learning platform, or shared device was involved, the school may need to reset credentials or warn other families.

If money was lost, a payment card was used, or identity information was disclosed, contact the financial institution and relevant fraud-reporting channel. If the message included threats, grooming, sexual exploitation, extortion, or instructions to meet offline, contact local child protection or law enforcement resources. For immediate danger, call emergency services.

When documenting the incident, keep the original message, sender profile, web address, screenshots, time stamps, transaction records, and any usernames involved. Avoid repeatedly interviewing the child in a way that feels like an interrogation. Instead, write down what they volunteer, ask a few neutral clarifying questions, and let trained safeguarding or law enforcement professionals handle more serious investigations. A trusted-adult network is especially useful: parents, caregivers, teachers, school counselors, healthcare professionals, and technology staff each have different roles in keeping the child safe.

Build prevention into everyday family routines

After the urgent steps are complete, turn the incident into skill-building. The goal is not to make children afraid of the internet; it is to make help-seeking automatic. Teach a family check-first rule for children: before opening unexpected links or attachments, downloading files, scanning codes, entering passwords, or sharing verification codes, pause and ask a trusted adult. This rule works best when adults respond calmly every time.

Review common warning signs together. Suspicious messages often create urgency,

offer prizes, threaten account closure, ask for secrecy, contain odd grammar, come from unknown senders, imitate a familiar brand, or send the child to a login page that does not quite look right. Help the child ask, Does this message make sense? Was I expecting it? Is it trying to rush me? Would this person or company normally ask for this information?

Set up practical barriers. Keep devices updated, use security software, back up important files, limit public profile information, and make social or gaming accounts private when appropriate. For younger children, keep app downloads and purchases behind caregiver approval. For older children, involve them in the settings so they understand the reason rather than experiencing safety tools as secret surveillance.

Finally, rehearse one simple script: I clicked something weird, and I need help. If the child can say that without fear, your family has built one of the strongest protections available. Online safety for children depends less on perfect behavior and more on quick disclosure, steady adult support, and repeated practice with realistic online safety threats.