beware of common scams targeting kids and teens online

Today, kids and teens organize many aspects of their lives online, using the internet for school, entertainment, and social interactions. Scammers are finding new and increasingly deceptive ways to exploit their innocence and take advantage of them — and their parents — financially.

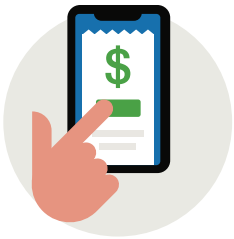
Kids use the internet much differently than adults do, and the schemes directed at them reflect that. Let's look at some of the most common ways kids are scammed and defrauded online.

18,000

Reported number of online scams targeting people younger than age 20 in 2023.[1]

$40.7M

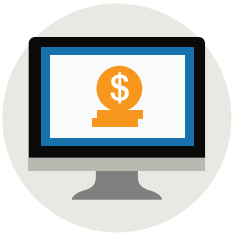
Amount of losses due to online scams targeting people younger than age 20 in 2023.[1]



Shopping and finance scams

Fake online stores
Fraudsters create fake websites that appear to sell popular items at discounted prices. When kids attempt to make a purchase, their payment information is stolen.

Financial aid
Fraudsters may trick teenagers into applying for fake scholarships or financial aid, and then ask them to provide personal information or payment before receiving the aid.



Game and quiz scams

Fake online stores
Scammers entice kids with promises of free in-game currency, gadgets, or other desirable items. Kids may be asked to pay a fee to enter a contest, or to provide personal information or download harmful software to claim a prize.

Quizzes
Hackers use online quizzes to gather information such as birthdays, pet names, street names and more, which can be used to hack passwords and gain access to your family's personal accounts.

Social scams

Online friend requests
Scammers pose as peers and befriend kids on social media. They gain their trust, then manipulate them into sharing personal details or sending money. Some even convince kids to send explicit images of themselves, and then threaten to share them publicly if payment demands are not met — a scheme known as "sextortion."

Social media phishing
Scammers create fake social media accounts that appear to belong to legitimate influencers or gaming sites. They lure followers and then trick kids into providing sensitive information or clicking on malicious links.

KeyBank

[1] FBI Internet Crime Report 2023. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

How to protect kids online

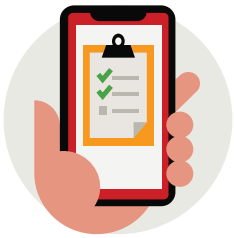
Teach children about the dangers of online scams, the red flags to watch for, and the importance of not sharing personal information with strangers.

Use digital security tools

Parental controls
Use parental control software to monitor your kids' online activity and restrict access to potentially harmful websites.

Privacy settings
Ensure your kids' social media accounts are set to private and encourage them only to accept friend requests from people they know in real life.

Device protection
Install a firewall, ad blockers, and security software on all devices in your household. Consider using a password management tool to help protect your family's accounts.



Discuss fraud and online safety

Open communication
Foster an environment where your kids feel comfortable discussing their online experiences with you. Regularly check in on their internet usage and address any concerns they might have.

Healthy skepticism
Teach your kids to be cautious and never to click on links, pop-up ads, or any messages that look even the slightest bit suspicious. Even if a message appears to be from a known company, your child should navigate to the website directly instead of clicking on the message.

Safe shopping
Tell your kids only to shop from trusted retailers and to navigate directly to their websites. Never click links, even in emails that appear to be from known retailers.

What to do if you think your child has been scammed.

If your child has become a victim of an online scam and you think your KeyBank accounts may be at risk, contact us as soon as possible. We can check to see whether your accounts have been compromised and take measures to help prevent further fraudulent activity.

Call the KeyBank Fraud Client Service Center at 1-800-433-0124, or dial 711 for TTY/TRS.

Stay involved and informed to stay safe.

To help protect your whole family from online scams, make sure everyone has access to the latest information and resources. Learn more about our commitment to fraud prevention and cybersecurity at key.com/fraud.

KeyBank