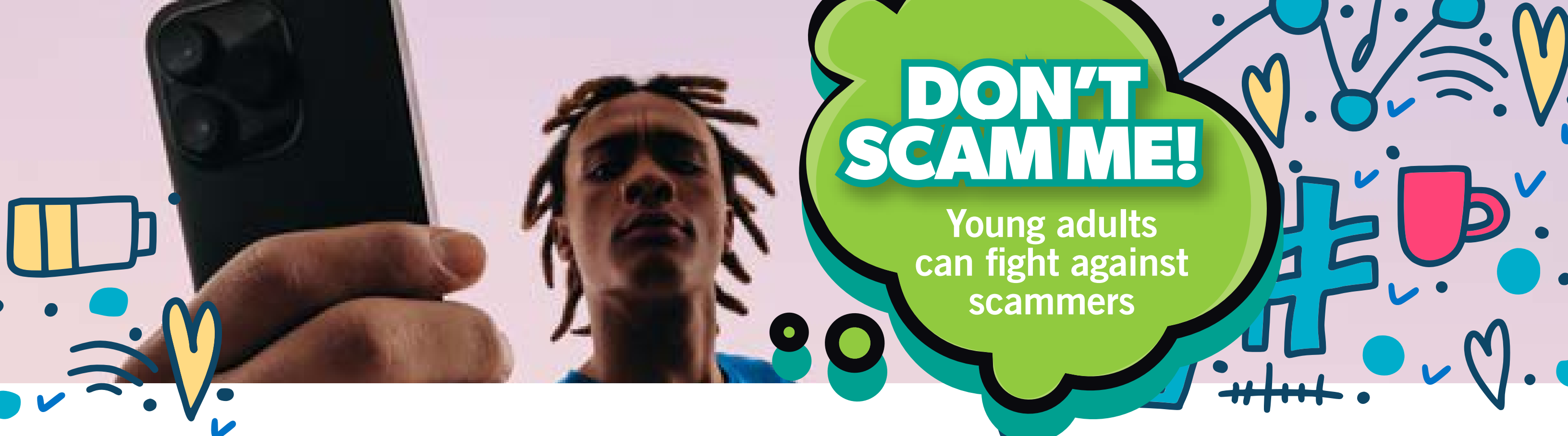

Get smart about common scams:

$16.6 BILLION lost to scams in 2024[1]

73% OF YOUNG ADULTS experienced ONLINE SCAMS[2]

83% OF YOUNG ADULTS tricked by SUSPICIOUS LINKS[3]

Online shopping scams

How it works

- Scammers create fake websites and ads selling popular products at unrealistically low prices.
- You purchase something from them online that never gets delivered or refunded.

How to avoid it

- Check if the seller's account is verified.
- Think twice before paying strangers with real-time payment apps that act like cash. It's almost impossible to get your money back.
- Using a credit card allows you to dispute the charge and get a refund if you don't receive the product.

Online gaming scams

How it works

- Scammers make fake gaming sites and get you to put your credit card on file for rewards that don't exist.
- They trick you with fake in-game purchases or other downloads that end up being spyware instead.

How to avoid it

- Double check directly on a game's website for available in-app purchases before buying anything.
- Use official platforms only. Avoid third party sellers offering discounted items or upgrades.

Deepfake impersonation scams

How it works

- Scammers use AI to create fake images, audio and videos to look and sound like anyone they want.
- You receive a call or text from a person or company that seems real, and they trick you into sending them money or sharing sensitive information.
- To trick you, they'll call you from a number you recognize. They can spoof the actual number to fake it.
- They can pretend to be an influencer you follow or use the identity of someone you trust and ask you for money.

How to avoid it

- Be skeptical when you get contacted unexpectedly.
- Hang up and call the person back at a number you trust.
- Never send anyone your bank information, and don't pay anyone you haven't met in person.
- If an influencer contacts you, check the number of followers they have. Fake influencers have less followers than real ones.
- Look for inconsistencies. Is the voice monotone? Are the audio and video out of sync? Is there unnatural lighting? Does the person rarely blink?
- Reverse image search any photos you receive, it's easy! Right click on the image and select "Search with Google Lens".

Sextortion scams

How it works

- Scammers connect with you as a friend or romantic interest, and they suddenly turn up the heat.
- They will share explicit pictures with you, then ask you for pictures in return.
- Once you send pictures, scammers threaten to post them unless you send money.

How to avoid it

- If you're interested in someone you've never met in person, do your research to confirm their identity.
- If they won't meet up in person, no matter the excuse, assume the person is fake!
- Don't send money to someone you've never met in person.
- Don't share explicit photos, ever.

Employment scams

How it works

- You get a text or email "following up" about a job that you never applied for.
- You accept a job, and they send you a check to cover "equipment costs," which is more money than you need so you are told to send some money back via a payment app.
- The initial check is fraudulent and will bounce, but not before you have already sent your own money to the scammer.

How to avoid it

- Remember that real jobs won't make you buy all your own equipment.
- Don't trust job listings that promise high pay for minimal effort.
- If it sounds too good to be true, it's most likely a scam.

1. Federal Bureau of Investigation 2024 Internet Crime Report

2. Pew Research Center, Online Scams and Attacks in America Today

3. PYMNTS, Report: 82.9% of Young Adults Have Been Tricked by Suspicious Links

What to do if you get scammed

Don't panic, and don't let fear of embarrassment keep you from getting help!

- Contact your bank right away if you've sent money or shared information to a scammer.
- Report the scammer's account on the app where they interacted with you.
- Save screenshots and proof of messages, then block the scammer.
- Contact the police and file a report with the **FBI at ic3.gov**.

FICO

GET SMART ABOUT CREDIT

ABA FOUNDATION