How To Recognize and Avoid Scams

Scam artists take advantage of millions of people each year, using the internet to commit fraud by stealing personal information or tricking people into spending money. Young people under the age of 20 have become the group most susceptible to scams because they use the internet more and have more social media accounts.

Common Scams That Target Teens and Young Adults

Social media scams

Scammers create contests, surveys, and games requesting personal information. They also create cloned (copied) accounts and pose as someone you know so they can get personal information or money.

Online shopping scams

Scammers often make fake websites selling popular knockoff or counterfeit products. They sometimes pretend to be online influencers promoting products to get you to click websites for more information. The item never arrives after you buy it, and they keep your money and have your personal and financial information.

Phishing

Scammers request personal information through fake applications for credit cards, scholarships, grants, and other freebies. Scammers often say that to win something, you must pay a fee or provide a bank account, or they say there is a problem with one of your accounts and you have to verify some information. They pressure you to act immediately and tell you to pay in a specific way (like a money transfer or gift card payment).

Catfishing

Scammers use pictures of famous people or young people to make you feel comfortable and ask for personal information or money. They may also ask for pictures of you, then ask for money not to share the pictures online or with your friends and family.

TIPS FOR AVOIDING SCAMS

- Do not share your email, address, or other personal information in pop-ups, online quizzes, or on unfamiliar websites.
- Only connect online with people you know.
- Never send money to or accept money from people you don't know.
- Do not share your bank account information until you have reviewed the company. Legitimate organizations will not call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.
- If you get an email or text message from a company you recognize and think it may be real, still do not to click on any links in the message. Instead, contact them using a website you know is trustworthy or look up their phone number. Do not call a number they gave you or the number from your caller ID.
- Filter and block unwanted calls and text messages.
- Resist the pressure to act immediately. Legitimate businesses will give you time to make a decision.
- Never pay someone who insists you pay with a gift card or by using a money transfer service. Never deposit a check and send money back to someone.
- Check the email or website URL. If the message or website has typos, uses Gmail or Yahoo, does not match a business you recognize, or has a strange address, it may be a scam.
- Stop and talk to someone you trust, such as a family member, caregiver, teacher, or neighbor.

To learn more about avoiding scams, visit the Federal Trade Commission web page or this Consumer Finance Protection Bureau web page.

To report a scam to the Federal Trade Commission at ReportFraud.ftc.gov or the FBI at https://www.fbi.gov/scams-and-safety.

To research a business, visit the Better Business Bureau at https://www.bbb.org/

FYSB Family & Youth Services Bureau

This resource was developed by RTI International under contract HHSP233201500039I/HSP23337016T with the U.S. Department of Health and Human Services, Administration on Children, Youth and Families, Family and Youth Services Bureau.