

Avoiding Online and Phone Scams

What is a scam?

A scam is when someone tries to trick or deceive you to take your money, personal information, or something valuable. Scammers often use the internet, phones, emails, or social media to try to trick people. It's important to know how to spot and avoid scams.

Common Types of Scams

Phishing Scams (Emails & Texts) send you an email that looks real but asks for personal information like passwords or bank information.

What to Do: Never give out your personal information over email or text when someone you don't know or know well is asking for it.

Fake Phone Calls are where a scammer calls and pretends to be from a bank, the government, or a company, and asks for money or personal information.

What to Do: Hang up and call the real business or government agency to check and see if the call is real.


Lottery or Prize Scams are when you get a message saying you won a prize or lottery, but they ask you to pay money to claim it.

What to Do: Never pay to win a real prize. If it sounds too good to be true, it probably is.

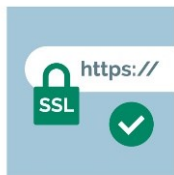
Romance Scams are when you meet someone online who pretends to be interested in you romantically and they ask you for money.

What to Do: Never send money to someone you've just met or only met online. Never give out your personal or financial information, including your address. Never agree to meet someone you have met online all by yourself. Have a trusted adult go with you to the meeting.

Online Shopping Scams are fake websites or sellers who are selling products that never come after you pay for them.

What to Do: Only buy from trusted websites and always check reviews. Check and make sure the URL starts with https:// instead of just http://. The "S" stands for secure which means the website keeps your data safe. A padlock icon () also indicates the website is secure. Fake websites may often have a slightly misspelled web address (domain name). They may use the number 0 instead of the letter O, for example.

HOW TO CHECK IF A WEBSITE IS SECURE



CHECK IF THE SITE USES SECURE ENCRYPTION (HTTPS)



PAY ATTENTION TO THE URL



LOOK FOR A PRIVACY POLICY



CHECK FOR CONTACT INFORMATION



USE WHOIS TO LOOK UP THE DOMAIN OWNER



USE SECURITY TOOLS TO EVALUATE THE SITE



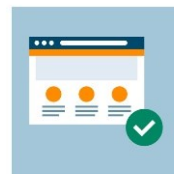
KNOW THE SIGNS OF WEBSITE MALWARE (POP-UPS, MALICIOUS REDIRECTS, SPAM..)



CHECK THE AUTHENTICITY OF THE SECURITY SEALS



READ CUSTOMER FEEDBACK AND REVIEWS



ANALYZE THE STYLE AND CONTENT OF THE WEBSITE

Fake Tech Support Scams are when scammers call or send a message saying there is something wrong with your computer and ask you for payment to fix it.

What to Do: Real tech people will not ask for payment before they fix your tech and will not ask for access to your computer out of nowhere. Contact a computer repair company if you think there is something wrong with your computer.

How to Stay Safe from Scams

Think before you Click:

Don't click on links in emails, texts, or social media posts unless you are sure they are from a trusted source. If you receive something that asks you to click on a link to access your account, do not click on the link. Go directly to the source and log in through the actual source, not through the emailed link.

Don't Share Personal Information:

Never give out your Social Security Number, passwords, or banking information over the phone, by email, or through text. Your bank and credit card provider will never call and ask you for that information.

Be Careful with Money Requests:

If someone you don't know well asks for money, it is likely a scam. Don't respond to fake emails saying you owe money or your credit card has been rejected if you know this is not true.

Check with a Trusted Person:

If you are unsure about something, ask someone you trust for help!

Look for Red Flags:

Scammers will try to pressure or threaten you. They might say something bad will happen if you don't act quickly. Always take your time to think, ask for help, and don't be rushed into doing anything that feels wrong. Check for poor grammar and spelling mistakes. Scammers often have these errors on posts and fake texts and websites.

What To Do If You Suspect a Scam

Hang up or Stop Communicating:

If something feels wrong, stop replying, hang up, or close the website. Never interact with someone who makes you feel uncomfortable or threatened.

Don't Give in to Pressure:

Scammers want to scare you or rush you into doing something, so take your time and ask for help. Don't let them rush you into doing something you don't want to do.

Report the Scam:

Call your local police or report the scam to a trusted adult who can report it for you. You can report online scams to the Federal Trade Commission (FTC) at www.ftc.gov or call 1-877-FTC-HELP (1-877-382-4357). For phone scams, report to the National Do Not Call Registry at www.donotcall.gov.

REMEMBER: Stay alert, stay safe, and always ask for help when unsure!

The contents of this tip sheet were developed under grant number H235F00011 from the U.S. Department of Education. However, those contents do not necessarily represent the policy of the U.S. Department of Education, and you should not assume endorsement by the Federal Government.



Independent Futures that Work!
A project of the Alabama Parent Education Center
PO Box 118 * Wetumpka AL, 36092
*334-567-2252 *866-532-7660
<https://independentfuturesthatwork.com>

