UPDATED FALL 2026

Scam Alert Reference Card

The scams going around right now, and the one move that stops each one.

THREE THINGS REAL ORGANIZATIONS NEVER ASK YOU TO DO

1. Move your money to a new account to "keep it safe"
2. Pay with gift cards, crypto, a wire transfer, or a payment app
3. Read back a code sent to your phone, or keep the call a secret

The "your account is at risk" call

WHAT IT LOOKS LIKE

A caller says they are from your bank, the FTC, or another agency. Your account has a problem and your money needs protecting.

THE GIVEAWAY

They want you to move money, or withdraw cash for a "courier" to pick up.

WHAT TO DO

Hang up. Call the number on the back of your card.

Unpaid toll or package texts

WHAT IT LOOKS LIKE

A text says you owe a small toll or delivery fee. Pay today through the link or face a penalty.

THE GIVEAWAY

A link, a small fee, and a deadline, all in one text.

WHAT TO DO

Do not tap. Type the toll agency's or carrier's website yourself and check there.

The "Hi, is this Sarah?" text

WHAT IT LOOKS LIKE

A friendly stranger texts the "wrong person," keeps chatting, then shares an investment that is "doing great."

THE GIVEAWAY

A new online friend who brings up money or crypto.

WHAT TO DO

Do not reply. Delete and block the number.

The easy job offer

WHAT IT LOOKS LIKE

A message offers good pay to like videos, rate products, or "complete tasks" from home.

THE GIVEAWAY

You have to pay or deposit money to unlock your earnings.

WHAT TO DO

Stop there. A real job pays you. It never charges you.

A loved one's voice in trouble

WHAT IT LOOKS LIKE

A call sounds just like your grandchild or child, needing money now. AI can copy a voice from a short clip.

THE GIVEAWAY

Panic, a rush, and "please do not tell anyone."

WHAT TO DO

Hang up. Call them back on the number you already have. Ask for your family code word.

The tech support pop-up

WHAT IT LOOKS LIKE

A loud warning says your computer is infected. Call this number.

THE GIVEAWAY

They want access to your device.

WHAT TO DO

Close the browser. If it will not close, restart. Never call a number on a pop-up.

QUICK CHECK FOR QR CODES

A QR code you were not expecting, in a text, email, letter, or on a parking meter? Do not scan it. Type the company's address instead.

IF IT ALREADY HAPPENED

1. *Call your bank right away, using the number on your card.*
2. *Change the password on any account you shared.*
3. *Report it at **ReportFraud.ftc.gov** or call 1-877-382-4357.*
4. *If someone has your personal details, visit **IdentityTheft.gov** for a step-by-step recovery plan.*

Keep these numbers handy

Fill these in now, so you never have to look them up in a hurry.

My bank's fraud line	
My credit card company	
Someone I trust to call	
Our family code word	Keep this one in your head, not on paper.

GET THE NEXT ALERT FIRST

Scams change every few weeks. Our free weekly Scam Alerts tell you what is new and exactly what to do about it.

Sign up at **simpledigitalsafety.com**

© 2026 Simple Digital Safety. All rights reserved.