SCAM RED FLAGS CHECKLIST

The 15 Warning Signs That Every Scam Has in Common

Prepared by the Sage Curriculum · aiclassforseniors.com

Most people who get scammed say "I knew something felt off." This checklist helps you listen to that instinct. Print it. Keep it by your phone or computer. When something feels wrong, check the list.

■ 1. Urgency or pressure to act immediately
"Your account will be closed in 24 hours!" Real organizations give you time. Scammers don't.

■ 2. Requests for personal information
Passwords, Social Security numbers, bank details — legitimate companies already have your info and won't ask for it by email or phone.

■ 3. Unusual sender address or phone number
The email says "Amazon" but the address is support@amaz0n-billing.net. Always check the actual sender.

■ 4. Grammar or spelling errors in official communication
Banks and government agencies proofread their emails. Scammers often don't.

■ 5. Links that don't match the text
The link says "Chase.com" but hovering shows it goes to "chase-secure-login.xyz". Always hover before clicking.

■ 6. Requests for unusual payment methods
Gift cards, wire transfers, cryptocurrency, or Zelle to strangers. Legitimate businesses don't ask for these.

■ 7. Too good to be true
You won a prize you didn't enter. You're getting a refund you didn't request. If it sounds too good, it is.

■ 8. Emotional manipulation
"Your grandchild is in trouble!" Scammers use fear, love, and urgency to bypass your judgment.

■ 9. Threats or intimidation
"You'll be arrested if you don't pay." The IRS, police, and courts don't threaten by email or phone.

■ 10. Requests to keep it secret
"Don't tell anyone about this call." Isolation is a scammer's most powerful tool.

■ 11. Unsolicited contact about money
You didn't reach out to them. They reached out to you. That alone is a red flag.

■ 12. Requests to download software or click links
"We need to fix your computer remotely." Never give remote access to someone who contacted you.

■ 13. Spoofed caller ID or email
Just because it says your bank is calling doesn't mean it is. Scammers can fake any number or address.

■ 14. Vague or generic greetings
"Dear Customer" or "Dear Account Holder" instead of your name. Real companies know who you are.

■ 15. Pressure to bypass your normal process
"Don't call your bank — just give us the information directly." Anyone who discourages verification is a scammer.

THE STOP-VERIFY-CONFIRM PROTOCOL

STOP	VERIFY	CONFIRM
Do not click, do not respond, do not send money. Pause.	Contact the real organization directly using a number you trust (not one from the message).	Only proceed after you have independently confirmed the request is legitimate.

HOW TO USE THIS CHECKLIST

When you receive a suspicious email, call, or message: **count the red flags**. If you see even **one or two**, be very skeptical. If you see **three or more**, it is almost certainly a scam. Use the STOP-VERIFY-CONFIRM protocol above before taking any action.