Online Scam Red Flags: Your Quick Reference Checklist

Use this checklist to help you spot potential scams in emails, texts, phone calls, and websites. If you notice any of these warning signs, proceed with caution and consider getting a second opinion from someone you trust.

Red Flag Checklist

Urgency Warning Signs

- [ ] Message claims I must "act now" or face serious consequences
- [ ] Threatens that my account will be closed or suspended if I don't respond immediately
- [ ] Gives an unreasonably short deadline to respond (hours or "today only")
- [ ] Uses alarming language designed to make me feel worried or frightened
- [ ] Pressures me to make a decision without time to think or verify

Payment Method Warning Signs

- [ ] Asks for payment via gift cards (Amazon, iTunes, Google Play, etc.)
- [ ] Requests wire transfers or money orders
- [ ] Wants payment through cryptocurrency (Bitcoin, Ethereum, etc.)
- [ ] Asks me to send cash through the mail
- [ ] Directs me to unusual payment websites I've never heard of

"Too Good to Be True" Warning Signs

- [ ] Notifies me I've won a contest or lottery I never entered
- [ ] Offers an inheritance from someone I don't know
- [ ] Promises unrealistic investment returns or profits
- [ ] Offers products at suspiciously low prices
- [ ] Promises jobs with high pay for minimal work

Communication Quality Warning Signs

- [ ] Message contains multiple spelling mistakes
- [ ] Has obvious grammatical errors or strange phrasing
- [ ] Uses awkward or unnatural language
- [ ] Addresses me as "Dear Customer" rather than by name

- [ ] General appearance looks unprofessional compared to legitimate messages

Email Address Warning Signs

- [ ] Sender's email doesn't match the organization they claim to represent
- [ ] Uses public email domains (gmail.com, yahoo.com) for official business
- [ ] Email address contains extra words or numbers (amazon-support123@gmail.com)
- [ ] Domain name has slight misspellings (amazom.com instead of amazon.com)
- [ ] Return address is completely different from the organization name mentioned

Personal Information Warning Signs

- [ ] Asks for my Social Security number via email, text, or unsolicited call
- [ ] Requests my account passwords or PIN numbers
- [ ] Asks for credit card information out of the blue
- [ ] Wants my Medicare or health insurance numbers
- [ ] Requests copies of personal identification documents

Link and Attachment Warning Signs

- [ ] Contains unexpected attachments I wasn't anticipating
- [ ] Urges me to click on links to "verify my account"
- [ ] Link shows a different URL when I hover over it than what appears in the text
- [ ] Attachment has an unusual file type (.exe, .zip, or .scr)
- [ ] Website URL is slightly different from the legitimate site (amaz0n.com vs. amazon.com)

If You Spot These Red Flags:

1. **Stop and think** - Take a moment to evaluate the situation
2. **Don't click** on any suspicious links or open unexpected attachments
3. **Contact the organization directly** using their official phone number or website (not the contact info provided in the suspicious message)
4. **Talk to someone you trust** about the situation
5. **Report suspected scams** to the Federal Trade Commission at ReportFraud.ftc.gov

Remember:

- Legitimate organizations won't pressure you to act immediately
- Government agencies like Social Security, Medicare, and the IRS typically contact you by mail first
- No legitimate organization asks for payment via gift cards
- When in doubt, verify independently before responding