



SENIOR SATURDAYS · A GUIDE FROM IgCE

How to Spot a Scam Email

You don't need to be a computer expert to catch a scam. Almost every scam email uses the same three tricks. Learn these three and you'll catch nearly all of them.

The 3 warning signs — every time

1 It contacts you first.

You didn't ask a question, request a password reset, or expect this message. A real company almost never surprises you out of nowhere.

2 It rushes you.

"Act within 24 hours." "Your account will be closed today." Real companies give you time. Scammers never do — because a calm reader is a reader who checks.

3 It asks for money, a gift card, or personal information.

Your Social Security number, a password, a bank login, or a request to buy gift cards. No real company asks for gift cards. Ever.

Before you click — check it yourself

- ☐ Hover your mouse over the link without clicking. Does the address match the real company's website?
- ☐ Look closely at who sent it. Is the email address misspelled or strange, like **support@amaz0n-secure.net**?
- ☐ Call the company yourself, using the number on your card or their real website — never a number from the email.
- ☐ Ask someone you trust before you click, reply, or send anything.

Scams going around right now

Fake package notices “Your delivery couldn’t be completed — click to reschedule.” A text or email about a package you weren’t expecting.	Tech-support pop-ups A scary message says your computer is infected and gives you a number to call. Real security software never does this.
Cloned-voice calls A call sounds exactly like a grandchild or loved one asking for emergency money. Scammers now use AI to copy real voices. Hang up and call that person back directly.	Government impersonation “Your Social Security number has been suspended.” Real agencies contact you by mail first — never by a threatening call or email.

Not sure? Call. It is always okay to ask.

- ☐ **AARP Fraud Watch Network Helpline** (free, anyone can call): **1-877-908-3360**
- ☐ Forward a suspicious **text message** to **7726** (it spells SPAM)
- ☐ Forward a suspicious **email** to **reportphishing@apwg.org**
- ☐ Or bring it to **Senior Saturdays** — we’ll look at it together, every week.