

Scam Safety Quick Guide

Keep this page nearby. Before you click, reply, or send money, run through these checks.

STOP

CHECK

VERIFY

A short pause can prevent a big problem.

1 Slow down when it feels urgent

Be cautious if a message tells you to act quickly, pay today, keep something secret, or risk losing an account. Urgency is meant to make you react before thinking.

2 Check the sender, not just the name

Logos and names can be copied. Look at the full email address, phone number, and website domain for misspellings, extra words, or strange endings.

3 Question unusual requests

Pause if someone asks for gift cards, crypto, wires, remote computer access, passwords, or one-time codes — especially if they contacted you first.

4 Verify through a separate channel

If family asks for money, call the number you already have. If a company contacts you, use its official app, card, statement, or trusted website to verify.

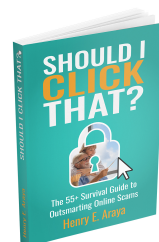
Already clicked?

- Password:** Change it on the real site and turn on 2-step verification.
- Payment:** Call your bank/card issuer using an official number.
- On the phone?** Hang up and call a trusted number from the company they claim to be.

Want to learn more?

Should I Click That? The 55+ Survival Guide to Outsmarting Online Scams has everything you need to know to stay safe online and more! Written by a senior-citizen cybersecurity expert, this book teaches you how to stay safe online, without assuming you are a tech expert who understands online lingo and jargon.

To get the book visit **shouldiclickthat.net** or write an email at support@shouldiclickthat.net.



SHOULDICLICKTHAT.NET