threat level: human

The attack vector you can't patch.

Elder Fraud and Tech-Support Scams

The scams that target older adults, and how families can shut them down.

$7.7B
losses reported by victims age 60+ in 2025
FBI IC3, 2025

+59%
year-over-year surge in elder-fraud losses
FBI IC3, 2025

$38,501
average loss per elderly victim
FBI IC3, 2025

TECH-SUPPORT AND POP-UP SCAMS

01 A pop-up or call about a virus
A warning that your computer is infected and you must call a number now.

02 A request for remote access
Letting a 'technician' control your screen to 'fix' or 'refund' you.

03 Payment in gift cards or wire
Any support that wants gift cards, crypto, or a bank transfer is a scam.

IMPOSTOR AND GRANDPARENT SCAMS

04 A panicked call from 'family'
A grandchild in jail or hurt, needing money kept secret from the rest of the family.

05 Government or prize impostors
Social Security, Medicare, or a lottery that needs a fee or your personal details.

CHARITY, DEBT AND ROMANCE IMPOSTORS

06 Urgent charity or disaster appeals
A donation demand by phone or email right after a tragedy in the news.

07 Debt or warrant threats
A caller demanding immediate payment to avoid arrest, a fine, or a cut-off.

08 A new online companion who needs help
A friendship or romance that soon turns to requests for money.

DO / DON'T

DO
- Hang up and call the person, bank, or agency back on a number you look up yourself.
- Agree on a family code word for real emergencies.
- Talk to a trusted relative before sending money or sharing details.
- Set up a credit freeze and screen calls from unknown numbers.

DON'T
- Do not pay with gift cards, wire, crypto, or cash couriers. Agencies never ask for these.
- Do not give remote computer access to anyone who calls you or pops up on screen.
- Do not share Social Security, Medicare, or bank details with an unexpected caller.
- Do not let anyone rush you or insist you keep it secret from family.

THE ONE MOVE

Hang up and call the person or agency back on a number you look up yourself, and never pay with gift cards, wire, or crypto. Agree on a family code word for real emergencies.

IF IT HAPPENS

1. Stop paying and hang up. It is never too late to stop.
2. Call your bank to halt or reverse recent transfers, and watch for follow-on scams.
3. If you gave computer access, run a trusted scan and change your passwords.
4. Report to reportfraud.ftc.gov and ic3.gov. In the US, the DOJ Elder Fraud line is 833-372-8311.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: FBI IC3 Elder Fraud Report (2025). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.