YOUR PERSONAL PROTECTION GUIDE

AI Scams & *Deepfake* Awareness

In 2025, AI-enabled fraud surged 1,210%. This handbook gives you the knowledge to fight back.

1,210%	$40B	3 sec
SURGE IN AI FRAUD IN 2025	PROJECTED LOSSES BY 2027	TO CLONE YOUR VOICE

Prepared by Sam Stern

What We Are Up Against

The technology that makes AI scams possible has advanced faster than almost any other technology in history. What looked obviously fake just three years ago is now indistinguishable from reality. Scammers are using what exists right now, today, to steal from people exactly like you.

WHY ELDERS ARE TARGETED

Two out of five seniors have fallen prey to a scam. The average financial loss per elder fraud victim exceeds $30,000 — often a full year's income for someone on a fixed budget. This is not a failure of intelligence. Scammers target elders deliberately because they tend to have accumulated assets, because they came of age when institutions were trustworthy, and because they are more likely to answer the phone.

THE HARDEST TRUTH

Your instincts, which have served you well for decades, are no longer sufficient on their own. You need a system. This handbook is that system.

Six Threats, Clearly Explained

Voice Cloning & The Grandparent Scam

A panicked voice — sounding exactly like your grandchild — calls to say they've been arrested and need bail money urgently. "Please don't tell Mom." The voice was cloned from a birthday video, a voicemail, or a social media clip. Three seconds of audio is all it takes.

Red flags: urgency, secrecy, gift card or wire transfer payment.

Tech Support Scam

An alarming popup appears on your screen claiming your computer has been compromised. A phone number is displayed. You call. A calm, authoritative "technician" asks to remotely access your computer to fix the problem — and once inside, steals your data or charges hundreds of dollars for a problem that never existed.

Red flags: unsolicited popup, request for remote access, payment in gift cards.

Medicare & Medical Fraud

A caller from the "Medicare Benefits Coordination Office" offers free medical equipment at no cost to you. They just need to verify your Medicare ID number and date of birth. That combination is a skeleton key to your identity and your finances.

Red flags: inbound call offering free benefits, request for Medicare ID or Social Security number.

Romance Scams

A sustained campaign of manufactured intimacy — weeks or months of daily contact, remembered details, expressed affection — before a financial "crisis" arises. AI can now run dozens of these relationships simultaneously, each perfectly calibrated to the individual victim. By the time money is requested, a genuine emotional bond exists.

Red flags: online-only relationship, person never available to meet, financial crisis after intimacy established.

Celebrity & Investment Deepfakes

A convincing video of a trusted public figure — a news anchor, a financial expert, even a family member — endorsing an investment opportunity or crypto giveaway. The face moves naturally. The voice is perfect. The opportunity does not exist.

Red flags: investment opportunity from a video, urgency to act before the window closes.

IRS & Government Impersonation

"There is a warrant out for your arrest. Press 1 to speak with an agent." The IRS never calls to threaten arrest. Neither does Medicare, Social Security, or any legitimate government agency. These calls are engineered to produce immediate panic.

Red flags: threat of arrest over the phone, demand for immediate payment.

How Your Defenses Get Turned Against You

These scams are not random. Every element is engineered to bypass the cognitive defenses that have protected you your entire life. Understanding the mechanisms is the first step to dismantling them.

URGENCY
Time pressure shuts down deliberate thinking. When we believe we have an hour, we stop analyzing and start reacting. Every major scam deploys urgency as its primary weapon.

SHAME & SECRECY
"Don't tell anyone." Isolation prevents the reality check that would almost certainly expose the fraud. A second opinion is the scammer's greatest enemy.

LOVE & LOYALTY
When the voice belongs to someone you love, every protective instinct you have gets turned against you. The emotional bond is the attack vector.

AUTHORITY
Police, IRS agents, Microsoft technicians, Medicare coordinators — institutional language carries weight that bypasses skepticism. We are trained from childhood to defer to authority.

BENEVOLENCE
Medical fraud leads with a gift. You're not being manipulated — you're finally getting what you deserve. Generosity disarms in ways that pure fear cannot.

SUNK COST
In romance scams especially, accepting that you've been deceived means accepting that the entire relationship was fabricated. Many people send more money rather than face that loss.

The single most important thing you can do in any suspicious situation is introduce a delay. Urgency is the mechanism. *Slow down* is the antidote.

Your System

STEP 1 — SLOW DOWN

Every scam you've seen runs on urgency. The grandchild who needs bail in the next hour. The Microsoft technician who says your computer will be compromised if you hang up. The Medicare window that closes today. Urgency is not incidental — it is the mechanism. It shuts down the part of your brain that asks questions. So give yourself permission to slow down. To say: *I need a minute.* That minute is worth more than anything else in this playbook.

STEP 2 — THE FAMILY PASSWORD SYSTEM

Agree on a password with your closest family members. One twist on this is to choose a real question with a false agreed-upon answer.

Example: "What's Mom's birthday?" Answer: "March 3rd." (It's actually November 15th.)

A scammer who has done their research will give the correct answer. That is precisely how you know it's not your family. The wrong answer is the right answer.

OUR FAMILY PASSWORD QUESTION	ANSWER

GENERAL RULES

Ten Things That Will Save You

01 Never give Medicare, Social Security, or financial information to an inbound caller — ever, for any reason.

02 Gift cards and cryptocurrency are never legitimate forms of payment. No government agency, utility, or bank will ever ask for them.

03 No legitimate institution will threaten you with immediate arrest or legal action over the phone.

04 If someone asks you to keep a conversation secret from your family, the secrecy is the scam.

05 Never allow anyone to remotely access your computer unless you initiated the call yourself.

06 When in doubt, hang up. You can always call back on a number you find yourself.

07 If an offer sounds too good to be true — free equipment, unexpected winnings, unclaimed benefits — it is.

08 Never click a link in a text message or email asking you to verify your account or confirm personal information.

09 A real emergency can withstand a ten-minute delay. If someone tells you there's no time to think, that's the scam talking.

10 If you receive a video or audio message from a public figure endorsing an investment, assume it's fabricated until proven otherwise.

IF YOU OR SOMEONE YOU LOVE HAS BEEN SCAMMED

First: it is not your fault. These operations are professionally engineered to deceive intelligent, careful people. The shame of staying silent costs more than the scam itself.

Report to the FTC

reportfraud.ftc.gov

Report to the FBI

ic3.gov

You came into today not knowing what you didn't know.

That changes now.

The technology will keep evolving. But so will you.

BRING THIS TALK TO YOUR COMMUNITY

Sam Stern

AI Educator · Speaker · Workshop Leader

aiscams.samstern.life	samstern.life	sam.stern@esalen.org
LANDING PAGE	MAIN WEBSITE	EMAIL