



A FREE SENIOR SAVVY SAFETY GUIDE

7 TECH SCAMS EVERY OHIO FAMILY SHOULD KNOW

The simple rule that defeats most scams: pause, verify, and use a contact method you already trust.

KEEP THIS GUIDE NEAR THE PHONE

Share it with a parent, neighbor, friend, or caregiver.

Questions? Call Senior Savvy: 513-444-6486

Patient technology help across Ohio • myseniorsavvy.com



PAUSE BEFORE YOU ACT

The 10-second scam test

STOP.

Do not click. Do not pay. Do not give access.

A real company or agency will let you hang up and verify independently.

1

Pause

Scammers manufacture urgency so you act before you think.

2

Verify

Call the person, bank, agency, or company using a number you already know.

3

Protect

Never share a password, one-time code, Social Security number, or remote access.

4

Talk

Ask a trusted person before sending money or changing an account.

If someone demands gift cards, cryptocurrency, wire transfers, cash, or gold:

STOP. IT IS A SCAM.



Scams 1–2

1 The fake tech-support warning

Warning signs: A pop-up, call, text, or email says your computer has a virus and tells you to call immediately.

Do this: Close the browser or turn off the device. Never call the number in the warning and never allow remote access. Contact a trusted helper or the real company through its official website.

2 The bank or account “fraud alert”

Warning signs: A message says money is at risk, your account is locked, or you must move funds to a “safe” account.

Do this: Do not reply or use the message link. Call the number printed on your card or statement. A real bank will never need your password or one-time verification code.

Caller ID and familiar company logos can be faked.

Trust the contact method you chose—not the one the stranger supplied.



Scams 3–4

3

The family emergency

Warning signs: A caller claims a child or grandchild is hurt, arrested, or stranded and begs you to keep it secret.

Do this: Hang up. Call the family member directly or contact another relative. Create a private family verification phrase for real emergencies.

4

The government or tax threat

Warning signs: Someone claims to be from the IRS, Social Security, Medicare, police, or a court and threatens arrest, lost benefits, or immediate penalties.

Do this: Hang up and verify through the agency's official website or published number. Government agencies do not demand gift cards, cryptocurrency, or secrecy.

Urgency + secrecy + unusual payment = a scam pattern.

Slow the conversation down and involve someone you trust.



Scams 5–7

5 Delivery or unpaid-toll text

Warning signs: An unexpected message says a package cannot be delivered or a small toll must be paid through a link.

Do this: Do not tap the link. Open the official delivery, toll, or government website yourself, or use the company's official app.

6 The romance or online-friend request

Warning signs: A new online relationship becomes intense quickly, avoids meeting, and eventually asks for money, investments, gift cards, or help with an emergency.

Do this: Stop sending money or information. Talk with a trusted person and reverse-image-search profile photos when possible.

7 The prize, refund, or investment promise

Warning signs: You “won” something you did not enter, are owed a surprise refund, or are promised guaranteed high returns with little risk.

Do this: Never pay to receive a prize or refund. Verify investments through official regulators and contact the real company using a trusted number.

A real opportunity does not require an immediate secret payment.



ACT QUICKLY—WITHOUT BLAME

If something already happened

1. Contact the payment company or bank

Tell them it may be fraud. Ask whether the charge or transfer can be stopped or reversed.

2. Change exposed passwords

Start with email and banking. Use a new password and turn on multi-factor authentication.

3. Remove remote access

Disconnect the device from the internet and have a trusted professional check for remote-control software.

4. Report the scam

Use [ReportFraud.ftc.gov](https://reportfraud.ftc.gov). For identity theft and a recovery plan, use [IdentityTheft.gov](https://identitytheft.gov).

5. Tell someone you trust

Scammers rely on shame and secrecy. Being tricked is not a character flaw; getting help quickly matters.

Need patient help checking a device or account settings?

Senior Savvy LLC • 513-444-6486 • seniorsavvyofficial@gmail.com

Serving Ohio by appointment. Travel availability and any fee are confirmed first.



WRITE THEM DOWN NOW

Keep these trusted contacts

Trusted family member or friend

Bank or credit-card fraud number

Doctor, insurance, or Medicare contact

Phone and internet provider

Trusted technology helper

The safest response is often:

Hang up. Look it up. Call back.



Senior Savvy help

Safety sources: Federal Trade Commission Consumer Advice (consumer.ftc.gov) and the Internal Revenue Service (irs.gov).