
Scams Are Exploding in America: How to Protect Yourself and Your Family in 2026

Scams are no longer a minor nuisance — they are a full-scale industry. Criminals are using email, text messages, phone calls, social media, and now **AI-generated voices** to trick people into sending money, sharing personal information, or clicking malicious links.

The numbers are staggering. According to the Federal Trade Commission, Americans reported **more than $12.5 billion in losses to fraud in 2024**, a 25% increase from the previous year. Older Americans alone reported nearly **$2.4 billion** in losses in 2024. And because most fraud is never reported, the real number is likely far higher — possibly as high as **$81.5 billion** for seniors alone.

This is not slowing down. It's accelerating.

Below is the practical, real-world guidance I give my own clients — and the advice I want every family to hear.

---

1. Do NOT Click Anything You Don't Recognize

If you receive:

- A text message
- An email
- A link
- A "delivery notice"
- A "bank alert"
- A "password reset"

…and you **don't recognize the sender**, **do not click it**.

Do not reply.
Do not open attachments.
Do not tap the link "just to check."

Email was the **most common way scammers contacted victims in 2024**. Clicking a single link can install malware, steal passwords, or give criminals access to your accounts.

If you're worried the message might be real, use this rule:

Call the person or company using a phone number YOU already have — not the one in the message.

If it's a family member, call the number saved in your phone.
If it's your bank, call the number on your statement or debit card.
If it's urgent, go in person.

Never trust the number in the email or text.

---

2. If Your Bank "Calls You," Hang Up

One of the fastest-growing scams is **bank impersonation**. Criminals spoof caller ID so it looks like your bank is calling.

If someone calls claiming to be your bank:

- Hang up immediately
- Call the number on your bank statement
- Or better yet, walk into the branch and talk to a real person

Imposter scams were the **second-highest source of losses in 2024**, costing Americans **$2.95 billion**.

Never give personal information to an incoming call — even if the caller ID looks legitimate.

---

3. The Newest Threat: AI Voice-Cloning Scams

This is the scam that terrifies parents and grandparents the most — and for good reason.

Criminals can now use AI to **clone a family member's voice** using just a few seconds of audio. They can make it sound like your child, spouse, or parent is calling you in a panic:

- "Mom, I'm in trouble."
- "Dad, this is my only phone call."
- "Please send money right now."

These scams are exploding because they work. And they work because they trigger fear before logic.

The solution: Create a Family Password.

Sit down with your family and choose a simple phrase that only your family knows.

If you ever receive a call claiming to be a family member in trouble, calmly ask:

“What’s the family password?”

If they don’t know it — hang up.

One of my clients who works in cybersecurity takes it a step further:
When choosing your family password, **do not discuss it near any electronic device**:

- Phones
- Laptops
- TVs
- iPads
- Smart speakers (Alexa, Google Home)
- Baby monitors
- Anything with a microphone

Assume every device can hear you. Choose the password **offline**, in person, with no electronics nearby.

This one step can save your family thousands of dollars — and a lot of heartache.

---

4. Scams Are Getting More Sophisticated — and More Expensive

Here are the latest verified statistics:

Total U.S. consumer losses to fraud in 2024:

$12.5 billion

Losses among older Americans (60+):

$2.4 billion reported — but the real number may be **$10.1 to $81.5 billion**

Top scam categories:

- **Investment scams:** $5.7 billion lost
- **Imposter scams:** $2.95 billion lost
- **Romance scams:** $329 million lost among older adults

- **Tech support scams:** $159 million lost among older adults

Most common contact method:

Email (for the second year in a row)

Most financially damaging payment methods:

- Bank transfers
- Cryptocurrency

Scammers are evolving faster than ever — and AI is accelerating the problem.

---

5. The Rules That Will Keep You Safe

Here are the rules I give every client:

Rule #1: Never click anything you don't recognize.

Delete it. Block it. Move on.

Rule #2: Never trust caller ID.

If your bank calls you, hang up and call the number on your statement.

Rule #3: Never send money because of fear or urgency.

Scammers create panic on purpose.

Rule #4: Create a family password.

Use it for emergencies.
Use it for verification.
Use it to protect the people you love.

Rule #5: Talk about scams with your family.

Especially older parents and grandparents.
Awareness is protection.

Final Thoughts

Scams are not going away. They are becoming more sophisticated, more personal, and more technologically advanced. But with the right habits — and a family plan — you can stay ahead of them.

Share this article with your family.
Create your password.
Stay alert.
And remember:
When in doubt, don’t click. Don’t reply. Don’t trust the caller ID.