SCAM DEFENSE GUIDE 2026

Marc Bautis
Wealth Manager
Bautis Financial

8 Hillside Ave
Suite LL1
Montclair, NJ 07042

862-205-5800

marc@bautisfinancial.com
http://www.bautisfinancial.com

Bautis Financial

WHY YOU COULD BE VULNERABLE:

Scammers weaponize urgency, authority, fear, and isolation faster than rational thinking can respond. The defense isn't being smarter. It's having a system. Keep this card handy and share it with your family members. Scams succeed by creating urgency and isolation. If anyone asks you to move money urgently, pause and call your advisor first. *(For educational purposes only. Scams continue to evolve, and no single method can eliminate fraud risk).*

1 2026 TOP 5 SCAMS AND HOW TO SPOT THEM*

1. **The Deep Fake Voice Clone Scam** — "I'm in jail, please don't tell mom." Scammers use AI to target parents or grandparents with a family member's fake voice urgently requesting money.
2. **The "Your Social Security Number Has Been Suspended" Call** — Caller claims to be from the Social Security Administration, threatens arrest or suspension of benefits.
3. **The Fake Bank Fraud Alert** — Claims suspicious activity on your account, asks to "verify" by moving money.
4. **The Computer Pop-Up** — "Your Computer Has Been Compromised" warning screen says to call a number immediately for tech support.
5. **Romance That Turns Into Gift Cards and Wire Transfers** — An online relationship builds over weeks/months, then they begin requesting money.

*As determined by Horsesmouth and based on FBI, FTC, and consumer groups.

2 WHAT TO SAY WHEN PRESSURED

Use these phrases to buy time and break the scammers' control:

- "I need to verify this independently."
- "I never make financial decisions under pressure."
- "My advisor requires me to call them first."
- "Let me call you back at the number I have on file for you."

3 SCAM WARNING SIGNS

If they ask for these payments or act this way, it's a scam:

1. Gift cards (iTunes, Google Play, Amazon, Visa, etc.)
2. Cryptocurrency/Bitcoin ATMs
3. Wire transfers to unknown accounts
4. Urgency or pressure to act immediately ("Act now or lose access")
5. Demands for secrecy ("Don't tell anyone about this")
6. Claims to be from official authority (IRS, bank, Social Security)
7. Anger or irritation when you ask questions

Legitimate organizations generally do not request payment using gift cards, cryptocurrency, or urgent wire transfers. If you encounter such requests, consider it a red flag and do not proceed.

4 IF YOU'VE BEEN SCAMMED

IMMEDIATE (next 30 minutes):

- Stop all contact with the scammer
- Call your bank/credit card company NOW (request to stop payment, freeze account, dispute charges, etc.)
- Change passwords if you shared any login information

FIRST 24 HOURS:

- File reports: **ReportFraud.ftc.gov** and **IC3.gov**
- Freeze your credit at all three bureaus for free: Equifax, Experian, and TransUnion

ONGOING (next 6 months):

- Monitor all accounts weekly for suspicious activity
- Consider credit monitoring service for added protection

Call AARP Fraud Watch Network: (877) 908-3360

This is helpful because it provides free, personalized support from trained specialists to help victims of scams/those targeted by them.

5 THE PROOF FRAMEWORK: YOUR 5-STEP SCAM DEFENSE

When you're under pressure, you need a system you can apply without thinking. The PROOF framework gives you five steps to evaluate any suspicious request and the confidence to act on what you find.

P

PAUSE (30–60 seconds):

Your first defense is slowing down. Take 30–60 seconds before responding to any urgent request. This breaks the scammer's momentum and restores rational thinking.

R

REQUIRE A SECOND SOURCE:

Never trust a single call, text, email, or video. Verify through a different channel. If they called, hang up and call them back using a number you look up for yourself; if they emailed, call the official number from their website.

O

OBSERVE INCONSISTENCIES:

Watch for red flags: urgency, secrecy, unusual payment methods, story changes, or anger when you question something. Your gut instinct is often right.

O

OUTSIDE VERIFICATION ONLY:

Look up contact information yourself. Never use what the scammer provides. Use saved contacts for family, not caller ID. Go directly to official websites.

F

FORGET THE REQUEST:

If anything feels off or doesn't pass PROOF, say no and end communication. Legitimate organizations never punish caution.

6 WHY YOU NEED A FAMILY PASSWORD

As technology evolves, scammers are finding new ways to impersonate family members or trusted contacts. Establishing a family password can help confirm whether an urgent request for money is legitimate. A family password is a shared, secret, family phrase that should be provided before any sensitive information is shared or money moves, regardless of how real the caller sounds. All trusted family members should know the family password.

Our family password (use this to verify an "emergency" call):

In a suspicious situation, I will verify by calling:

PRIMARY CONTACT	BACK UP CONTACT
Name:	Name:
Phone:	Phone:

7 REPORTING/RESOURCES

- ReportFraud.ftc.gov
- IC3.gov
- AARP Fraud Watch Network: (877) 908-3360
- Equifax.com
- Experian.com
- Transunion.com