Advisor Article

Protect Yourself From Financial Scams

Initial Version November 2026

Raymond Eustace
ray@eustaceadvisors.com
910-377-5021 office

www.eustaceadvisors.com

NADAJE HOLDINGS LLC dba EUSTACE ADVISORS is an Investment Advisor offering services in North Carolina and in other jurisdictions where exempt from registration. All views, expressions, and opinions included in this communication are subject to change. The content included has been developed from sources believed to be providing accurate information. The information in this material is not intended as tax or legal advice - please consult legal or tax professionals for specific information regarding your individual situation.

© 2026 EUSTACE ADVISORS

Background Information

Many people picture a scam as something obviously off: a strange email, a robotic voice, a too-good-to-be-true offer.

The more dangerous version sounds like rescue. A calm, professional voice tells you your bank or financial account has been compromised, and they're calling to help you fix it before it's too late.

That's what makes it work.

Impersonation scams, where criminals pose as banks, financial institutions and other trusted businesses, have become one of the more common ways people expose their savings. The Federal Trade Commission (FTC) has reported a sharp rise in these schemes, with some victims losing tens or even hundreds of thousands of dollars. Some of these scams tend to follow a predictable script, and once you know it, it can be easier to spot.

Why the "Rescue" Script Is So Effective

These scams don't rely on greed. They rely on fear and trust working together.

First, the caller creates a problem: suspicious activity, a hacked account, money at risk. Then they present themselves as the solution. By the time they ask you to do something, you've already accepted that there's an emergency and that the person on the line is on your side.

It's a bit like someone showing up at your door in a delivery uniform. The uniform says "legitimate." But a uniform is easy to come by, and so is a confident phone voice, a spoofed caller ID or an official-looking email.

How a Typical Call Unfolds

The details vary, but the scenario is often the same:

1. You get an unexpected call, text or email that appears to come from your bank or another financial institution.
2. You're told there's a problem with your account and your money could be in danger.
3. You're given urgent instructions, such as moving your funds to a "safe" account, sharing a verification code or confirming account details.
4. You're encouraged to act right away and keep it to yourself.

The "safe" account, of course, may belong to the scammer. And once money moves, it can be very difficult to get back.

Red Flags in What They Ask For

Some warning signs show up in the request itself. Consider pausing if someone asks you to:

- **Move money you weren't planning to move.** An unexpected transfer request, especially one framed as protecting your savings, deserves a second look.
- **Share passwords, PINs or one-time codes.** Those codes sent to your phone are there to keep others out of your accounts. Anyone asking you to read them aloud may be trying to get in.
- **Pay in unusual ways.** Gift cards, cryptocurrency and transfers to unfamiliar accounts are common ways scammers redirect money.

© 2026 EUSTACE ADVISORS

Red Flags in How They Ask

Other warning signs are about the pressure, not the request:

- **Urgency.** Being told you'll lose everything unless you act right now is designed to keep you from thinking it through.
- **Secrecy.** If someone discourages you from telling a spouse, family member or financial professional, ask yourself why. Often it's because another person might recognize the scam.
- **Resistance to questions.** A legitimate institution should be comfortable with you taking a moment to verify. Pushback is a signal on its own.

Put these together and a pattern emerges: nearly every tactic is built to stop you from checking.

The Simple Habit That Breaks the Script

The most effective defense is also the simplest: hang up and call back.

If you receive an unexpected financial request, end the conversation and contact the institution directly, using a phone number you've confirmed yourself. You can find one on the official website, on the back of your card or in previous statements. Avoid using any phone number, link or contact details provided in the suspicious message.

A real bank won't mind. A scammer may lose their grip the moment you step outside their script.

Make It a Family Conversation

Scams thrive on silence. People who've been targeted often feel embarrassed, and that embarrassment keeps the warning signs from spreading.

Consider talking about this with the people in your life: aging parents, adult children, close friends. Agree that a "just checking" call is always welcome, no matter how minor the question seems. That one habit can help create a safety net around the people you care about.

Summary

Impersonation scams succeed when they convince you that the fastest action is the safest one. In reality, the safest move is almost always to slow down and verify.

You don't have to memorize every tactic. Just remember that unexpected urgency is a reason to pause, not to act. And if a message claiming to come from a financial institution you work with ever feels off, a quick call to confirm is always worth making.

Resources

1. https://consumer.ftc.gov/articles/how-avoid-scam.
2. https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds.
3. https://www.aarp.org/money/scams-fraud/bank-impersonation-fake-text-messages-emails-calls/.

**This content was developed from sources believed to be providing accurate information. The information provided is not intended as tax or legal advice, and readers are encouraged to seek advice from their own tax or legal counsel. This material was developed and produced by Eustace Advisors to provide information on a topic that may be of interest. Copyright 2026 Eustace Advisors.*

© 2026 EUSTACE ADVISORS