ANTI-SCAM SURVIVOR'S GUIDE

Information and resources current as of October 2026.

Fraud has changed. The warning signs many of us learned to look for are no longer enough. A call can come from a familiar number. A voice can sound like someone you have known for years. A website can look legitimate. The person contacting you may know things about your life that make it difficult to believe you are talking to a stranger.

I learned that the hard way. I was deceived more than once, despite asking questions, checking information, and believing I was being careful.

I don't want what happened to me to make you suspicious of everyone.

When I held focus groups with retirees while writing this book, they repeatedly told me they wanted something practical: a short, easy-to-understand guide to some of the most important things they could do to protect themselves. That is what I have tried to provide here.

No guide can cover every safeguard or every kind of fraud. Things are changing too quickly. I have concentrated on some of the most useful protections I found, along with what to do if you think you have already been defrauded. I have tried to keep them simple enough to understand and practical enough to use.

None of these safeguards can guarantee that you will never be deceived. No guide can do that.

1. KEEP THIS PAGE NEAR YOUR PHONE

Keep these four rules where you can reach them quickly. You might tear out this page or make a copy to keep near your phone. Take a photo of it, too, so you have it with you when you are away from home.

1. Hang up and call back yourself. If someone calls and says they are from your bank, your brokerage, a government agency, or a company you use, end the call. Find the number yourself—on the back of your card, on a statement, or in an app you already use. Never use a number the caller gives you. Caller ID can be faked.

2. Pay attention to how you are being asked to send money. Gift cards, cryptocurrency, wire transfers, and payment apps can be difficult or impossible to reverse once the money is sent. Being asked to use one of them does not by itself mean you are being defrauded. If someone is also pressuring you to act quickly, stop and verify who you are dealing with before you send anything.

3. Don't use the link they send you. Go to the company's website or app yourself. A fake website can look almost exactly like the real one.

4. Urgency is a reason to slow down. “You have to do this now.” “Don't tell anyone.” “The opportunity will be gone.” Those words don't necessarily mean you are being defrauded. They do mean you should stop and verify before you act.

One more rule may be the most important:

Never let the person asking you for money also tell you how to check on them.

2. WHO IS DOING THIS

Many sophisticated scams are not carried out by one person working alone. They are run by organized groups. One person may make the first contact, another may take over later, and others may be responsible for moving the money.

These groups may contact hundreds or thousands of people. They know what has worked before, and they use it again. What may feel to you like a conversation with one convincing person may be part of an operation that does this every day.

Afterward, I kept asking myself how I could have believed what I was being told. It took me a long time to understand that the people who deceived me had probably done this before. I was still responsible for the decisions I made. Knowing more about how these groups operate helped me see how someone who believed he was being careful could still be deceived.

3. WHEN SOMEONE CONTACTS YOU

Don't rely on whether they seem legitimate

Someone trying to deceive you may sound professional, call from a familiar number, send you to a convincing website, and know things about you that make them seem legitimate.

Instead, ask yourself a different question:

How can I check this without using anything this person gave me?

If someone says they are calling from your bank, call the bank yourself. If they say they are your financial adviser, use the number you have always used. If they claim to represent a company, find the company yourself. If a family member appears to be in trouble, end the call and contact that person yourself—or call another family member who may know where they are.

A familiar voice is not proof

“Grandpa, I'm in trouble.”

“Mom, I've been in an accident.”

A voice that sounds exactly like someone you know may not be that person. If someone you care about calls with an emergency, contact that person another way before you send money or provide personal information. If you can't reach them, call someone else who may know where they are.

Some families use a private word that everyone knows and can use in a real emergency. It is a simple precaution that costs nothing.

Video is not proof either

Seeing someone on a video call is no longer enough to establish that you are actually talking to that person. Artificial intelligence can create convincing video as well as voices.

Don't depend on your ability to recognize a fake. End the call and contact the person yourself, using a number or other method you already know.

4. BEFORE YOU SEND MONEY

In Chapter 12, I described several things I now do before making an important decision. They apply here as well. One of them becomes especially important when someone is asking you to send money:

Don't let the person asking for the money also tell you how to check whether what they are saying is true.

In many scams, the person is trying to persuade you to send the money yourself.

I learned this from my own experience. The people who deceived me gave me documents, websites, names, and other information that appeared to confirm what they were telling me. **I** thought I was checking. I didn't understand that much of what I was checking had come from the very people I was trying to verify.

Check the important information yourself. Use a phone number, website, or other source that you found independently and that the person asking for the money does not control.

If you cannot verify the important information without relying on what that person gave you, stop before you send the money.

5. MAKE YOURSELF HARDER TO STEAL FROM

You don't need to become a technology expert. A few basic precautions can make it harder for someone to get into your accounts or use your personal information.

If you're not sure where to begin, start with these three.

DO THESE FIRST

Turn on transaction alerts

Banks, credit-card companies, and brokerage firms can alert you when money is withdrawn, transferred, or charged to your account. Turn these alerts on and choose amounts low enough that you are likely to notice a transaction you didn't make.

Protect your email

Your email account is especially important because it can be used to reset passwords on many of your other accounts. Use a password for your email that you don't use anywhere else, and turn on multi-factor authentication.

It is also worth checking your email settings occasionally to make sure messages are not being forwarded to an address you don't recognize and that the recovery email address and phone number belong to you.

Use multi-factor authentication for your financial accounts

Multi-factor authentication adds another step before someone can get into an account even if they have your password. Turn it on for your bank, brokerage, and other important financial accounts whenever it is available.

If you are given a choice, consider using an authenticator app or a security key because they provide stronger protection than receiving a code by text message. Authenticator apps, such as Google Authenticator or Microsoft Authenticator, can be downloaded from the app store on your phone.

THEN THESE

Don't reuse important passwords

If you use the same password for several accounts, someone who obtains it from one account may be able to use it to get into others.

A password manager can create and store different passwords for you so you don't have to remember all of them.

Protect your phone number

Someone who takes control of your phone number may be able to receive security codes intended for you. Ask your cellular carrier about protections against someone transferring your number to another phone, such as a number lock or port-out PIN.

If your phone suddenly loses cellular service and you don't know why, contact your carrier from another phone.

Keep your devices updated

Install security and software updates on your phone, computer, and tablet when they become available. These updates often correct security problems that have been discovered since the software was installed.

Limit the personal information that is easy to find about you

People-search and data-broker sites may contain your address, age, phone number, relatives, former employers, and other information. Someone trying to deceive you can use that information to make it seem as though they know you or someone close to you.

You can ask individual sites to remove your information yourself, or you can use a service that does much of the work for you. No service can remove everything permanently. Information can reappear, and some public records cannot be removed.

The purpose is not to disappear from the internet. It is to make it harder for a stranger to learn enough about you to create a convincing story.

IF YOU DON'T KNOW WHICH COMPANY TO TRUST

You may decide that you want help with some of these protections. The number of companies offering password managers, identity-theft protection, data-removal services, antivirus programs, and other security products can make it difficult to know which ones to trust.

Rather than relying on an advertisement or a company's own website, look for an independent evaluation. Consumer Reports is a nonprofit organization that tests and reviews thousands of products and services, including some related to digital security and privacy. Its ratings and reviews are available through its website, although access to many of them requires a small membership fee.

You won't find every product or service reviewed there, but it can give you an independent place to begin when you aren't sure which company to trust.

6. IF YOU THINK YOU'VE BEEN DEFRAUDED

If you think you may have sent money to someone who deceived you, act as quickly as you can. Don't wait until you are certain.

Contact the financial institution immediately

Call the bank, brokerage firm, credit-card company, payment service, cryptocurrency exchange, or other institution involved. Tell them you believe you may have been defrauded and ask whether the payment or transfer can be stopped, recalled, or frozen.

Use a phone number or website you find yourself, not contact information provided by the person who received the money.

Even if you think it may be too late, make the call.

Report what happened

Report the fraud to the appropriate law-enforcement and government agencies. The resources at the end of this guide will tell you where to begin.

If a bank, brokerage firm, payment service, cryptocurrency exchange, or other company was involved, report it there as well.

Protect your accounts

If you gave someone a password or other information they could use to get into one of your accounts, change the password and turn on multi-factor authentication. If you used the same password on other important accounts, change it there too.

Freeze your credit

Consider freezing your credit, especially if someone may have obtained personal information they could use to open an account in your name. A credit freeze is free and does not affect your credit score. To place one, contact each of the three credit bureaus:

1. **Equifax: 800-685-1111**
2. **Experian: 888-397-3742**
3. **TransUnion: 888-909-8872**

You can also find each bureau online by searching its name and "credit freeze." Be sure you are on the credit bureau's official website. You can lift the freeze when you need to apply for credit.

Ask about possible tax consequences

A fraud can sometimes create tax consequences you may not expect. For example, money stolen from a retirement account may be reported as a distribution even though you never received or benefited from the money.

If money was taken from a retirement account, ask a qualified tax professional whether it was reported as a distribution, what the tax consequences may be, and what, if anything, can be done about them. Don't wait until tax time to ask.

Save everything

Don't delete emails, text messages, voicemails, documents, receipts, or other communications. Write down what happened while you still remember it clearly, including names, dates, amounts, contact information, and how the money was transferred.

Tell someone you trust

Don't try to handle everything by yourself. Tell a family member, friend, lawyer, financial adviser, or someone else you trust what happened.

Another person may see something you don't, ask a question you haven't considered, or simply help you decide what to do next.

If what happened has left you feeling that you don't want to go on, see **Crisis Resources** at the back of the book.

Be especially careful about anyone offering to recover your money

After a fraud, you may be contacted by someone who says they can recover what you lost. They may claim to be an investigator, lawyer, government official, recovery specialist, or someone who has located your money.

They may know details about what happened to you. That does not mean they are legitimate.

Don't send more money because someone promises to recover what you lost. Verify the person and the organization yourself before you agree to anything.

7. WHAT RECOVERY REALLY LOOKS LIKE

Sometimes stolen money can be recovered. Often it cannot.

Whether money can be recovered depends on many things, including how it was sent, where it went, how quickly the fraud was discovered, and whether the money can still be located or stopped.

Some types of payments are easier to reverse or recover than others.

That is why acting quickly matters. There are circumstances in which financial institutions or law enforcement may still be able to stop or freeze funds.

I was fortunate that investigators were able to trace and recover a substantial portion of the money stolen from me in the first fraud. It took months and involved law enforcement in more than one country.

My experience should not suggest that your money will be recovered. If there is a chance to recover some of it, acting quickly may help preserve that chance.

8. BEWARE OF THE SECOND SCAM

I learned about the danger of a second scam the hard way.

After a substantial portion of the money stolen from me in the first fraud was recovered, I was contacted by people who claimed they could help recover more. They knew details about what had happened to me, and I believed them.

I was defrauded again.

Knowing details about what happened to you does not mean the person offering to help is legitimate.

The desire to recover what you lost can be powerful. It was for me. Before you respond to someone offering to help recover your money, involve someone you trust.

9. WHERE TO GO

You don't need to contact every organization on this list. Start with the ones that fit what happened to you.

If money has just been sent:

Contact the bank, brokerage firm, credit-card company, payment service, cryptocurrency exchange, or other financial institution involved immediately. Ask whether the transaction can be stopped, recalled, or frozen.

To report a fraud:

The Federal Trade Commission accepts reports of fraud and scams at **ReportFraud.ftc.gov**.

If your identity has been stolen:

The Federal Trade Commission provides a step-by-step recovery plan at **IdentityTheft.gov**.

To freeze your credit:
Contact Equifax, Experian, and TransUnion. You must place the freeze with each bureau separately. See “Freeze your credit” in Section 6 for telephone numbers.

For internet-related fraud:

Report it to the FBI's Internet Crime Complaint Center at **IC3.gov**.

For investment fraud or a problem involving an investment professional:

The Securities and Exchange Commission provides information and complaint forms at **Investor.gov** and **SEC.gov**. You can file a complaint with FINRA at FINRA.org/complaint. FINRA also operates a Securities Helpline for Seniors at **844-574-3577 (844-57-HELPS).**

If you aren't sure where to begin or simply want to talk with someone:

The AARP Fraud Watch Network Helpline provides free guidance to anyone, whether or not you are an AARP member. Its fraud specialists can help you think through what happened and what to do next. The current number is **877-908-3360**.

If the person exploiting you is a caregiver, family member, or someone in a position of trust:

Adult Protective Services in your state may be able to help.

For local help:

Your state attorney general, state securities regulator, local police department, or other local law-enforcement agency may also be appropriate, depending on what happened.

Websites, telephone numbers, and procedures can change. Check the organization's official website for current information.

10. A FINAL WORD

None of this requires us to stop trusting people. I don't want to live that way.

The most important thing we can protect is our judgment.

REFERENCES FOR THE ANTI-SCAM SURVIVOR'S GUIDE

The information and recommendations in this guide were reviewed against government and other authoritative sources and were current as of October 2026.

Section 1 — Keep This Page Near Your Phone

Federal Trade Commission. "What Are the Signs of a Scam?"
https://consumer.ftc.gov/consumer-alerts/2025/03/what-are-signs-scam

Federal Trade Commission. “Phone Scams.”
https://consumer.ftc.gov/articles/phone-scams

Section 2 — Who Is Doing This

United Nations Office on Drugs and Crime. “Organized Fraud — Issue Paper.”
https://www.unodc.org/documents/organized-crime/Publications/IssuePaperFraud-eBook.pdf

Section 3 — When Someone Contacts You

Federal Trade Commission. “Scammers Use Fake Emergencies To Steal Your Money.”
https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money

Federal Bureau of Investigation. “Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams.”
https://www.fbi.gov/investigate/cyber/alerts/2025/criminals-using-altered-proof-of-life-media-to-extort-victims-in-virtual-kidnapping-for-ransom-scams

Section 4 — Before You Send Money

Federal Trade Commission. “How To Avoid Imposter Scams.”
https://consumer.ftc.gov/features/how-avoid-imposter-scams

Section 5 — Make Yourself Harder to Steal From

Federal Trade Commission. “How To Recover Your Hacked Email or Social Media Account.”
https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account

Cybersecurity and Infrastructure Security Agency. “Require Multifactor Authentication.”
https://www.cisa.gov/secure-our-world/turn-mfa

Consumer Reports. “Who We Are.”
https://www.consumerreports.org/about-us/what-we-do/research-testing/

Cybersecurity and Infrastructure Security Agency. “Require Multifactor Authentication.”
https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication

Federal Trade Commission. “What To Know About People-Search Sites That Sell Your Information.”
https://consumer.ftc.gov/articles/what-know-about-people-search-sites-sell-your-information

Section 6 — If You Think You've Been Defrauded

Federal Trade Commission. “What To Do if You Were Scammed.”
https://consumer.ftc.gov/articles/what-do-if-you-were-scammed

Federal Bureau of Investigation, Internet Crime Complaint Center. “Scammers Impersonating Law Enforcement and Government Officials in Fraud Schemes.” https://www.ic3.gov/PSA/2026/PSA260917

Federal Trade Commission. “Refund and Recovery Scams.” https://consumer.ftc.gov/articles/refund-and-recovery-scams

Federal Trade Commission. “Understanding Your Credit.” Consumer Advice, November 19, 2024.

Section 7 — What Recovery Really Looks Like

Federal Bureau of Investigation, Internet Crime Complaint Center. “Business Email Compromise: The $55 Billion Scam.” https://www.ic3.gov/PSA/2024/PSA240911

Federal Trade Commission. “What To Do if You Were Scammed.” Consumer Advice, June 30, 2026.

Section 8 — Beware of the Second Scam

Federal Trade Commission. “Refund and Recovery Scams.” https://consumer.ftc.gov/articles/refund-and-recovery-scams

Federal Bureau of Investigation, Internet Crime Complaint Center. “FBI Warns of Scammers Impersonating the IC3.” https://www.ic3.gov/PSA/2026/PSA260720

Section 9 — Where to Go

Federal Trade Commission. “ReportFraud.ftc.gov.” https://reportfraud.ftc.gov/

Federal Trade Commission. “IdentityTheft.gov.” https://www.identitytheft.gov/

Federal Bureau of Investigation, Internet Crime Complaint Center. “Internet Crime Complaint Center.” https://www.ic3.gov/

U.S. Securities and Exchange Commission. “Report a Problem with an Investment Account or Financial Professional.” https://www.sec.gov/submit-tip-or-complaint/report-problem-investment-account-or-financial-professional

FINRA. “Investor Contacts.”
https://www.finra.org/investors/investor-contacts

AARP. “Fraud Watch Network Helpline.”
https://www.aarp.org/money/scams-fraud/helpline/

Administration for Community Living. “Supporting Adult Protective Services.”
https://acl.gov/programs/elder-justice/supporting-adult-protective-services