ScamSecurityCheck.com

What To Do If You've Been Scammed

Act fast — the sooner you respond, the better your chances of recovery

Step 1: Protect Your Money

1 Credit or Debit Card

Call the card issuer's emergency number on the back of your card. Report fraud and ask them to reverse the charge and issue a new card immediately.

2 Bank Account or Wire Transfer

Call your bank's fraud department immediately. Ask if they can freeze, reverse, or recall the transfer. Request that they secure all your accounts.

3 Payment Apps (Zelle, Venmo, Cash App, PayPal)

Report the transaction as unauthorized in the app. Also notify any linked bank or card. Each app has a fraud dispute process — use it right away.

Protect Your Money (continued)

4 Gift Cards

Keep the card and receipt. Contact the gift card issuer immediately — tell them it was used in a scam and ask if they can freeze or refund the remaining balance.

5 Cryptocurrency

Contact the exchange you used and report the wallet address you sent to. Recovery is difficult, but they may flag the scammer's account and prevent further fraud.

6 Mailed Cash

Contact the carrier immediately. For USPS, call 1-877-876-2455 to request a package intercept if possible. For other carriers, call their customer service line.

TIME MATTERS: The faster you act, the better your chances.

Many banks can reverse charges within 24-48 hours. After that, it gets harder.

Step 2: Secure Your Identity & Accounts

1 Change Your Passwords Immediately

Start with email and financial accounts — these are the most critical. Then change social media and any other account the scammer might know about. Use strong, unique passwords for each account.

2 Enable Two-Factor Authentication

Turn on 2FA (codes by text message or authenticator app) on every account that supports it. This means even if a scammer has your password, they still can't log in without the code.

3 Freeze Your Credit (If Sensitive Info Was Shared)

If you gave out your Social Security number, date of birth, driver's license, or full banking details, place a fraud alert or credit freeze with all three bureaus: Experian, Equifax, and TransUnion.

4 Monitor Everything for 30+ Days

Watch bank, card, and payment app activity closely for the next several months. Dispute any unfamiliar charges immediately. Set up alerts for all transactions on your accounts.

Step 3: Report It to the Right Places

Reporting may not get money back directly, but it helps investigations and creates a paper trail.

1 Your Local Police Department

File a report to get a report number. This can help with bank disputes, insurance claims, and proving you were a victim.

2 Federal Trade Commission (FTC)

Report at ReportFraud.ftc.gov for most consumer scams. This is the main federal database that tracks scam patterns nationwide.

3 Internet Crime Complaint Center (IC3)

Report at IC3.gov for online or cyber scams. This is the FBI's reporting center for internet-related fraud and cybercrime.

4 Your State Attorney General

Contact your state attorney general's office for state-level consumer protection issues. Search online for your state's consumer complaint form.

5 The Platform Where It Happened

Report the scammer on the platform they used — Facebook, Instagram, dating sites, Etsy, Thumbtack, etc. This helps get their accounts shut down.

Step 4: Watch for Follow-Up Scams

CRITICAL WARNING: After one scam, criminals often try again.

They may sell your info to other scammers or come back pretending to help.
Be extra cautious in the weeks and months after being scammed.

1 Fake Recovery Services

Scammers pretend to be 'recovery agents' who promise to get your money back — for a fee. No legitimate agency charges you upfront to recover stolen funds. This is always a second scam.

2 Fake Law Enforcement Calls

Someone may call pretending to be police, the FBI, or a government agency saying they've found your money or need info to 'process your case.' Real agencies won't call asking for payment.

3 Requests for More Personal Info

Scammers may contact you asking for 'verification' details or remote access to your devices to 'fix' things. Never give additional info to anyone who contacts you unsolicited.

REMEMBER: Legitimate agencies will NEVER ask you to pay to get stolen money back.

They will never demand payment in gift cards, crypto, or wire transfer.

How to File an FTC Report (Step by Step)

Before you start: gather dates, amounts, how you paid, names, and screenshots.

1 Go to ReportFraud.ftc.gov

Open your browser and type ReportFraud.ftc.gov directly (don't click links in emails). On the homepage, click the 'Report Now' button to begin your report.

2 Choose the Type of Scam

The site will ask what your report is about: impersonator, online shopping, tech support, prize/lottery, romance, etc. Click the category that best matches, then click Continue.

3 Enter What Happened

Answer the questions: where it happened (phone, text, email, website), what the scammer said, whether they pretended to be a company, and any info you have about them (names, numbers, URLs).

FTC Report (continued)

4 Add Payment Details

Enter whether you paid money, how you paid (credit card, wire, Zelle, Cash App, gift card, crypto), the total amount, and the dates of payments. Be as accurate as possible.

5 Add Your Contact Info (Optional)

The FTC will ask for your name, address, phone, and email. You can choose how much to share. Giving contact info helps if investigators need more details, but it's not required.

6 Review and Submit

Check your answers for accuracy, especially amounts and contact info. Click Submit. You'll get a confirmation or report number — write it down or save/print the page.

After You Submit:

The site gives next-step tips based on your scam type (contacting your bank, placing fraud alerts, or visiting IdentityTheft.gov for identity theft).

Step 5: Take Care of Yourself

Being scammed is not your fault.

Being scammed is emotionally heavy and very common.
Embarrassment is part of how scammers keep people quiet.
Talk to a trusted friend or family member, especially
if you're unsure what to do next.

Consider contacting a local legal aid or consumer protection nonprofit if the amount is large.

Check Suspicious Messages Free

ScamSecurityCheck.com/scanner

Paste any suspicious message and our AI analyzes it instantly.

Key Phone Numbers & Websites

FTC Scam Reporting: ReportFraud.ftc.gov | 1-800-382-4357
FBI Cybercrime: IC3.gov
Identity Theft Recovery: IdentityTheft.gov
Credit Bureaus: Experian | Equifax | TransUnion
AARP Fraud Watch: 1-877-908-3360
Elder Fraud Hotline: 833-372-8311