How to Protect Yourself After a Scam

Actions to take after a scam to protect your money, personal information, and devices.

IF YOU SENT MONEY

Credit or Debit Card	Contact your bank or card issuer immediately. Report the charge as fraudulent and ask for a refund.
Bank Transfer	Contact your bank immediately. Report the unauthorized transfer and ask them to reverse the transaction.
Gift Card	Contact the company that issued the gift card. Report the scam and ask for a refund. Keep the gift card and receipt.
Wire Transfer	Contact your bank or wire transfer company immediately. Report the fraudulent transfer and ask them to reverse it.
Money Transfer Apps	Report the fraudulent transaction to the money transfer app. If it's linked to a credit or debit card, also contact your bank or card issuer to reverse the charge.
Crypto-currency	Cryptocurrency payments usually cannot be reversed. Report the fraudulent transaction to the exchange or wallet provider and ask them to reverse it, if possible.
Mailed Cash	Contact the delivery company immediately and ask them to intercept the package.

IF YOU SHARED PERSONAL INFORMATION

Social Security Number

Visit IdentityTheft.gov to see what steps to take, including how to monitor your credit.

Username or Password

Create a new, strong password. If you use the same password on other accounts, change it there too.

IF A SCAMMER HAS ACCESS TO YOUR DEVICE

Computer Access

Update your computer's security software, run a full scan, and remove any threats. Change your passwords and protect your personal information.

Cell Phone Number and Account

Contact your mobile service provider immediately. Change your password, check your financial accounts for unauthorized activity, report any fraud, and visit IdentityTheft.gov for recovery steps.

ReportFraud.ftc.gov

This flyer's content is based on FTC guidance.

Recovery Scams

Scammers may offer to "recover" money.

You are not alone. Help is available.

ScamEducation.org
STRONGER AGAINST SCAMS