



The First Hour: What to Do After a Scam

It can happen to anyone. Fast, calm steps make the biggest difference. Work down the list that fits.

If money or payment details were sent

- ☐ Call your bank or card issuer using the number on the back of your card. Ask them to stop or reverse the payment.
- ☐ If you paid with a gift card, call the company that issued the card and ask for a refund.
- ☐ If you gave remote access to your computer, disconnect it from the internet and have it checked.
- ☐ Change the password on any account involved.

If an account was taken over

- ☐ Reset the password from a device you trust, starting with your email.
- ☐ Turn on extra login codes (multi-factor authentication).
- ☐ Check recovery phone numbers, emails, and forwarding rules for changes.
- ☐ Warn friends and family not to trust messages sent from that account.

My numbers

Bank fraud line: _____

Card fraud line: _____

If personal information was shared

- ☐ Social Security number shared: place a free credit freeze at Equifax, Experian, and TransUnion.
- ☐ Follow the recovery plan at IdentityTheft.gov.
- ☐ Watch bank and card statements closely for 90 days.

Within the day

- ☐ Report at ReportFraud.ftc.gov.
- ☐ If money was lost online, report at IC3.gov.
- ☐ Tell your family. Scammers often come back posing as someone who can "recover" your money.
- ☐ Write down what happened while it is fresh: dates, names, numbers, amounts.

A child is being threatened with images? Do not pay. Save the evidence and report to the NCMEC CyberTipline (report.cybertip.org, 1-800-843-5678) and the FBI (tips.fbi.gov). In immediate danger, call 911. For crisis support, call or text 988.