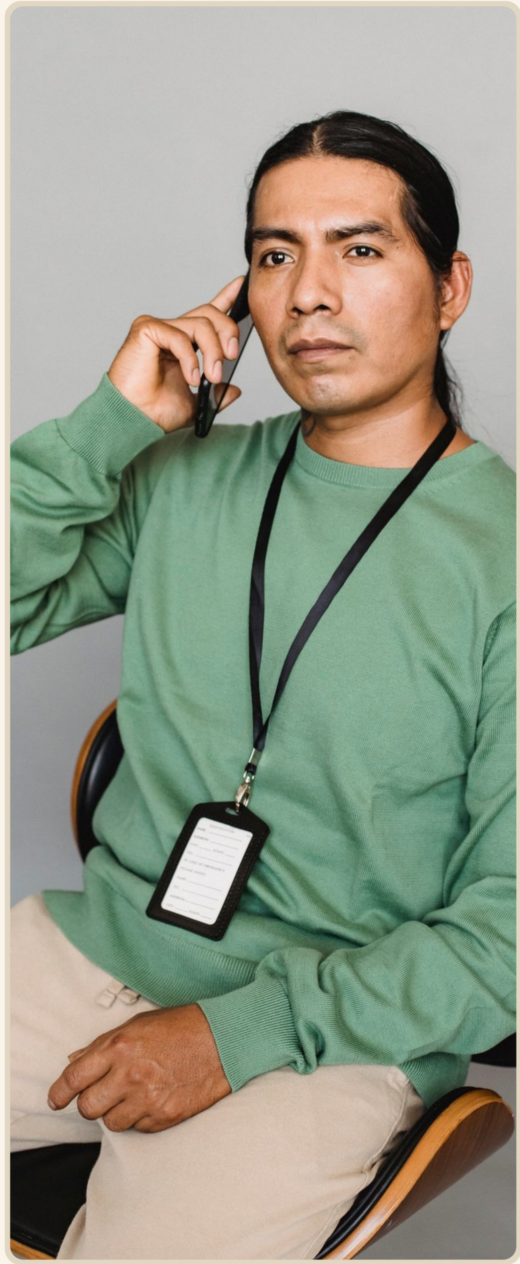
Lumoset

FREE ONLINE-SAFETY EDUCATION

Scammed? Your First 48 Hours

The exact order of steps that gives you the best chance of stopping the damage.

A Lumoset Foundation guide · Part of the free Stay-Safe-Online series



Who it's for: anyone who just realized they've been scammed and needs to know exactly what to do next. **Plain language, no jargon.**

WHAT'S INSIDE THIS GUIDE

Who we are

Lumoset Foundation is a nonprofit that helps everyday people stay safe and confident online. We make clear, plain-language lessons about spotting scams and using technology, and we keep everything 100% free, with no account and no catch. We are a registered 501(c)(3) charity based in Fort Wayne, Indiana.

Why we made this guide

If you've just realized you've been scammed, you are not alone, and it is not your fault. What you do in the next 48 hours matters more than anything else. This guide puts the right steps in the right order, so you don't have to figure it out while panicking.

> **Remember: Speed matters more than perfection. Do the next right step, then the one after that.**

Jump to what you need:

The First Hour: Stop the Bleeding

Do this now

1. Stop all contact with the scammer. Do not explain, argue, or ask for money back.

2. If money is still moving (a payment pending, a check not yet cashed), call your bank's fraud line immediately, the number on the back of your card, not one given by the scammer.

3. If you shared a password, change it right now, on a device you're sure is safe.

The First Day: Lock Down Your Accounts

Do this now

1. Change passwords on any account you shared or that shares a password with the compromised one.

2. Turn on two-factor authentication everywhere you can.

3. If you shared your Social Security number or ID, place a free fraud alert or credit freeze with the three credit bureaus.

4. Check recent bank and card statements for anything else unfamiliar.

Report It (Where, and Why It Matters)

Why it matters. Reporting doesn't just help you, it feeds the data that shuts scam operations down and warns others.

1. IdentityTheft.gov (FTC) — if any personal information was shared; gives you a personal, step-by-step recovery plan.

2. ReportFraud.ftc.gov — for the scam itself.

3. IC3.gov (FBI) — for online/internet-based scams, including crypto.

4. National Elder Fraud Hotline, 833-372-8311 — free help for older adults, including help figuring out next steps, not just reporting.

5. Your local police, especially if you have a specific suspect or in-person contact.

If It Was a Wire, Gift Card, or Crypto Payment

Wire transfer: call your bank immediately; a recall may occasionally still work in the first hours. **Gift card:** call the number on the back of the card or the retailer's fraud line right away; some retailers can freeze an unspent balance if you're fast. **Cryptocurrency:** contact the exchange used immediately; recovery is rare, but reporting still helps investigators trace the wider operation.

> **Remember: These payment methods are hard to reverse, not always impossible. Speed is everything.**

The Days After: Watch for Round Two

What it is. Scammers often sell victim information to each other. A common next move is a fake “recovery service” that promises to get your money back for an upfront fee.

Red flags

• Anyone who contacts you offering to recover money you lost, for a fee, especially if they found you right after you reported the first scam.

Do this now

1. Treat any unsolicited “recovery” offer as a second scam.

2. Legitimate help never charges an upfront fee to return your own money.

Putting It Together

Stop contact, protect what's left, lock down your accounts, report it in the right places, and stay alert for a second scam aimed at you specifically because you were just targeted once.

Keep learning, free.

This guide is a start. Our free course **Spot the Scam · Level 1: Protecting Yourself Online** helps you recognize the next one before it costs you anything.

- **No account. No cost. No catch.** Ever.
- Start anytime at lumoset.org.
- Know someone who was just scammed? Please share this with them.

Key Terms in This Guide

Wire Transfer: A direct bank-to-bank money transfer that lands almost instantly and generally cannot be reversed once sent, which is why scammers frequently request it.

Two-Factor Authentication (2FA): A second login step (a text code, an app, or a fingerprint) beyond your password. The single most effective everyday step against hacked accounts.

Credit Freeze: A free lock you can put on your credit report so no one, including you, can open new credit in your name until you unlock it. The strongest protection after identity theft.

Fraud Alert: A free, lighter-weight flag on your credit report (compared to a credit freeze) that tells lenders to verify your identity extra carefully before opening new credit.

Sources

FTC, IdentityTheft.gov · FTC, ReportFraud.ftc.gov · FBI, IC3.gov · U.S. Department of Justice, National Elder Fraud Hotline (833-372-8311, justice.gov/elderjustice).

Help us reach one more person. Lumoset is a donor-funded 501(c)(3) nonprofit. If this helped you, you can help us teach someone else, free, at lumoset.org. Every gift keeps every lesson free.

Lend a hand. We are volunteer-powered. If you would like to help write, teach, translate, or share our free lessons, see lumoset.org.

For librarians, senior centers, and Area Agencies on Aging: please print and share this guide freely with the people you serve. That is exactly what it is for.

Did this help? Tell us at lumoset.org. Your story helps us reach more people, and shapes what we teach next.