

# What To Do If You've Been Scammed

**Don't be embarrassed.** Scammers are professional liars, and anyone can fall for a scam. Act quickly and get help.

**Don't go through this alone.** Tell someone you trust like a family member or friend. **The AARP Fraud Helpline** offers free advice and support for everyone, not just seniors: **877-908-3360**

**Report what happened.** Even if you can't get your money back, reporting helps law enforcement shut down scams and protect others. Where you report (and what else you need to) depends on what happened. Find your situation below for specific steps:

## What if I gave personal info (SSN, credit card info, bank account info, passwords, etc.) to a scammer?

- Contact your bank/credit card companies immediately and follow their instructions
- Change your passwords—use a different, strong password for each account
- Place a **fraud alert** or **credit freeze** with the major credit bureaus
  - ❑ Equifax: 800-525-6285, equifax.com
  - ❑ Experian: 888-397-3742, experian.com
  - ❑ TransUnion: 800-680-7289, transunion.com
- Visit **IdentityTheft.gov** for a personalized recovery plan from the FTC



## What if I think my account has been hacked?

- Create a new, strong password (different from all your other passwords)
- Turn on two-factor authentication if available
- Report the hack to the company that runs the account
- Notify your bank if payment info was saved in the account
- Monitor your statements for unusual activity

## What if I opened a harmful link or installed bad software (malware)?

- **Cut the connection immediately**—turn off Wi-Fi, enable airplane mode, or unplug ethernet
- Run an up-to-date antivirus scan and follow instructions to remove threats
- Use a **different** device to change passwords for important accounts
- If malware won't go away, you may need to wipe the device (keep backups!)

## What if I gave out a password or security code?

- Change that password immediately—even if you're not sure they used it
- Change it on ALL accounts where you used the same password
- Notify the company that your credentials may be compromised

## What if I lost money to a scammer?

- Report to your bank/credit card company ASAP—they may be able to stop or refund the transaction
- Report to the **FTC** at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov)
- Report to **PA Attorney General**: 800-441-2555 or [scams@attorneygeneral.gov](mailto:scams@attorneygeneral.gov)
- File an **FBI report** at [ic3.gov](https://ic3.gov)

