What to Do After a Scam: Your Quick Checklist

1. Stop Contact

- Hang up if it was a phone call
- Stop replying to texts, emails, or messages
- Don’t engage or argue with the scammer

---

2. Secure Your Accounts

- Change any passwords you shared
- Change passwords on accounts where you used the same password
- If you clicked a suspicious link, don’t use it again — go directly to the real website to update your info (bank, credit card, Amazon, etc.)

---

3. Contact Your Bank or Card Company

- Call the number on the back of your card or use the official app/website
- Tell them you may have been scammed
- Ask to freeze, flag, or monitor your account
- Request a new card or account number if needed

---

4. Write Down What Happened

- How you were contacted

- What they said or asked for
- What info you shared
- When it happened

---

5. Manage Your Feelings

- Remind yourself: this is not your fault
- Don’t blame yourself
- Talk to a trusted person — not for judgment, but for support

---

6. Protect Your Personal Information (If Shared)

- Notify your bank about possible identity theft
- Visit the Social Security Administration’s website if your SSN was exposed
- Place a fraud alert on your credit report with Equifax, Experian, or TransUnion

---

7. What NOT to Do

- Don’t keep engaging with the scammer
- Don’t send more money to “fix” things
- Don’t click on random links in panic
- Don’t dwell on shame — focus on action
