# Scammed Online? Take These 12 Steps Immediately

**1. Secure your devices**

Run antivirus/malware scans, update passwords, and enable two-factor authentication.

**2. Contact your financial institutions**

Notify your bank, credit card providers, and crypto wallet services immediately.

**3. Place a fraud alert**

Contact one of the major credit bureaus:

- Equifax: https://www.equifax.com/personal/credit-report-services/
- Experian: https://www.experian.com/fraud/center.html
- TransUnion: https://www.transunion.com/fraud-alerts

**4. Report identity theft**

Report to the FTC at https://www.IdentityTheft.gov to create a recovery plan.

**5. Report the scam**

File complaints with:

- FBI IC3: https://www.ic3.gov
- FTC: https://reportfraud.ftc.gov
- State Attorney General: https://www.naag.org/find-my-ag/

**6. Secure your email**

Update passwords and enable 2FA. Google recovery: https://accounts.google.com/signin/recovery

**7. Report a stolen driver's license**

Contact your state DMV for a replacement.

**8. Secure your phone number**

Call your carrier to prevent SIM swapping.

**9. File a police report**

Bring evidence such as emails, screenshots, and transaction details.

**10. Report the scam to platforms**

Report scams on Facebook, YouTube, Craigslist, and other sites.

# Scammed Online? Take These 12 Steps Immediately

### 11. Keep records

Save all confirmation numbers, reports, and correspondence.

### 12. Continue monitoring

Check your credit reports and accounts regularly.