AFTER A SCAM: ACT NOW

Use the sections that match what happened - speed matters, but panic does not help

FIRST: Stop communicating with the scammer. Do not pay anyone who promises recovery.

If there is immediate physical danger or a threat of violence, call 911.

MONEY OR PAYMENT SENT

- [ ] Call the bank, card issuer, payment app, gift-card company, or wire service immediately.
- [ ] Say the payment was fraudulent and ask whether it can be stopped or reversed.

PASSWORD, CODE, OR ACCOUNT INFORMATION SHARED

- [ ] From a device you believe is safe, change the affected password and any reused passwords.
- [ ] Start with email, banking, and mobile-phone accounts. Turn on multifactor authentication.

REMOTE COMPUTER OR PHONE ACCESS GIVEN

- [ ] Disconnect the device from the internet. Do not use it for banking or password changes.
- [ ] Have the device checked before reconnecting or using sensitive accounts.

PERSONAL OR IDENTITY INFORMATION SHARED

- [ ] Contact affected organizations directly and follow a recovery plan at IdentityTheft.gov.
- [ ] Review financial statements and consider a credit freeze with all three credit bureaus.

Save evidence and report

Keep messages, receipts, phone numbers, screenshots, and transaction details. Report fraud at ReportFraud.ftc.gov and internet-enabled crime at IC3.gov.

Tell someone you trust. Scammers manipulate normal emotions; asking for help is a protective step.