Before You Pay or Share

Keep this sheet near your phone or computer. Use it for unexpected calls, texts, emails, mail and visitors.

PAUSE

Stop the conversation. Do not click a link, send money, install software or give someone control of your device.

VERIFY

Call the person or organization using a number you already trust, such as the number on your bank card or statement. Do not use the number or link in the suspicious message.

INVOLVE

Talk to a trusted person before acting. If your first contact is unavailable, call your backup.

Watch for these warning signs

"Act now." "Do not tell anyone." "Move your money to protect it."
"Buy gift cards." "Send cryptocurrency." "Read me your login code."

Caller ID, logos, names and even a familiar voice can be faked. Do not give passwords, one-time login codes, Social Security or Medicare numbers to an unexpected contact.

Use this response

"I do not make payments or share information during unexpected calls. I will hang up and check this myself."

My trusted contacts

First contact _____ Phone _____

Backup contact _____ Phone _____

Bank fraud number from my card _____

Agree together: We will check unexpected payments and requests for private information with a trusted person first. Never write passwords, PINs or account numbers on this sheet.

If a Scam May Have Happened

Tell someone promptly. You deserve help without blame.

1 Stop contact and further payments

Do not respond again. Do not pay someone who promises to recover the money for a fee. If someone has remote access, disconnect the device from the internet and get trusted technical help.

2 Call the bank or payment provider now

Use its official number. Explain what happened and ask whether the payment can be stopped or reversed and the account protected. For gift cards, contact the card issuer and keep the cards and receipts. Recovery is not guaranteed.

3 Save evidence and secure accounts

Save messages, receipts, phone numbers and transaction details. If a password was exposed, change it and any reused passwords from a trusted device. Enable multifactor authentication. If remote access was allowed, have the device checked before using it for sensitive tasks.

4 Get reporting and recovery help

ReportFraud.ftc.gov - report scams to the FTC.
IdentityTheft.gov - help if personal information was stolen or misused.
National Elder Fraud Hotline: 833-372-8311
For financial fraud involving adults 60 and older; caregivers can call for guidance. Monday-Friday, 10 a.m.-6 p.m. Eastern, except some holidays. The hotline helps with reporting; it does not investigate or guarantee refunds.
Contact local police for theft or threats. Call **911** for immediate danger.

Caregiver setup checklist

[ ] Save genuine bank, family, insurance and support numbers.
[ ] Agree on a primary helper and a backup; respect the person's choices.
[ ] Set transaction alerts and review statements together with permission.
[ ] Turn on device updates; use unique passwords and multifactor authentication.
[ ] Discuss call filtering; check voicemail for genuine callers.
[ ] Keep account access within your permission or legal authority.

A helpful first response: "Thank you for telling me. Let us work on the next step together."

Official resources checked October 10, 2026: FTC consumer guidance and DOJ National Elder Fraud Hotline. Household checklist is a suggested care plan.

consumer.ftc.gov/articles/what-do-if-you-were-scammed
consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money
consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams
ovc.ojp.gov/program/stop-elder-fraud/faqs

Spot the Warning Before You Tap

Look at the sender, subject and preview first. These are fictional scam examples, shown as inbox and notification previews.

EMAIL INBOX PREVIEW

Bank Security 9:41 AM

URGENT: Account locked - act within 30 minutes 1

Preview: Confirm your password and login code to 2

restore access. Tap the link to avoid suspension...

1 Pressure to hurry. A threat and deadline push you to act before checking.

2 Password or code request. An unexpected request for login details is a serious warning sign.

TEXT NOTIFICATION PREVIEW

Messages now

+1 (202) 555-0146

Postal Service: Your package cannot be delivered.

Pay $1.25 now to reschedule: 3

https://delivery-fee.example/pay 4

3 Unexpected fee. A small charge can bait you into giving up card details.

4 Unfamiliar web address. A delivery claim and a strange payment link are reasons to stop. Do not tap to investigate.

A professional look does not prove it is real

A familiar sender name, good spelling, your name or a padlock can appear in scams. The full sender address may be hidden until you open details. Previews vary; you may not see every clue.

SAFER NEXT STEP

Leave the message alone. Open the company app yourself or call the number on your card or statement. Do not reply, open attachments or use the message link.

Sources: consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams; ftc.gov/textscams.
Fictional .example address. Printed links are not clickable.