



SPOT THE PRESSURE. TAKE BACK TIME.

Scammers impersonate people you trust and use urgency or fear to stop you checking. Use this with the one-page Suspicious Message? Quick Guide.

DO NOT PAY BECAUSE AN UNEXPECTED CONTACT PRESSURES YOU

Do not send money to stop an arrest, protect savings, pay a ransom, or help a relative you have not verified. Never use gift cards, cryptocurrency, wire transfers, payment apps, or cash drops under pressure.

RED FLAGS ACROSS MANY SCAMS

- ☐ They demand immediate action or tell you to keep it secret.
- ☐ They ask for money, a password, a verification code, or remote access.
- ☐ They say not to call your bank, family, police, or another trusted person.
- ☐ They want payment by gift card, crypto, wire, payment app, or cash.

PAUSE AND VERIFY

- ☐ End the call or stop replying. Do not use links or numbers they sent.
- ☐ Call the organization using a number or website you already know is real.
- ☐ If a relative is supposedly in danger, contact them directly at a saved number.
- ☐ If you cannot reach them, contact another family member or trusted person.

MAKE A FAMILY CHECK-IN PLAN

Choose a family code word and agree to verify emergencies by calling a known number or another relative. Caller ID, a familiar voice, and urgent photos or videos are not proof on their own.



ROMANCE AND ONLINE INVESTMENT SCAMS

A person you meet online may build a close relationship before asking for money or steering you to an investment.

NEVER SEND MONEY OR GIFTS TO AN ONLINE LOVE INTEREST YOU HAVE NOT MET IN PERSON

Do not send money, gift cards, cryptocurrency, or account details. A request to invest through a platform they recommend is also a major warning sign.

HOW THE STORY MAY SOUND

- ☐ They quickly move the chat off a dating or social platform.
- ☐ They say they live or work far away and cannot meet in person.
- ☐ They need help with travel, medical bills, a visa, or an emergency.
- ☐ They offer to teach you how to invest in crypto, stocks, or forex.

WARNING SIGNS

- ☐ The relationship becomes intense very quickly.
- ☐ They repeatedly cancel plans to meet or video chat.
- ☐ They ask you to keep the relationship or money request secret.
- ☐ A trading site shows growing profits but requires more deposits to withdraw.

WHAT TO DO

- ☐ Stop sending money and do not install an app they recommend.
- ☐ Talk to someone you trust before making a financial decision.
- ☐ Search the person's job or story with the word scam; reverse-search photos.
- ☐ Report the profile to the dating or social platform.

IF YOU PAID OR SHARED DETAILS

- ☐ Contact your bank, card issuer, payment app, or crypto exchange now.
- ☐ Ask whether the payment can be stopped and the account secured.
- ☐ Report the scam to [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).
- ☐ For online-enabled fraud, file a report at [ic3.gov](https://www.ic3.gov).



FAMILY EMERGENCY / KIDNAPPING SCAM

A caller may claim a relative was arrested, hurt, or kidnapped and demand money before you can check on them.

DO NOT SEND A RANSOM OR EMERGENCY PAYMENT BEFORE VERIFYING

Scammers rely on panic and may keep you on the phone so you cannot reach your family. A familiar voice or urgent photo can be faked or altered.

WHAT YOU MAY HEAR

- ☐ A panicked person says they are your child, grandchild, or another relative.
- ☐ A second caller claims to be a kidnapper, lawyer, officer, or hospital worker.
- ☐ They demand money for bail, medical care, release, or safe return.
- ☐ They may send a photo or video as supposed proof the person is held.

PRESSURE TACTICS

- ☐ They tell you to stay on the phone and not call anyone.
- ☐ They demand a fast wire, crypto, gift card, cash drop, or app payment.
- ☐ They may know a name or detail from social media or public sources.
- ☐ They discourage you from contacting police or other family.

CHECK THAT YOUR FAMILY IS SAFE

- ☐ Do not say the relative's name or reveal extra family details.
- ☐ Hang up or use a second phone to call the relative at a saved number.
- ☐ If they do not answer, contact another relative, friend, or trusted person near them.
- ☐ Use a family code word if your family has already agreed on one.

IF THE THREAT MAY BE REAL

- ☐ Do not meet or hand over money to the caller.
- ☐ If you cannot verify the person's safety and have a credible threat, call 911 or local police.
- ☐ Preserve numbers, messages, voice mails, payment demands, and times.
- ☐ Report the extortion to the FBI at ic3.gov and the FTC.



ARREST AND WARRANT IMPOSTER SCAMS

Scammers may claim to be police, a court, a federal agency, or a government employee to frighten you into paying or moving money.

A CALLER CANNOT MAKE YOU PAY TO AVOID AN ARREST BY GIFT CARD, CRYPTO, WIRE, OR APP

Real law enforcement will not text or email you an arrest warrant. Courts and government agencies do not demand payment over the phone or tell you to move money to 'protect' it.

WHAT THE SCAM MAY INCLUDE

- ☐ A claim that you missed jury duty, owe a fine, or have a warrant.
- ☐ A caller ID that appears to show a police department or agency.
- ☐ A badge number, employee ID, official-sounding name, or fake warrant.
- ☐ A threat of arrest unless you pay immediately or keep the call secret.

WHAT MAKES IT SUSPICIOUS

- ☐ They insist you must pay during the call or message.
- ☐ They tell you to buy gift cards, send crypto, wire money, or use an app.
- ☐ They ask you to withdraw cash or transfer funds to a 'safe' account.
- ☐ They say not to hang up or contact a real court, agency, or family member.

WHAT TO DO

- ☐ Hang up. Do not reply to the text or open its links or attachments.
- ☐ Do not give money, banking details, passwords, or verification codes.
- ☐ If concerned, contact the court or agency through its official website or published number.
- ☐ Ask a trusted person to help you verify before taking action.

REPORT IT

- ☐ Report the impersonation to [ReportFraud.ftc.gov](https://reportfraud.ftc.gov).
- ☐ Contact your local court or agency using independently found contact details.
- ☐ Report online messages or payment requests at ic3.gov.
- ☐ If someone is at your door or you face an immediate threat, call 911.



FAKE ALERTS, SUPPORT, AND DELIVERY

A message or pop-up may pretend to be a bank, retailer, delivery company, toll agency, or tech support provider.

COMMON VERSIONS

- ☐ A fake bank alert says to click a link or share a login code.
- ☐ A pop-up says your device is infected and tells you to call a number.
- ☐ A delivery or toll text claims a fee is due and links to a payment page.
- ☐ A fake support agent asks to control your device or install software.

RED FLAGS

- ☐ The message is unexpected and creates urgency or fear.
- ☐ The link opens a look-alike website or asks for card details.
- ☐ A caller requests your password, one-time code, or remote access.
- ☐ They ask you to pay with gift cards, crypto, wire, or a payment app.

VERIFY AND PROTECT YOURSELF

- ☐ Do not tap links, call the number, or open attachments in the message.
- ☐ Check the account in its official app or use the number on your card.
- ☐ Check delivery status in the retailer's or carrier's official app/site.
- ☐ Never share login codes or give an unsolicited caller device access.

REPORT AND RECOVER

- ☐ Report suspicious texts in your messaging app or forward them to 7726.
- ☐ Report scams at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud); report online fraud at [ic3.gov](https://www.ic3.gov).
- ☐ If you shared a password, change it on the official site and enable MFA.
- ☐ If you paid, contact your bank or payment provider immediately.

CLICKED A LINK OR ALLOWED DEVICE ACCESS?

Do not enter more information. If you installed software or allowed remote access, update security software, run a scan, and seek help from a tech support source you know and trust.



IF YOU ALREADY PAID OR SHARED INFO

You are not alone, and acting quickly may help limit further loss. Do not pay anyone who promises guaranteed recovery.

STOP CONTACT AND DO NOT SEND MORE

End the conversation. Do not pay a 'refund agent,' investigator, or recovery service that contacts you unexpectedly and promises to get your money back.

CONTACT THE PROVIDER NOW

- ☐ Call your bank, card issuer, payment app, wire service, or crypto exchange using an official number.
- ☐ Say you were scammed and ask whether the payment can be stopped or reversed.
- ☐ Ask the provider to secure the account and review recent transactions.
- ☐ For a gift card, contact the issuer and keep the card and receipt.

SECURE YOUR IDENTITY AND ACCOUNTS

- ☐ Change any shared password and any other account using that password.
- ☐ Turn on multifactor authentication and follow official account-recovery steps.
- ☐ If your Social Security number was exposed, use [IdentityTheft.gov](https://www.identitytheft.gov).
- ☐ Tell a trusted person and ask them to help you make a recovery plan.

KEEP USEFUL RECORDS

- ☐ Save texts, emails, call logs, usernames, website addresses, and screenshots.
- ☐ Keep receipts, gift cards, transaction IDs, wallet addresses, and account notices.
- ☐ Write down dates, times, payment methods, amounts, and what was said.
- ☐ Do not delete relevant messages before preserving a copy.

WHERE TO REPORT

- ☐ FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) for scams and impersonation.
- ☐ FBI IC3: [ic3.gov](https://www.fbi.gov/intercept) for online-enabled fraud and extortion.
- ☐ Local police: contact them about threats, theft, or a possible real emergency.
- ☐ Call 911 for immediate danger or a credible, active threat.

KEEP THE NEXT STEP SIMPLE

Contact the affected provider, preserve what happened, and make a report. Reporting does not guarantee a refund, but it can help the right organizations understand and respond to the fraud.