

Stay Safe and Be Aware of Mobile Scams

Financial scams can happen any time. Use this guide to have conversations with family and friends about how to proactively protect against scams, texts and calls.



(Un)Official Caller

What would you do if you get a call that appears to be from your bank, law enforcement or a company you may know and you are asked to send money or provide sensitive information?

Have this Conversation

Don't answer unless you are expecting a call. If an organization is making a legitimate call, such as your bank, law enforcement or insurance company, they will usually contact you via mail and/or leave a voice mail. Numbers displayed on your device may be spoofed to make you think the call is coming from a legitimate source.

If it appears to be legitimate, look up the company's number to verify that you are calling the correct organization. Scammers may provide a phone number for you to call back, but these numbers will be routed to an imposter's call center.

Don't provide sensitive information such as your social security number or bank account information, unless you have confirmed you are speaking to a legitimate company. You can find the organization's contact information by looking it up on the company's official website. Never provide your passcode or access codes to anyone.

Do not send money to anyone you do not know personally. Scammers may ask you to provide cash, gift cards, access to your bank account, send or invest in cryptocurrency, or use a peer-to-peer payment app. These are red flags that you are being scammed.

What to do

Do not answer the call. Saying just a few words such as "yes" or your name gives the scammer enough of a voice sample to impersonate you.

If the caller is a suspected scammer:

- Report the call as junk or spam.
- Block the number. Refer to your mobile device provider's instructions.
- Delete the number.



Payments
Innovation Alliance®



Have this Conversation

With artificial intelligence, they could record your voice then try to impersonate you.

What to do

- If the caller is a suspected scammer, do not answer the call. Saying just a few words such as “yes” or your name gives the scammer enough of a voice sample to impersonate you.
- Report the call as junk or spam.
- Block the number. Refer to your mobile device provider’s instructions.
- Delete the number from your received calls to prevent an accidental call-back.



What would you do if you got a text message from someone you don't know? For example, "When are we meeting for lunch tomorrow?" or "I just got a new phone and lost my contacts. Who is this?" or simply "Hi!" or "Have a great day!"

Have this Conversation

Don't respond. Once you send a text back with a message like "Who is this?" or "Sorry, wrong number," the scammer tries to pull you into a friendly conversation, which is the start of the scam.

The conversation is a ruse designed to get you to let down your guard or try to establish an emotional connection so you will be more susceptible to falling for their scam.

What to do

- Forward the scam text to 7726. The major carriers use this information to report and block similar messages.
- Report the text as junk or spam.
- Block the number. Refer to your mobile device provider's instructions.
- Delete the text.



A Program of

Nacha