Help to protect yourself from the latest scams.

Scammers use different tactics to get victims to fall for their schemes. In some cases, they can be friendly, sympathetic and seem willing to help. In others, they use fear tactics to persuade victims. Being vigilant is your first line of defense. Review the following types of scams and learn how to better protect yourself.

Issues with package delivery

You receive an email or text indicating there's an issue with your package or a failed delivery attempt. You'll be asked to click a link to pay a small fee or provide personal information.

Tip: Do not open unfamiliar links for payment or personal information, this may be a phishing attempt. Read more about phishing.

Donating money to a cause

Use caution if asked to donate money in person, to a cause, using your phone. You'll be told to log into your banking app but then told to hand over your phone for the “representative” to input the charity's information and complete the transaction for you - but the scammer is sometimes actually sending money to themselves.

Tip: Don't hand over your device to anyone to complete a transaction and never ignore bank warning messages.

Social Media

Cyber criminals are actively using social media platforms and design posts that lure you into sharing personal information or scam you out of money.

Tip: Be mindful about what information you share and see on social media. If something seems too good to be true, its most likely a scam. Read about social media scams.

Imposter

Scammers may pose as businesses or people you know — like your bank, utility company, phone provider or even a friend or relative. They'll spoof legitimate phone numbers to call or text and tell you to send funds to yourself or others using online or mobile banking. They may even tell you to ignore or bypass scam warnings and alerts. If you share information, the scammer could enroll in bank features like Zelle using your information.

Tip: Stop and verify. While Bank of America may send you a text to validate unusual activity, we will never contact you to request you share a code over the phone or send us or anyone else money, including through Zelle. Read about social engineering.

Multi-step scams

Scammers are now combining multiple scam types by taking a phased approach to try to gain your trust and make scams even more convincing.

- Step 1 - you'll receive a request for remote access on your device.
- Step 2 you'll get a call from your bank stating there is an issue or potential fraud.
- Step 3 another imposter claiming to be a government official will send you an official email or letter.

Tip: Don't download software or provide remote access to anyone you don't know. Bank of America will never call you to request that you move money to protect yourself from fraud.

Read our tip sheet on talking to friends and family about fraud, scams and cyber security, and read on to review more scams and learn how to help better protect yourself.

Online sales scams, Real estate scams, Investment scams
Romance scams, Technology scams, Compromise scams
Natural disaster scams

Know the red flags

No matter which technique the scammers use, the red flags remain the same. You may be:

- Contacted unexpectedly by phone, email, text, direct message or pop-up with a request for personal information or money. Never click a link or download an attachment from someone you don't know. Bank of America will never text, email or call you asking for personal or account information.

- Pressured to act immediately with an alarming phone call, email or text that plays with your emotions. Scammers may pose as an employee from a familiar organization, such as Bank of America and say there's a problem that needs immediate attention. Do not act unless you have verified the person who has contacted you and the story or request is legitimate.

- Asked to pay in an unusual way, like gift cards, bitcoin, prepaid debit cards or digital currency, including Zelle® to resolve fraud. Bank of America will never ask you to transfer money to anyone, including yourself and will never ask you to transfer money because we detected fraud on your account.

- Asked to provide personal or account information, such as an account verification code, bank account number or PIN. When in doubt, don't give it out. Bank of America will never text, email or call you asking for an account authorization code.

- Offered a free product or 'get rich quick' opportunity that seems too good to be true. If something sounds too good to be true, it probably is. Never cash a check for someone you don't know.

If you authorize a transfer or send money to a scammer, there's often little we can do to help get your money back.