Together, we can help protect your money

STOP | VERIFY | PREVENT | PROTECT

Stopping scams is everyone's responsibility. Together, we can help keep your accounts protected.

We continuously monitor your transactions for suspicious activity and share resources to inform you about trending scams and steps you can take to help protect yourself. It's a partnership between you and Bank of America.

If you send money to a scammer, there is little we can do to get your money back.

Imposters are real, but their requests are not. Don't be fooled, no matter how "real" or how "urgent" they seem. Their goal is to deceive, yours is to detect — and to protect.

STOP

Don't let anyone rush you. If someone asks for money or personal info and it feels "off," it probably is. Trust your instincts and don't engage with them.

VERIFY

Even if the request appears legitimate, talk it over with someone you trust, like a friend or family member. You can call back using trusted and known numbers, such as those listed on the back of your debit or credit card or on your statement. Remember: Bank of America will not reach out and ask for personal information or codes with a request to withdraw, send or move money.

PREVENT

Knowing the signs of a scam and sharing them with family and friends can build community awareness. Help others stay alert and avoid scams by spreading the word.

PROTECT

Don't reuse passwords or PIN numbers for multiple accounts. Create complex passwords. Use two-factor authentication and biometrics that put additional steps between someone and your account access.

"They said my bank account was compromised and to not trust the manager since they were 'in on it.'"

"They said they were the bank's fraud team and needed access to my online banking to prevent a fraud attack."

"They told me to pay with gift cards."

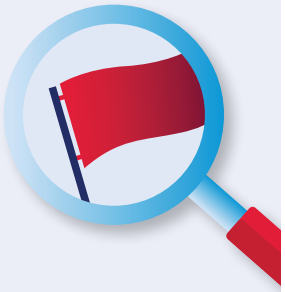
"They said I had to give them my password and PIN number."

"They told me I needed to transfer money to resolve fraud."

To learn more about scams, talk to an associate or visit our Security Center at BofA.com/HelpProtectYourself.

For the latest tips, just ask Erica®, your virtual financial assistant[1] in the Mobile Banking app[2]: "Learn about scams."

BANK OF AMERICA



Watch for the red flags

Surprise! An unexpected call, text, email or social media message can catch you off guard. Be aware of common scam tactics. They change all the time, but the red flags remain the same. Even if a story makes sense, verify the information through a trusted source.

FALSE URGENCY

Scammers may say there's a problem that needs your immediate attention. They want you to act before you think, so they'll rush you into making hasty decisions. Slow down and consult with a friend or family member.

EMOTION

Scammers use stories to make you feel fear, greed, sympathy or love and urge you to ignore your instincts or lie about why you're moving money.

IMPERSONATION

They'll pretend to be an official, company representative, bank, or even a friend or family member.

DECEPTION

You may be instructed not to trust Bank of America, told to ignore warning messages or coached on what to say — including to lie.

REWARDS OR THREATS

They may offer money, a job, a prize, make claims of an emergency, or threaten you with legal action or notifying law enforcement.

UNUSUAL PAYMENTS

Scammers may tell you to send money or payment in a less common way, such as a wire transfer, gift cards, non-traditional forms of payment like gold or cryptocurrency, or pre-loaded debit cards.

VERIFICATION CODES

Scammers may try to "confirm" your identity with a verification code that appears to come from your bank, but was triggered by the scammer. It's a red flag if they called you.

To learn more about scams, talk to an associate or visit our Security Center at **BofA.com/HelpProtectYourself**.

For the latest tips, just ask Erica®, your virtual financial assistant[1] in the Mobile Banking app[2]: "Learn about scams."

Stay scam smart

Here are some trending scams to look out for.

Online and social media offers	Social media is a leading starting point for fraud and scams. Before you buy from a post or ad, check who's behind it and use secure checkout on trusted sites. If it sounds unbelievable, it probably is!
Ticket sales	Going to the big game or hottest concert? Don't let your enthusiasm get the better of you. Scammers prey on excited fans by selling fake tickets, stealing credit card information, overcharging for the cheap seats and leaving you out in the cold.
Imposter	Imposters may pose as a trusted figure. They claim there's an issue and urge you to act quickly to resolve it. Today, bank impersonation scams are very popular. Verify you're speaking with your financial institution by calling the number on the back of your credit or debit card or published on their official web site.
Text	Never click on links or call phone numbers in unexpected texts or emails. Messages about "unpaid tolls" or "package delivery attempts" are usually scams. That unexpected "hi" from an unknown number is often a scammer attempting to establish contact.
Fake tech support	Don't grant access to your computer or devices. You could reveal personal information and lose money.
Get rich quick	The old saying is, "If it seems too good to be true, it is." Always research investment opportunities before sharing information or committing money. Speak to a trusted and accredited financial advisor first.
Rental and real estate	Imagine showing up to your new home or dream vacation only to find out it doesn't exist, or that you've been double booked! Scammers may create fake listings to steal your information and your money.

At Bank of America, we're committed to helping you stay informed and protected against scams. Staying alert is your best defense. Remember these tips so you'll know what to do when you receive a suspicious message or request.

To learn more about scams, talk to an associate or visit our Security Center at **BofA.com/HelpProtectYourself**.

For the latest tips, just ask Erica®, your virtual financial assistant[1] in the Mobile Banking app[2]: "Learn about scams."

Stay scam smart (continued)

Here are some trending scams to look out for.

Travel	Travel scams often use "too-good-to-be-true" deals, urgent pressure to pay, look-alike websites, or requests to move messaging and payment off trusted platforms—if it feels rushed or unusual, it's a red flag! Check reviews and book on official websites before purchasing.
Email (phishing)	Scammers use fake email addresses that closely resemble real ones. They might create a sense of urgency or redirect upcoming payments to a fraudster. Always verify any payment request directly with the sender through a trusted method.
Youth and elder adult	Be cautious! Scammers may impersonate family members or influencers to gain your trust and try to steal your information and money. Consider creating a family password or phrase to prove identity.
Overpayment	If someone offers to send you money but requests that you return extra funds, be skeptical. Be wary if a company claims they mistakenly deposited money or the incorrect amount into your account and asks for it back. This is a common tactic of scammers.
Expedited enrollment	Scammers may impersonate transportation officials by claiming they can expedite enrollment or renew your application for travel benefits for an additional fee.
Romance	Fraudsters build emotional relationships online to gain trust and request money. Prevention tip: Never send money to someone you haven't met in person. Be cautious of urgent financial requests.
Crypto ATM	Scammers pose as officials or companies and create fake emergencies. They may rush you to withdraw cash and deposit it into a crypto ATM and your money may be gone instantly. No government agency or bank will ever request crypto payments.

At Bank of America, we're committed to helping you stay informed and protected against scams. Staying alert is your best defense. Remember these tips so you'll know what to do when you receive a suspicious message or request.

To learn more about scams, talk to an associate or visit our Security Center at **BofA.com/HelpProtectYourself**.

For the latest tips, just ask Erica®, your virtual financial assistant[1] in the Mobile Banking app[2]: "Learn about scams."

If you suspect fraud or if you've been contacted by scammers, contact us immediately at one of the phone numbers listed below.

Deposit Accounts, Debit Cards, Checks and Zelle®, including lost or stolen debit cards or checkbooks: 800.432.1000

Consumer Credit Card: 800.421.2110

Wire Transfers: 877.337.8357 in the U.S. From outside the U.S. contact us at 1.302.781.6374

Home Loans: 800.669.6607

Home Equity Line of Credit (HELOC): 800.934.5626

Auto Financing: 800.215.6195

For the latest information on scams and how to help protect your money, visit our online resources below.

Bank of America Scam page
Links to: **BofA.com/HelpProtectYourself**

Bank of America Fraud page
Links to: **bankofamerica.com/security-center/bank-fraud-prevention/**

Online Banking Security Center
Links to: **bankofamerica.com/security-center/online-banking/**

To learn more about scams, talk to an associate or visit our Security Center at **BofA.com/HelpProtectYourself**.

For the latest tips, just ask Erica®, your virtual financial assistant[1] in the Mobile Banking app[2]: "Learn about scams."

[1] The mobile feature, Erica, is only available in the English language. The feature requires that you download the latest version of the Mobile Banking app and is only available in the Mobile Banking app for select iOS and Android devices. Message and data rates may apply. Your chat may be recorded and monitored for quality assurance. For SafeBalance Banking® for Family Banking accounts, the parent owner and their child age 13 or older have access to Erica.

[2] Mobile Banking requires that you download the Mobile Banking app and is only available for select mobile devices. Message and data rates may apply.

BANK OF AMERICA