Check out these trending scams

Imposter scams

"Your package was returned, and you need to reschedule your delivery"

How it works:

Initial Contact: You receive a communication about an issue - it may be with a delivery, your account, a family member or a device.
Deceptive instructions: You may be urged to provide information such as a code, or take an action such as provide remote access, move money to another account or digital wallet, ***ignore warning messages or input *72 or **21 in the phone.***
The scammer wins: After following the instructions, the scammer now has access to your money, and it's unlikely you'll see your money again.

Help protect your money – pause, verify, help prevent scams
Banks will never ask you to take these actions. Verify all requests for information or money. Talk to your friends and family about the tactics scammers use.

Investment Scams

"***They guaranteed a quick return on the investment, and I was receiving those returns in the beginning***"

How it works:

Initial Contact: The scammer will reach out through social media, text or email with a unique investment opportunity or a chance to ***get rich quick.***
Deceptive instructions: You'll be convinced to invest your money and will start to receive small returns.
Fake returns: You're then encouraged to invest larger sums of money based on the returns you are receiving but ***suddenly all communications stop***.

Help protect yourself and your money
Always validate investment opportunities. Use caution if asked to provide personal or financial information, ***especially if asked to send money through digital currency or instant money transfers***.

Tech support scams

"***They needed remote access to remove a virus from my device***"

How it works:

Initial Contact: Scammers reach out, via computer pop-up or phone call, claiming there is an issue with your device.
Deceptive instructions: You are instructed to ***provide remote access to the device and to download an app to fix the issue.***
Access to personal information: Once you grant remote access or download the app, ***the scammer has access to your personal information. They can install malware*** on your device and demand a payment before they give back your access.

Help protect yourself and your money
No matter the reason given, ***be cautious about granting device access or downloading unfamiliar apps*** to fix issues with your devices. Run a full system virus and spyware scan and power off the device. Read more about tech scams.

Online sales

"***I thought I'd scored really hard-to-get tickets***"

How it works:

Initial Contact: Scammers create ***a fake website or post a "great deal***" on social media for an item you're had your eye on.
Deceptive instructions: They ask you to ***pay in less common ways such as cash, gift cards or wire transfers***.
Pressured to act: You'll be ***pressured to act quickly*** so you don't miss out on the deal.

Help protect yourself and your money

Slow down and use caution if pressured to act quickly. Research the seller and products independently, check reviews for possible scam notices. Most online promotions that sounds too good to be true - typically are.

Know the red flags that signal a scam

Scammers are constantly reinventing new ways to trick people. While their stories may change, their tactics remain the same. Being aware of these red flags should make you pause, verify, and help stay protected:

Read how to stay safe from Cybercrime layer

Beware of the following RED flags

- **Contacted unexpectedly** by phone, email, text, direct message or pop-up with a request for personal information or money. Banks will never text, email, call, or visit you at your home asking for personal or account information. Remember, never click a link or download an attachment from someone you don't know.
- **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 banks can do to help get your money back.