Find out how to protect yourself from identity theft.

Identity (ID) theft

ID theft occurs when someone gains access to your personal information such as name, date of birth and Social Security number (SSN) and uses that information to commit fraudulent acts.

Know the warning signs

Knowing what to look out for can help prevent fraud sooner:

- You notice unauthorized activity on your bank account or spot new accounts on your credit report.
- You receive communications about an issue with your taxes, or about a debt that you don't owe.
- You're alerted that your account was accessed from a new device you don't recognize.
- You're unexpectedly denied credit.

Help protect yourself

ID theft can happen to anyone but taking these steps will help reduce the risk of becoming a victim:

Keep your personal information secure

- Never give out your personal information via email, text or to an unsolicited caller.
- Switch to paperless statements and shred documents, such as tax forms, bank statements and medical bills that contain sensitive information.
- Avoid carrying your Social Security Number in your wallet and give it out only when necessary.
- Don't overshare on social media, and use privacy controls so that personal information is not made public.

- Discuss internet safety with your children, and prevent them from sharing information online without your permission.

Monitor your accounts and credit reports

- Regularly review bank statements to ensure there's no unauthorized transactions on the accounts.
- Review your credit reports and look for any accounts that you do not recognize.
- Consider freezing your credit with all three bureaus to help limit access to your credit reports and prevent unauthorized new accounts from being opened using your information.

Protect your devices

- Keep all of your devices updated with the latest browser, operating system and antivirus software.
- Secure your devices and home Wi-Fi network with a unique password of at least eight characters.
- Enable biometrics such as fingerprint sign-on, and retina or facial recognition where available.

Control access to your accounts

- Create a strong password for each of your accounts, and never reuse the same password on multiple websites.
- Use multifactor authentication to add an extra layer of protection when signing in to your accounts.
- Activate account alerts to help you monitor your finances and keep your accounts safe. See how to manage your alerts.
- Make sure your phone number and email address are up to date on your financial accounts so you can be contacted if anything looks suspicious.
- Consider using a digital wallet on your phone which is a fast, secure way to make in-store, in-app or online purchases. Learn how to enroll in a digital wallet.
- Take all these actions by logging into Mobile or Online Banking Security Center and checking your security level. You'll see it rise as you take the actions and help protect your accounts against fraud.

If you become a victim, act quickly and take the following actions:

- **Check your credit report** to make sure there are no other accounts you're not aware of that have been opened in your name. Visit annualcreditreport.com or call 877.322.8228 to obtain a credit report.
- **Contact any of the credit reporting agencies** to place a fraud alert on your file:
  - **Experian:** Experian.com or 888.397.3742
  - **TransUnion:** TransUnion.com or 800.680.7289
  - **Equifax:** Equifax.com or 888.766.0008
- **Freeze your credit.** Place a credit freeze (security freeze) with all three bureaus to help limit access to your credit reports and prevent unauthorized new accounts from being opened using your information.
  - Once you freeze your credit, you'll need to remove the freeze when applying for a new account.
  - You can lift or suspend the freeze temporarily or permanently. Check with each credit bureau regarding their specific process.
- **Contact your financial institutions** and creditors to speak with the fraud department and tell them your identity may have been compromised. Report Suspicious Activity
- **Consider changing your logins and passwords** to help better protect your accounts.
- You may choose to also **file a report with your local law enforcement**.

Learn how cyber criminals try to trick you into revealing your personal information

Be cyber secure: Smishing

Smishing is a way that cyber criminals will try to trick you into revealing confidential or sensitive company information. Smishing occurs when text messages or other messaging platforms are used to send a fraudulent or deceptive message to gain access to sensitive information. Cyber criminals when they reach out will often create a sense of urgency to trick you into clicking a link or open an attachment which will infiltrate your devices to steal passwords and bank account information.

Cyber criminals smish by:

- **Claiming suspicious activity** has been detected on an account or suspicious log-in, including posing as your bank or company's help desk.
- **Claiming there is a problem** with your account or your payment information.
- **Asking you to click** on a link to make a payment.
- **Trick you to bypass your company's procedures** to provide them with data or money that you ordinarily would not.
- **Remember** that Bank of America, like many companies, will never ask you for account or CashPro® details unless you call us first.

Be proactive:

- **Be careful** when posting personally identifiable information on social media. Be compliant with your company's social media policies.
- **Don't reply, click or answer from unknown sources** or click on their links or attachments.
- **Invest in antivirus software** and other cyber security software that can flag suspicious sites.

- **Don’t fall for the bait.** If an offer sounds too good to be true, it probably is. Or if a text looks strange, look up the sender and call them (don’t use the number they provide).
- **Never trust** unknown individuals. Verify everything they claim and do not send sensitive information to anyone whose identity you can’t verify.

If you suspect you have been targeted:

- **Don’t delay.** Acting quickly after you have been targeted can minimize damage to you or your company.
- **Contact your bank’s servicing desk** or support staff to report a fraudulent transaction as soon as you can.
- **Change all passwords** that may have been compromised.
- **Know and follow your local laws** and guidelines for cyber incidents.
- **Report the threat** to the platform on which it occured.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation by your company and the better prepared you will be against future attempts.

Cyber criminals go smishing by:

- **Contacting you** through fraudulent, spoofed or compromised phone numbers or accounts for messaging apps.
- **Providing an urgent pretext** for why you must send confidential or financial information.
- **Encouraging you to click** a link that downloads malware onto your mobile devices and gives criminals access to your devices and information.

Visit www.bankofamerica.com/security to learn how to help protect yourself and your business.

Help 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 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.