FRAUD AND CYBER SECURITY

Be Cyber Secure: Red flags and smart steps to avoid scams

You work hard for your money. Unfortunately, crooks work hard as well, attempting various tactics to take your money. As it can be incredibly difficult to recover stolen funds, it is important to be vigilant and proactive about your security to keep your personal and financial information safe. In order to keep your financial and personal information safe, it's necessary to look for red flags and be proactive about security.

Know the red flags

Whether it's a phone call or a sophisticated cyber campaign leveraging cutting edge technologies, criminals will try a variety of strategies to gain access to your money. If you experience any of the following, consider it a "red flag" and pause before you act:

- A person calls or emails, pretending to be someone you trust, such as a family member, government official, or a well-known business or nonprofit organization. These tactics are known as "phishing" respectively, and the intention is for you to let your guard down immediately.
- You're asked to make decisions in a hurry, asking for personal information such as an authorization code, threatening legal action, or using intimidation tactics to get you to act. They know fast action can mean you won't think things through, causing you to make mistakes.
- You're asked to send money through undetectable methods such as wire transfers and gift cards, or they may even send a check and ask you to return some of the money through these methods.

Learn the Dos and Don'ts:

- **Do** protect your devices by keeping your phone, tablet, and computer updated with the latest browser, operating system, and antivirus software. If you think any of your devices have been compromised, seek the help of a security or IT professional.
- **Do** stay on top of account activity and ensure all contact information with your financial institution is up-to-date.
- **Do** trust your gut. If it doesn't feel right, it probably isn't. Your intuition is usually correct, so take the time to pause and evaluate before sharing personal info, sending money, or revealing private data. If you have any concerns, hang up, don't click, or don't respond to requests for your data or financial information.
- **Don't** send money or give out your personal information in response to an unsolicited text, phone call, or email. Companies, such as Bank of America, will never call you and ask you for an authorization code.
- **Don't** be rushed to respond to unexpected requests. And if they tell you to not tell anyone or provide you talking points to say to your bank or family, you can be absolutely sure it is a scam. Research, validate, or talk to someone you trust. Look up the business and phone number online and contact them directly if necessary.
- **Don't** trust caller ID. Scammers can fake caller ID information, known as spoofing, so don't always trust the name and number that appears on-screen. If the caller asks for money or personal information, hang up and call back through a validated number.
- **Don't** deposit a check and immediately send back funds. Scammers send checks for larger amounts than agreed upon and then ask you to send the excess back by wire transfer, gift card codes, or a form of cash payment. You might send the money back right away, and their check might never clear, leaving you without any money.
- **Don't** fall for work from home scams. No legitimate company will require you to buy things or pay for equipment up front. Fake opportunities to put a logo on your car, become a mystery shopper, or baby-sit are a few ways you can be targeted.

Be Cyber Secure: Red flags and smart steps to avoid scams

IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill") makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation ("BofA Corp."). MLPF&S is a registered broker-dealer, Member SIPC, and a wholly-owned subsidiary of BofA Corp.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC, and a wholly-owned subsidiary of BofA Corp.

Banking products are provided by Bank of America, N.A., and affiliated banks, Members FDIC, and wholly-owned subsidiaries of BofA Corp.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value

3565853

Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe who work 24/7 to keep data and information safe.

Learn more and find out about the latest scam and fraud prevention news by visiting:

www.bankofamerica.com/security