Be cyber secure: protect against tech support scams

Tech support fraud occurs when a cyber criminal posts as a service or support representative to resolve technology issues such as viruses, compromised email or bank account, or a software license renewal. After the cyber criminals have remote access to devices or accounts, they can compromise your data and finances.

With access to your account, cyber criminals can:

- **Transfer funds** out of your accounts or charge purchases to them.
- **Steal your identity** and claim your tax refund or government benefits.
- **Create a fake identity** with some of your information and use it to open a new credit card or apply for a loan.
- **Phish** your contacts using your email account, and convince them to share confidential information.

Be proactive:

- **Invest in antivirus software** and other cyber security software that may reduce pop ups and that can flag suspicious emails and websites. Ensure all antivirus and cyber security software is kept up to date.
- **Never trust unknown individuals.** Verify everything they claim and do not send sensitive information to anyone whose identity you can't confirm.
- **Don't reply, click or answer to unknown sources** or click on their links or attachments. Legitimate security or tech support companies will not make unsolicited contact.
- **Wait, if you are at all unsure.** Take the time to research who you are talking to. Legitimate companies will allow time for you to respond and ask questions.

If you suspect you have been targeted:

- **Don't delay.** Acting quickly after you have been targeted can minimize damage.
- **Call your bank** and freeze financial accounts that may be affected and inform credit bureaus.
- **Change all passwords** that may have been compromised.
- **Call the police** and file reports with the relevant local authorities.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation and the better prepared you will be against future attempts.

Cyber criminals may contact you by the following ways:

- **Unsolicited telephone calls** from a cyber criminal impersonating computer, bank and utility companies.
- **Search engine advertising** occurs when an individual searches online to find telephone support numbers. Cyber criminals pay to have a fraudulent link at the top of the search list.
- **Pop up message** that claims a virus has been found on the computer. The message request tells you to call a phone number that links back to the cyber criminal.
- **An email** that claims you have a software subscription expiring or a potential fraudulent charge to your bank account. You will then be encouraged to contact the cyber criminal by phone.

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

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.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value