Common scams that target the at-risk population

Cyber criminals often target those who are at risk, using sophisticated social engineering tactics. Cyber criminals will try to earn their trust or establish an emotional relationship that may lead to exploitation or create a sense of urgency to produce fear and lure victims into immediate action to access their personal data and/or money.

Scams targeting those at risk can take many forms. Here are some common types to look out for:

- **Romance/confidence scams** occur when a cyber criminal creates a fake online identity and attempts to establish a trusting and believable relationship, then deploys different methods to ask for money.
- **Tech support scams** occur when a cyber criminal poses as a service or support representative to resolve technology issues and gain remote access to devices or accounts in order to compromise data and finances.
- **Lottery/sweepstakes scams** may happen when criminals make contact by phone, email, mail or social media claiming a victim has won a prize. However, to claim the prize, they may be required to pay bogus upfront fees or taxes.
- **Email compromise** may happen when a criminal contacts an individual through their email address and uses a hacked or fake account that looks legitimate to trick the target into sending funds.
- **Grandparent scams** occur when a scammer impersonates a grandchild and creates an urgent problem. The cyber criminal will appeal to the emotions of the grandparent and then request money to solve the problem.
- **Impersonation** is a common tactic that scammers will use to target individuals. Scammers may impersonate government officials, a loved one, a trusted person or even their bank.

Here are some tips that can help protect and prevent scams that target those at risk:

- **Be careful** what you post about yourself or your family online, including personally identifiable information such as your address or cell phone number.
- **Monitor** your privacy settings on online accounts.
- **Verify** unsolicited phone calls or emails. When in doubt, try to contact the person or organization through a verified website or alternate phone number.
- **Never share** information with people you don't know, especially if they contacted you.
- **Never click on pop-up messages** as they are regularly used to spread malicious software.
- **Trust** your instincts. If an offer looks too good to be true, it probably is.
- **Remember** that anyone can become a target for a scam, even if you do not have disposable income.
- **Reach out** to a family member or a friend that you trust to help you validate any suspicious correspondence you receive.
- If you have been targeted, **report** the incident to local law enforcement immediately and contact your bank.

Visit www.bankofamerica.com/security to learn how to help protect yourself and those closest to you.

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