

Be cyber secure: 401(k) and other retirement plans



Cyber criminals seek out information they can utilize and exploit. Here is how you can help mitigate risks with your 401(k) or other retirement plans:

→ Avoid phishing attempts:

- **Phishing** is a common social engineering method where seemingly legitimate messages are sent via email or messaging platforms
- **Spoofing** disguises communications in order to appear to be from someone else, including legitimate businesses or employees. Cyber criminals can spoof emails, phone numbers and websites.

→ Know the warning signs of a phishing email:

- **Mistakes:** Check for any misspellings, grammatical errors, and typos.
- **Suspicious return address:** Check the sender's email address. Look for discrepancies in the company name like an extra letter or added digit.
- **Sense of urgency:** You may be urged to take immediate action by clicking on a link or confirming personal information so your account will not be affected.

→ Here are some tips that can help protect your 401(k) and other retirement plans from cyber theft:

- **Be careful** about what you post about yourself online, including personally identifiable information such as your address or cell phone number.
- **Enable multifactor authentication** and use unique strong passwords for all your accounts.
- **Verify** any unsolicited phone call or voicemail. If you want more information, try to contact the person or organization through a verified website or alternative phone number.
- **Don't give any caller personal or company information**, even if the criminal already has it. Criminals can find personal information online or on the dark web.
- **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.

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.