BANK OF AMERICA

CYBER SECURITY

Be cyber secure: protect against tech support scams

Tips to protect yourself, and how to respond if you think you have been targeted.

Technology is in widespread use. With around 46 billion connected devices in circulation, there are many open doors for cyber criminals.[1] Tech support fraud occurs when a cyber criminal poses 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.

How to protect yourself

Be proactive:

- **Confirm all unusual money requests** in person or on the phone. If an email looks strange, call the sender using a verified number.
- **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've been targeted:

- **Don't delay.** Acting quickly after you have been targeted can minimize damage.
- **Call your bank** and freeze your financial accounts that may be affected and inform credit bureaus.
- **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 cyber crime attempts.

The growing threat, measured

203%

Percentage increase in total estimated losses due to Tech Support Scams in 2020, compared to 2019.[2]

39%

Percentage increase in total complaints in the Tech Support Scam category in 2020, compared to 2019.[2]

$116.4 million

Total losses due to Tech Support Scams in elderly population.[2]

[1] https://techjury.net/blog/how-many-iot-devices-are-there/#gref

[2] FBI, Elder Fraud IC3 Report, 2020

BANK OF AMERICA

Why it's important

With access to your devices and financial accounts, 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.

How do they contact you?

- **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.

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.

For more information, go to: www.bankofamerica.com/privacy/overview.go