BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Social Engineering

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

Social engineering is the use of deception to obtain sensitive or confidential information for criminal, fraudulent or malicious purposes. Using information available online, criminals in the guise of trusted individuals, bosses or authority figures coerce individuals into revealing sensitive information that can be used against them. This threat relies on and exploits the human tendency to trust, but being vigilant can be your first line of defense.

How to Protect Yourself

Be proactive:

- **Be careful** when posting personally identifiable information on social media. Enable security settings on your social media profiles to limit what you share publicly.
- **Download app updates.** Unpatched software can make you an easy target.
- **Invest in antivirus software** and other cyber security software that can flag suspicious emails and sites.
- **Don't fall for the bait.** If an offer sounds too good to be true, it probably is. Or if an email looks strange, look up the sender and call them using a known number.
- **Never trust** unknown individuals. Verify everything they claim and do not send sensitive information to anyone whose identity you can't verify.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to you or your business.
- **Call your bank** and freeze financial accounts that may be affected.
- **Change all passwords** that may have been compromised.
- **Freeze financial accounts** that may be affected and inform credit bureaus.
- **Call the police** and file reports with the relevant local authorities.
- **Notify the company** on whose platform the threat originated.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation by your company, bank and law enforcement officials, and the better prepared you will be against future events.

The Growing Threat, Measured

165,772

Number of unique phishing websites detected in the first quarter of 2020.[1]

650,572

Number of individuals who reported identity theft in 2019.[2]

467,361

Number of cyber security complaints reported to IC3 with losses exceeding $3.5 billion[3]

[1] https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

[2] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

[3] https://pdf.ic3.gov/2019_IC3Report.pdf

Be Cyber Secure: Social Engineering

Why It's Important

A common social engineering threat method is called phishing, where seemingly legitimate messages are sent via email or messaging platforms. Other methods of phishing are:

- **Vishing**: a cyber criminal impersonates a trusted source or utilizes tactics such as robocalls, to scam people out of data and money over the phone.
- **Smishing**: utilizes SMS and messaging apps to scam people out of data and money.
- **Spear phishing**: highly targeted phishing campaign designed for specific individuals.
- **Spoofing**: disguises communications in order to appear to be from someone else, including legitimate businesses or employees. Cyber criminals can spoof emails, phones numbers and websites.

Cyber criminals target by:

1. **Contacting you** through fraudulent, spoofed or compromised email accounts or accounts for messaging apps.
2. **Offering a bait** that gets you to click a link, which downloads malware onto your computer and gives criminals access to your device and information.
3. **Providing an urgent pretext** for why you must send confidential or financial information.

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