The Academy at Bank of America

Cyber Security Awareness – Resource guide

The Academy is Bank of America's training and professional development organization dedicated to the growth and success of our local communities and teammates.
Visit the career events page to sign up for additional professional skills workshops.
Visit the careers site to apply for a job with Bank of America.

BANK OF AMERICA

Overview

Description

This **Cyber Security Awareness** guide will serve as a resource to provide learners the skills needed to raise awareness about digital threats and security while also feeling empowered to protect your personal information. This guide is ideal for individuals looking to elevate their understanding of the importance of information security.

Introduction

Information security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The three tenets of information security are confidentiality, integrity, and availability.

This resource guide includes exercises and resources for the following:

- Understanding the threat landscape
- Best practices and scenarios

Understanding the threat landscape

Threat actors

There are four types of threat actors with a variety of potential objectives.

- Insider – Malicious or negligent, an authorized user with access to organization's data or information assets.
- Criminal – An individual or group who uses cyber to commit theft, fraud or other criminal acts.
- Hacktivist – A person or group who uses cyber activities to achieve political, social, or personal goals.
- Nation state – Government-backed actors with training, resources and offensive capabilities.

The difference between fraud and scams

Fraud is when a criminal ***obtains*** your personal or financial information and uses it for their own financial or personal gain.

A scam is when a criminal ***convinces*** you to send money or provide your personal or financial information for something that you believe to be legitimate when it's not.

Social engineering

Threat actors use social engineering to fool unsuspecting people into providing confidential or sensitive data. Social engineering involves some form of communication.

- Phishing – Any email message asking you to click a link, download/open a file, or reply with confidential information.
- Vishing – A phone call from a person asking you to provide confidential information.
- Smishing – A text message asking you to click a link or reply with confidential information.

Best practices and scenarios

Common scams

Scams often use intimidation and threat tactics to take advantage of people.

- Fake rentals – The listing sounds too good to be true, or you can't see the unit in person.
- Employment offers – You're told you need to pay an application fee or they offer the job without an interview.
- Service outage – You're told your online service is suspended until your payment information is updated.
- Personal loan – The offer sounds too good to be true or is unsolicited.
- Unpaid tax bill – You're up-to-date on your taxes or the caller pressures you to pay immediately.
- Social media – You're asked for financial or personal information, even if you think you know the person.

How to stay safe

Remember these cyber security best practices to stay safe again fraud and cyber threats.

- Be careful about what you post about yourself online, including personally identifiable information such as your address or cell phone number.
- Monitor your privacy settings on any online account.
- Verify any unsolicited phone call or email. If you want more information, 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. Resist the pressure to act quickly.

BANK OF AMERICA

If you suspect your personal information is compromised

- **Contact your financial institutions and creditors**. Speak with their fraud departments and explain that someone has stolen your identity.
- **Check your credit reports and place a fraud alert on your file**. Initiate a fraud alert by contacting one of the three credit bureaus (when you contact one credit bureau, the other two bureaus are notified automatically): Experian: 888.397.3742 TransUnion: 800.680.7289 Equifax: 888.766.0008
- **File an identity theft report and retain it for your records**. Complete a report online at the Federal Trade Commissions (FTC) identity theft website and contact your local law enforcement to report the crime.
- **Watch out for suspicious emails, phone calls or text messages asking you for your personal information**. Always verify that the communication is legitimate by calling the organization back through an official phone number.
- **Protect your device against malware or malicious software**. Download and install security software that updates automatically from a reputable company you trust. Make sure to change your online sign-in credentials, passwords and PINs.

Additional resources

www.BetterMoneyHabits.com
Continue building your financial know-how and learn more about keeping your information safe.

www.StaySafeOnline.org
Expand your knowledge and get tips for talking with your family and friends about their cybersecurity behaviors.

www.AnnualCreditReport.com
Regularly monitor your credit ratings and check on any unusual or incorrect information.

www.OnGuardOnline.gov
Get tips about protecting yourself from fraud and being a smarter consumer on issues related to spyware, scams and more.

www.DoNotCall.gov
Register your phone number to stop solicitation calls except from political and charitable organizations.

Visit the career events page to sign up for additional professional skills workshops.

Visit the careers site to apply for a job with Bank of America.

BANK OF AMERICA