MERRILL
A BANK OF AMERICA COMPANY

CYBER SECURITY

Be Cyber-Secure: Travel Safety

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

Whether you're a frequent business traveler or take the occasional family vacation, traveling abroad can make you more vulnerable to cyber attacks. Business travelers are especially at risk because they often carry sensitive data on their devices. And in many countries there is no right to privacy or legal restrictions against technical surveillance. So when you travel overseas, it's a good idea to take extra precautions.

How to Protect Yourself

Be proactive:

- **Bring only "clean" devices** your company has approved for travel, or remove sensitive data (including voicemails) from devices before traveling.
- **Disable remote and automatic connection** to Wi-Fi and Bluetooth on your devices. Use Bluetooth in "hidden" mode, rather than "discoverable."
- **Update your operating systems** and security software before you travel.
- **Avoid all public Wi-Fi** networks, especially in airports, hotels and cafes.
- **Install a virtual private network,** or VPN, on your devices to encrypt and protect your internet traffic and passwords even when using public Wi-Fi.
- **Stay constantly aware** of your surroundings and use privacy screens when you can.
- **Don't leave your devices** unattended, even in your hotel room or in a safe.
- **Don't use USB drives** that are not your own, and never plug an unknown storage device into your laptop or phone.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an attack can minimize damage to your business.
- **Tell your employer** if your work device has been stolen, or if you think your company's network has been breached.
- **Call your bank** and freeze financial accounts that may be affected (Bank of America's number for stolen or lost cards is 800-432-1000) and inform credit bureaus.
- **Change all passwords** that may have been compromised.
- **Call the police** and file reports with the relevant local authorities.
- **Document everything** about the attack. 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 attacks.

The Growing Threat, Measured

8,800

Number of machines identified by Interpol as actively trying to exploit malware on computers.[1]

457

Number of U.S. intellectual property-related arrests in 2017.[2]

$90 million

Total fraud losses that Secret Service agents investigated in 2017.[3]

[1] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/INTERPOL-led-cybercrime-operation-across-ASEAN-unites-public-and-private-sectors

[2, 3] https://www.secretservice.gov/data/press/reports/CMR-2017_Annual_Report_online.pdf

Why It’s Important

When out of the country, you should consider your computer, devices and confidential information as targets.

What are cyber criminals trying to steal?

- Intellectual property and trade secrets
- Employee, customer and vendor information
- Computer access protocols and computer network info

How are they trying to steal it?

- Wi-Fi networks
- Bluetooth connections
- Shoulder surfing (reading your screen or watching your keystrokes)
- Spyware that you unwittingly download by visiting an untrustworthy website or plugging in a corrupted or compromised USB drive
- Searching your belongings when you’re not watching

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 that work 24/7 to keep data and information safe.

For more information, go to:
www.ml.com/privacy-and-security-center/privacy-and-security-center.html

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.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as “MLPF&S” or “Merrill”) makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation (“BofA Corp.”). MLPF&S is a registered broker-dealer, Member SIPC, and a wholly-owned subsidiary of BofA Corp.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC, and a wholly-owned subsidiary of BofA Corp.

Banking products are provided by Bank of America, N.A., and affiliated banks, Members FDIC, and wholly-owned subsidiaries of BofA Corp.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value