



CYBER-SECURITY: CHECKLIST

Consider taking these steps if your family's devices have been targeted

Best practices to help you respond to a cyber event

- Don't delay.** Acting quickly after an event can minimize damage to you and your family.
- Disconnect your devices from the Internet.** Immediately unplug your internet cable or turn off your Wi-Fi router.
- Scan your network and devices.** Once you're offline, check for infected files or malicious programs with a strong antivirus program. Apply software patches and security updates to your devices. If you don't have an antivirus program on your system or it's outdated, consider calling a cyber-security professional to eradicate any suspicious programs and set up better defenses before you go back online with any connected device.
- Determine what happened.** Identify (if possible) what kind of event occurred, whether it was successful and what was lost or damaged.
- Restore lost files.** Recover corrupted files from backups.
- Change all your passwords.** Using a device that hasn't been compromised, change the passwords on all sites that contain personal or financial information. Also change passwords for any apps on your devices that may have been affected.
- Contact your bank's servicing desk or support staff.** Report fraudulent transactions as soon as you can.
- Call your financial institutions.** Have them put a freeze on any financial accounts that might be affected.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value
----------------------	-------------------------	----------------

- Call the credit bureaus.** Ask them to place a fraud alert on your credit report and freeze your credit.
- 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, and the better prepared you will be against future events.
- Contact law enforcement.** File reports with police and other relevant local authorities.

For more tips and insights, visit <https://www.privatebank.bankofamerica.com/articles/cyber-security-and-fraud.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.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC, and a wholly owned subsidiary of Bank of America Corporation ("BofA Corp.").