



CYBERSECURITY CHECKLIST

Consider taking these steps if your business has been targeted

Best practices to help your business respond to a cyber event

- Prepare and don't delay.** An immediate, strong response always helps to better address any incidents. Understand your cyber insurance policy (if you have one) and follow any guidelines outlined. A planned response to any event is critical to mitigating any risks. Acting quickly after a cyber event can minimize damage to your business.
- Detect and assess.** Identify (if possible) what happened, where and when the incident was first reported, and document whether it was successful, including any losses or damage by scanning all company networks to determine the extent of the intrusion or compromise. Work with internal or partner cybersecurity professionals to eradicate any suspicious programs or unauthorized access and set up better defenses before you go back online. Be sure to apply all software patches and security updates.
- Report.** Contact your bank and other financial institutions if you believe your accounts have been compromised. Report fraudulent transactions as soon as you can. To protect at-risk corporate assets, ensure access to bank systems have been secured and emergency workflows for any financial activities are followed.
- Initiate recovery.** Begin recovery of systems and data to pre-incident status once all evidence of the intrusion has been eradicated. Instruct all affected personnel to reset passwords and systems access controls, preferably while utilizing MFA or similar authentication methods. If you've experienced an incident that has compromised multiple accounts, require your employees to change their passwords to prevent criminal access of key systems and financial data.

Investment products:

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

- Review and improve your cyber policies.** Take lessons learned from the incident and review and improve cyber policies and response plans. Ensure that your employee training, firewalls, antivirus software and email protection are up to date and take steps to improve the effectiveness of your business network protection. To protect against future financial fraud, require multiple-person approvals for account and financial change requests. Use verified contact information from within the company's internal contact management system when verifying requests to change information or transfer funds.
- Document everything about the event.** The more information you have, the better prepared you will be to assist an investigation, and the better prepared you will be against future cybercrime attempts.
- Contact law enforcement. Know and follow your local laws and guidelines for cyber incidents.** If you discover evidence that account credentials or data has been stolen, or you experience financial loss, file a report. Companies that do business on a national level should also reach out to the FBI's Internet Crime Complaint Center (www.ic3.gov).

**For more tips and insights, visit
ml.com/privacy-and-security-center/additional-resources.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 ("BoFA Corp."). MLPF&S is a registered broker-dealer, registered investment adviser, [Member SIPC](#), and a wholly owned subsidiary of BoFA Corp. When you visit the Securities Investor Protection Corporation (SIPC) website at sipc.org, that website may have a different privacy policy and level of security. Please refer to SIPC's policies for the privacy and security practices for their website.

Merrill Private Wealth Management is a division of MLPF&S that offers a broad array of personalized wealth management products and services. Both brokerage and investment advisory services (including financial planning) are offered by the Private Wealth Advisors through MLPF&S. The nature and degree of advice and assistance provided, the fees charged, and client rights and Merrill's obligations will differ among these services. The banking, credit and trust services sold by the Private Wealth Advisors are offered by licensed banks and trust companies, including Bank of America, N.A., Member FDIC, and other affiliated banks.