BANK OF AMERICA

Big events, increased risk: how to help stay cyber secure



Major events increase travel, remote work and time sensitive communications, which can create additional cyber risk for businesses. Cybercriminals use event-related messages to trick employees and clients, often by creating urgency around payments or account activity. These tactics are designed to blend in with legitimate business activity and pressure employees to act quickly without verifying first.

Key cyber risks for businesses:

- **Event-themed phishing** targeting employees with fake updates, invitations or access requests.
- **Fraudulent invoices or payment requests** tied to travel, sponsorships, vendors or hospitality.
- **Attempts to take over accounts** by impersonating executives or trusted partners.
- **Increased risk during travel,** including public Wi-Fi, public charging stations and lost devices.
- **Point-of-sale (POS) compromise attempts** where criminals tamper with on-site payment devices or systems during an event, seeking to steal customer card data.

How to help reduce risk:

- **Remind employees to pause and verify.** Do not click links or open attachments tied to unexpected event messages.
- **Verify payment requests independently,** especially those marked urgent or event-related. Use known contact methods.
- **Require secondary approval** for payments or changes to vendor instructions.
- **Use secure connections.** Avoid public Wi-Fi when accessing work applications or company accounts, and use a virtual private network (VPN) when working remotely.
- **Avoid public USB charging stations.** Encourage employees to use power banks or power-only cables.
- **Protect your devices.** Lock your screen and use security features that help protect or erase your device if it's lost or stolen.
- **Limit exposure.** Disable auto-connect for Wi-Fi and Bluetooth. Be cautious with QR codes at venues.
- **Secure payment devices.** Limit access to POS equipment and check it regularly for any signs of unusual activity.

If suspicious activity is detected:

- **Don't delay.** Acting quickly after an incident can minimize its impact.
- **Notify your employer immediately** if your work device is stolen or if you believe your company's network may have been compromised.
- **Change all passwords** that may have been compromised using a minimum of twelve characters.
- **Notify your bank** if you suspect fraudulent or unauthorized transactions.
- **Follow all applicable local laws** and guidelines for responding to cyber incidents, and promptly report the situation to law enforcement or other appropriate local authorities.
- **Document everything about the incident.** The more information that you have, the better prepared you may be to respond and protect yourself against future attempts.

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" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value

© 2026 Bank of America Corporation. All rights reserved. 8943375