

Be cybersecure: AI-powered social engineering



Cybercriminals are increasingly leveraging generative artificial intelligence (AI) and deepfake technologies to produce highly convincing phishing emails, synthetic voice recordings, and manipulated video content. These tools enable attackers to credibly imitate executives, colleagues and even family members with unprecedented realism. Modern AI tools can replicate an individual's communication style, tone and linguistic patterns across any industry, and these can be created in virtually any language — mimicking dialects, accents and informal speech with remarkable precision.

→ How are these attacks different compared to traditional social engineering:

- **Real-time impersonation** — Deepfake voices or videos can appear in live calls or meetings, making impersonation highly convincing.
- **Highly polished messaging** — AI now produces flawless, natural-sounding messages, removing the grammatical mistakes and awkward phrasing that once made phishing attempts easy to spot.
- **Hyper-personalized** — Generative AI allows cybercriminals to scan social media and public information about an individual. Using this personalized information can help create a convincing, tailored communication.
- **Massive automation** — AI accelerates the creation and delivery of large-scale, customized phishing campaigns, far surpassing manual methods.

→ You're the first line of defense:

- **Don't let your guard down.** Pause and verify unexpected requests, especially when those requests involve sending payments, sensitive information or credentials.
- **Deepfakes are becoming more realistic and harder to detect.** While visual and audio anomalies such as syncing issues or unusual speech patterns can be warning signs, their absence does not guarantee authenticity.
- **Consider your digital footprint** — Reduce publicly available content, lock down privacy settings, and be mindful of what you share.
- **Verify any request about your bank account.** If you get an unexpected call, text or email claiming to be from your relationship manager or the fraud team hang up or do not respond to the message. Confirm it using contact information from an official website, verified bill, card or statement.
- **Use multifactor authentication** for an extra layer of defense. Choose phishing-resistant MFA methods like passkeys, security keys or smart cards.

→ If you suspect you've been targeted:

- **Don't delay** if you receive a password change notice, log-in alert or account update you didn't request, verify it immediately. Use official channels — log in directly through the app or the verified official website — to confirm and secure your account if necessary.
- **Report** any suspicious Bank of America web pages or messages to abuse@bofa.com
- **Check your accounts and turn on alerts** — cybercriminals will often access bank, credit card and other financial accounts first after they gain access to your information.
- **Update operating systems on your devices.** Ensure your banking and retail apps are also updated in the applications folder or store.
- **Change all passwords** that may have been compromised and run antivirus software on your device to confirm what may have been compromised and to remove malware.

IMPORTANT INFORMATION

This material is aimed at increasing your understanding of cyber threats and gives you some ideas about how you can be safer and more secure online. While we hope you find this content useful, it does not identify every cybersecurity best practice and is provided for your information only. You are responsible for determining how to best protect yourself against cyber threats. We make no promises that this material will prevent cyber threats and we are not responsible for actions you take or fail to take based on this material.

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.

“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 and are members of the NFA.

Investment products:

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

© 2026 Bank of America Corporation. All rights reserved. 8867904

Be cybersecure: how to build a cyber awareness program

Your employees are the first line of defense against cybercriminals. Adopting a cybersecurity awareness training program will help you create a culture of security throughout your organization, and prepare employees to detect potential threats and minimize the risk of a cyber breach.

Develop strong internal tools and processes

→ Define roles and responsibilities

Create formal cybersecurity policies for digital interactions of all kinds, including the use of devices and software.

Define role-based guidelines for each team, including what individual members need to know about IT security, online safety and privacy.

Build a formal security handbook that codifies these guidelines and share it with your employees.

Assign employees clear security-related responsibilities in the event that cyber threats are detected, including who has decision-making authority.

→ Provide formal training

Offer managers step-by-step actions they can take to educate new hires while providing ongoing training for existing employees.

Provide employees with access to educational, training and certification programs that offer knowledge of cyber threats and hands-on experience with them.

Refresh employees' knowledge of industry best practices and standards every six months.

Supplement linear sources of education, such as books, training guides and online videos, with interactive exercises and team-based activities that test employees' skills.

→ Integrate learning opportunities

Transform routine cybersecurity challenges, such as phishing emails or social engineering attacks, into simulated real-world scenarios that employees can learn from.

Offer instructional feedback as workers tackle these challenges and help them determine the best way to address each situation.

Quiz employees on what they've learned, review the results and discuss where their actions could have been more effective.

Share the insights obtained from these exercises with the rest of the organization.



Reinforce cyber awareness

Plan and schedule regular employee engagement campaigns that promote awareness of current cybersecurity trends.

Reach out to employees on a routine basis, weekly or monthly, to inform them about hot topics in the cybersecurity space.

Create a communications plan and workflow for dealing with IT security incidents and make sure your teams are familiar with it.

Use security issues as opportunities for employees to learn best practices.



Establish lines of communication

Identify the key person(s) accountable for cybersecurity within each of your organization's departments and circulate their contact information. Do the same for each of your partners and vendors.

Implement official communications channels, online forums or emergency email accounts, through which employees can report cybersecurity incidents.

Use standardized templates for threat reports and updates to help employees share information quickly.



To learn more

The Global Information Security (GIS) team at Bank of America is made up of information security professionals, staffing multiple security operations centers across the globe, who work 24/7 to keep data and information safe.

Visit www.business.bofa.com/managingfraudrisk to learn how to help protect yourself and those closest to you.

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
----------------------	-------------------------	----------------

Be cybersecurity: business email compromise



You do not have to work in the finance department of a big company to be the target of business email scams. Business Email Compromise (BEC) is the term for financial cyber events in which a targeted individual is contacted through their work email. The cybercriminal uses a hacked or fake account that looks legitimate in an effort to trick the target into sending funds.

→ Cybercriminals may imitate:

- **A supplier.** A message arrives from a hacked email address to notify you of a bank account change or to request payment.
- **A legal professional.** A message arrives during a transaction with directions to send an expected payment. For example, during a home purchase, you receive a fraudulent request to make a down payment.
- **A familiar address.** A message appears to come from someone you know and asks for confidential information, such as payroll records.

→ Be proactive:

- **Know your company's cybersecurity plan** and how to report any suspicious emails.
- **Confirm all unusual money requests** in person or on the phone. If an email seems strange, look up the sender and call them from a verified and trusted number.
- **Invest in antivirus software** and other cybersecurity software that can flag suspicious emails and websites.
- **Never trust unknown individuals.** Verify everything they claim, and do not send sensitive information to anyone whose identity you can't confirm.
- **Don't reply to emails from people you don't know** or click on any links or attachments.
- **Wait, if you are at all unsure.** Take the time to discuss your suspicions with your manager or a colleague.
- **Be on the lookout for BIMl**, or Brand Indicators for Message Identification, which some companies have started implementing. BIMl generates a company-defined, verified and authenticated logo in emails.

→ If you suspect you have been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to your business.
- **Call your bank** and freeze financial accounts that may be affected.
- **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 financial fraud. The more information you have, the better you may be able to assist an investigation, and the better prepared you may be against future cybercrime attempts.

Visit www.bankofamerica.com/security to learn how to help protect yourself and those closest to you.

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 BofA Corp.

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

"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 and are members of the NFA.

Investment products:

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

© 2025 Bank of America Corporation. All rights reserved. 8409808

Be cybersecure: cybersecurity best practices

Preparedness and response planning are critical for any technology-driven business. As threat actors continue to refine their tactics and tailor attacks to specific industries and organizations, companies must remain vigilant and adaptable. A strong security posture integrates effective network controls, consistent system maintenance and updates, and a company-wide culture of awareness that enables timely detection and response.

Develop strong internal tools and processes

→ Protect your networks and data

- Employ a password management strategy that leverages multifactor authentication, an enterprise password manager and best practices for password security, including using numbers, different cases and at least 8 characters.
- Track the activity of network users to facilitate an audit trail if there is a security investigation. Restrict network access based on employee need.
- Apply software updates and security patches to your devices, applications and operating systems.
- Follow robust backup procedures for all systems and data. Ensure important business information is backed up regularly and automatically at least once a week. Store backup copies offsite, ideally in multiple secure locations.

→ Create a cyber defense program

- Analyze your company's critical processes and systems to pinpoint cyber vulnerabilities. Know which data could disrupt operations or weaken your competitive advantage if lost or stolen.
- Assess storage, access and control policies for your company's most sensitive information.
- Monitor user activity within your systems and network. Periodically review the access granted to your systems and applications, ensuring you include third parties as a core aspect of that review.
- Pay attention to breaches in your industry. If incidents occur within a specific sector, they can reveal systemic weaknesses. Understanding these trends can help companies identify potential threats.

→ Develop a cyber incident response plan

- Establish clear roles and decision authority for cybersecurity incidents, and run regular exercises to test and strengthen your company's readiness.
- Designate cybersecurity ownership either by functional area or centrally, depending on organizational size, and maintain a named list of internal and external security points of contact to share with your team.
- Document all details of any cybersecurity incident. Use this information to evaluate and revise your incident response plan following each event.
- Clarify how you will communicate and share information about an incident with those inside your organization, external partners, investors and the general public.

→ Establish a cyber awareness program

Create an ongoing education program for employees that identifies and explains the security risks and threats they will most likely face in their company role, and discusses threat detection and response.

Implement regular cybersecurity training programs for employees and extend the same education to vendors and third-party partners with network access.

Encourage employees and IT decision-makers to readily share information about potential security threats.

→ Focus on your employees

- Incorporate ongoing, hands-on exercises such as phishing and social engineering simulations to ensure everyone remains vigilant and prepared.
- Create clear cybersecurity policies and protocols and ensure employees understand the chain of reporting during a cybersecurity incident.
- Train every employee to recognize that cybersecurity begins with them and to follow company procedures if they suspect a cybersecurity incident has occurred.
- Institute an accountability policy that covers all employees and emphasizes the importance of identifying and discussing cybersecurity risks and reporting suspicious activity.

→ To learn more

The Global Information Security (GIS) team at Bank of America 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.

Visit www.bankofamerica.com/managingfraudrisk to learn how to help protect yourself and your business.

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 and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured

Are Not Bank Guaranteed

May Lose Value

Malware prevention

How to defend your devices and networks from malicious software



Malware, or 'malicious software,' is a term for any software program or code designed to compromise or damage electronic devices. It can be delivered through phishing, infected downloads and attachments, and mobile device compromise.

Malware can take many forms, but bots, ransomware and spyware are among the most common, with so many tactics at criminals' disposal and the number of exploitable endpoints growing exponentially.

When successful, malware may compromise system operations, facilitate theft of company data or resources, encrypt files and compromise business reputations. Unsecured Wi-Fi networks, weaknesses in front line defenses and third-party contractor's compromised networks are not the only concerns for businesses. Despite a constantly evolving landscape, there are many ways for organizations to prepare for and deflect malware attempts.

→ Maintain and regularly update lines of defense

Install up-to-date versions of antivirus software programs, spyware scanning solutions and system firewall tools. Keep these tools current with regular downloads and installations.

Run virus scanning software automatically on your systems at regular intervals.

Use the most current version of operating systems and web browsers, with all security patches applied. Do this on all company devices that connect to the internet, including smartphones and other internet enabled hardware units.

Minimize risk by using the "least-privileged" access model, granting users access to only those core features and systems needed to perform their job.

Maintain daily backups of data, store backups away from your primary network and only allow read (not write) access to backups to maintain their integrity. Regularly test and restore these backups to ensure they remain operational.

Encrypt data to protect information from external threat actors.

→ Watch for unusual behavior in your networks

Monitor every system, app and device attached to your networks for viruses and spyware. Conduct routine penetration testing on all endpoints and IT infrastructure to minimize system vulnerabilities. Prohibit the use of external storage solutions such as USB drives when possible.

Implement threat intelligence monitoring, which can provide data on specific threats and threat actors, and can assess potential system vulnerabilities in the context of current and past cybersecurity incidents.

Safeguard cloud networks, content management systems and other external technology solutions that touch your networks.

Create baseline readings for internal network and user activity, and stay alert for anomalies or user behavior that falls outside the norms.

Reject incoming email with executable attachments. Filter out communications from known sources of malware and spam.



Promote secure online interactions

Train your staff to resist clicking on suspicious text messages and emails with links, files or attachments, and to confirm these transmissions' legitimacy with verified sources.

Warn employees to be suspicious about requests for sensitive information that occur in emails or phone calls.

Encourage employees to examine any communications received for spoofed domains, inconsistent language or anomalies, and to be wary of any forwarded web links.

Instruct employees who work remotely to avoid using public Wi-Fi networks, and to operate with virtual private networks (VPNs) whenever possible.

Employ multifactor authentication, an enterprise password manager and best practices for password security, including using numbers, different cases and at least eight characters.

Visit only secure websites and trusted sources for software downloads, such as company websites or official app stores.

Delete from your devices any unused applications, which may contain vulnerabilities that cybercriminals can utilize.

Sign out from all apps, networks and devices when you are finished using them.



Maintain organizational preparedness and awareness

Build a formal, well-defined malware response plan based on a step-by-step playbook that describes specific actions employees must perform.

Test your response plan in simulated cyber event scenarios, using real-world encounters and exercises to ensure that your organization is strategically and tactically prepared to address a malware attempt.

Institute an open-door policy that encourages employees to express their concerns. Emphasize that workers do not need to be certain a problem exists before reporting suspicious activity.

Ensure employees understand the chain of reporting during a malware incident, especially if systems, websites or services need to be quarantined or shut down.

Create a threat prevention model wherein employees are encouraged to **prevent** (deter threats), **detect** (identify and prepare for incidents) and **respond** (rapidly address concerns) when issues arise.

Reach out to skilled third-party organizations or law enforcement agencies if you suspect a serious malware infection of your system.



Educate employees about digital risks

Provide employees with access to cybersecurity education and training programs, and supplement that instruction with ongoing education opportunities.

Create team-building activities that promote knowledge and awareness of malware and other cybersecurity threats.

Supply online resources and forums to help employees stay current on malware risks and other cybersecurity trends.

Encourage teams not to use the same network systems for email and external communications that they use for banking, finance or other sensitive business functions. Educate employees to employ safe and secure online and information sharing habits.

Train every employee to recognize that cybersecurity begins with them, and to follow company procedures for creating an alert if they suspect a malware incident has occurred.



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

For more information, go to www.business.bofa.com/managingfraudrisk

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 and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

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

© 2025 Bank of America Corporation. All rights reserved. 8333276

Ransomware protection

Reduce the risk of cybercriminals taking your network and data hostage



Ransomware is a type of malware that encrypts data on computers, mobile devices and networks and allows criminals to demand payment for the release of data or return of service. It can be delivered in an increasing variety of ways, including fraudulent emails and websites, unpatched remote network portals and pop-up warnings with malicious links to technical support.

This type of cybercrime is becoming more sophisticated and ransomware demands are increasing. There are no guaranteed defenses against any type of cybercrime, but organizations with a proactive approach to cybersecurity and employee awareness can detect and prevent ransomware attempts.

Here are five strategies that can help your organization build a culture of cyber preparedness, safeguard its systems and deploy overarching, informed defense against ransomware.

→ Regularly back up and protect your systems and data

Maintain daily backups of data, store backups away from your primary network and only allow read (not write) access to backups to maintain their integrity. Regularly test and restore these backups to ensure that they remain operational.

Keep multiple backups in place in case recent editions have been infected with ransomware files.

Encrypt data to protect information from external threat actors.

Segment networks into zones that require different login credentials to limit cybercriminals' ability to infiltrate systems and the amount of information they can access.

Set network parameters that can control system usage and how individual users connect with remote devices. Also restrict downloads over public Wi-Fi.

→ Maintain and update lines of defense

Install ransomware prevention software that can detect incidents in progress, quarantine infected devices, initiate scans or provide alerts and updates to IT security employees in real time.

Reject incoming email with executable attachments and filter out communications from known sources of ransomware and spam.

Install up-to-date versions of anti-virus software programs and threat-scanning solutions.

Run virus scanning software automatically on your systems at preset intervals.

Use the most current versions and security patches for operating systems, web browsers and company devices, including mobile devices.

Minimize risk by using the "least-privileged" access model, granting users access to only those core features and systems needed to perform their job.

Monitor every system, app and device attached to your networks for viruses and spyware and conduct routine penetration testing on your organization's apps, devices and IT infrastructure elements.

Implement threat intelligence monitoring to assess potential system vulnerabilities.

Safeguard cloud networks, content management systems and other external technology solutions that touch your networks.

Create baseline readings for internal network activity and watch for unusual user behavior.



Promote secure online interactions

Train your staff to resist clicking on suspicious emails with links, files or attachments, and to confirm these transmissions' legitimacy with verified sources.

Warn employees to be suspicious about requests for sensitive information that occur in emails or phone calls.

Encourage employees to examine any communications received for misspellings, grammatical errors or anomalies, and to be wary of any forwarded web links.

Instruct employees who work remotely to avoid using public Wi-Fi networks, and to operate with virtual private networks (VPNs) whenever possible.

Employ multifactor authentication, an enterprise password manager and best practices for password security, including using numbers, different cases and at least eight characters.

Allow users to identify file types, such as by enabling file extension visibility, to reduce the likelihood of installing ransomware.

Visit only secure websites and trusted sources for software downloads, such as company websites or official app stores.

Delete any unused applications from your devices, which may contain vulnerabilities that cybercriminals can exploit.

Sign out from all apps, networks and devices when you are finished using them.



Maintain organizational preparedness and awareness

Build a formal, well-defined ransomware response plan based on a step-by-step playbook that describes specific actions employees must perform.

Test your ransomware response plan in simulated cyber event scenarios, using real-world encounters and exercises to ensure that your organization is strategically and tactically prepared to address a ransomware attempt.

Institute an open-door policy that encourages employees to express their concerns. Emphasize that workers do not need to be certain a problem exists before reporting suspicious activity.

Ensure employees understand the chain of reporting during a ransomware incident, especially if systems, websites or services need to be quarantined or shut down.

Create a threat prevention model wherein employees are encouraged to **prevent** (deter threats), **detect** (identify and prepare for incidents) and **respond** (rapidly address concerns) when issues arise.

Reach out to skilled third-party organizations or law enforcement agencies if you suspect a serious ransomware infection of your system.

→ Educate employees about digital risks

Provide employees with access to cybersecurity education and training programs, and supplement that instruction with ongoing education opportunities.

Create team-building activities that promote knowledge and awareness of ransomware and other cybersecurity threats.

Supply online resources and forums to help employees stay current on ransomware risks and other cybersecurity trends.

Encourage teams not to use the same network systems for email and external communications that they use for banking, finance or other sensitive business functions, and train them to employ safe and secure online and information sharing habits.

Train every employee to recognize that cybersecurity begins with them, and to follow company procedures for creating an alert if they suspect a ransomware incident has occurred.

→ 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 who work 24/7 to keep data and information safe.

For more information, go to www.business.bofa.com/managingfraudrisk

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 and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

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

© 2025 Bank of America Corporation. All rights reserved. 8333352

Be cyber secure: navigate search results safely



When you use an online search engine, do you ever question if the website results are legitimate? Cybercriminals know we use and trust search engine and AI chatbot results — they ‘poison’ the list of options to appear legitimate but instead can lead you to impersonating or malicious websites with malware. Check these tips before you click.

→ Cybercriminals look for opportunities when you’re doing routine tasks:

- **Spoofed websites and login pages** — these fraudulent websites target banking, retail, utilities and package tracking. They can often be identified by incorrect domain spelling, poor design quality or unfamiliar buttons or actions.
- **Checking your balance, shopping or downloading** — be vigilant when completing familiar tasks as financial services, utilities and retailers are often targeted. Moreover, search engine optimization (SEO) rankings can be fraudulent and lure you into action.

→ You’re the first line of defense:

- **Don’t let your guard down.** It’s easy to complete a routine task quickly, but you could be tricked by a fraudulent website. Bookmark your official banking, retail and utility websites to log in and complete tasks. If you’re on the go, use the phone number on the back of your debit or credit card for contact information.
- **Investigate information provided by AI chatbots.** When using AI chatbots, you may only see one website option or phone number. These answers may have been exploited by SEO poisoning, so investigate thoroughly.
- **Verify requests made about your bank account.** If you receive an unexpected call, text or email from someone claiming to be a relationship manager or the fraud department, always verify the source using contact information taken from a legitimate website, verified bill, card or statement.
- **Don’t click on ads in search engine results.** These could be fraudulent links leading to a spoofed website that may include malware or a phishing attempt. Type a verified website URL directly into the address bar.
- **Use caution with shipping messages.** If you’re asked to provide payment, it may be financial fraud.

→ If you suspect you’ve been targeted:

- **Don’t delay** — acting quickly after clicking on a potentially bad link can minimize damage.
- **Tell your employer** if you believe your work device has been comprised or if you think your company’s network has been breached.
- **Report any suspicious Bank of America web pages** or messages to abuse@bankofamerica.com.
- **Check your accounts and turn on alerts** — cybercriminals will often access bank, credit card and other financial accounts after they gain access to your information.
- **Update operating systems on your devices.** Ensure your banking and retail apps are also updated in the applications folder or store.
- **Change all passwords** that may have been compromised using a minimum of eight characters. Consider using passphrases instead of passwords.
- **Run antivirus software** on your device to confirm if you’ve been compromised and to remove malware.

Report any suspicious bank communications or website pages to abuse@bankofamerica.com

IMPORTANT INFORMATION

This material is aimed at increasing your understanding of cyber threats and gives you some ideas about how you can be safer and more secure online. While we hope you find this content useful, it does not identify every cybersecurity best practice and is provided for your information only. You are responsible for determining how to best protect yourself against cyber threats. We make no promises that this material will prevent cyber threats and we are not responsible for actions you take or fail to take based on this material.

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.

“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 and are members of the NFA.

Investment products:

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

© 2025 Bank of America Corporation. All rights reserved. 8442927

Be cybersecurity: business travel safety



Whether you're a frequent business traveler or take the occasional trip, traveling can make you more vulnerable to cyberattacks. Business travelers are especially at risk because they often carry sensitive data on their devices. In many countries, there are no privacy or legal restrictions against technical surveillance. When you travel, it's a good idea to take extra precautions.

→ Cybercriminals may be trying to steal confidential information by:

- **Shoulder surfing** — reading your screen or watching your keystrokes.
- **Juice jacking** — using public charging stations to gain access to your device.
- **Using spyware** that you unknowingly download by visiting an untrustworthy website or plugging in a corrupted or compromised USB drive.
- **Searching your belongings** when you're not watching.

→ Be proactive:

- **Only bring devices your company has approved for travel** or remove sensitive data (including voicemails) from devices before traveling.
- **Disable remote and automatic connections** to Wi-Fi and Bluetooth on your devices and avoid using public Wi-Fi networks.
- **Only download apps from official app stores** and regularly update both your apps and your operating system to protect your devices.
- **Install a virtual private network***, or VPN, on your devices to encrypt and protect your internet traffic and passwords.
- **Stay constantly aware** of your surroundings and use privacy screens when you can. Don't leave your devices unattended; keep them on your person or in a secure location.
- **Consider carrying a power-only charging cable**, which prevents data from sending or receiving while you're charging.
- **Notify your bank** of travel if using debit/credit cards.

→ If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to your business network.
- **Notify your employer immediately** if your work device is stolen or if you believe your company's network may have been compromised.
- **Enable multifactor authentication (MFA)** everywhere possible to prevent further unauthorized access.
- **Change all passwords** that may have been compromised using a minimum of eight characters.
- **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 event.** The more information you have, the better prepared you may be to assist an investigation, and the better equipped you may be against future attempts.

Visit www.bankofamerica.com/security to learn how to help protect yourself and those closest to you.

IMPORTANT INFORMATION

This material is aimed at increasing your understanding of cyber threats and gives you some ideas about how you can be safer and more secure online. While we hope you find this content useful, it does not identify every cybersecurity best practice and is provided for your information only. You are responsible for determining how to best protect yourself against cyber threats. We make no promises that this material will prevent cyber threats and we are not responsible for actions you take or fail to take based on this material.

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.

“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 and are members of the NFA.

Investment products:

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

© 2026 Bank of America Corporation. All rights reserved. 8784182