

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 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