



OUR COMMITMENT TO CYBERSECURITY

Learn how Raymond James safeguards your assets and information – and how you can help.

RAYMOND JAMES



Raymond James uses advanced infrastructure and applications as well as highly skilled personnel to protect your personal information and the assets in your accounts from cyber threats.

NEXT-GENERATION FIREWALLS: Firewalls block unwanted incoming internet traffic, stop users from downloading and installing viruses, and prevent users from connecting to malicious or harmful websites.

INTRUSION-DETECTION SYSTEMS: Every day, there are thousands of failed attempts to compromise our networks. Our intrusion detection systems alert our teams when attempts are being made on a network and allow the team to quickly respond to possible threats.

DATA-LOSS PREVENTION: Our data loss prevention software looks for sensitive data that is being stored or used incorrectly when it is being worked on by a user or transferred through our networks and systems.

SECURITY INFORMATION AND EVENT MANAGEMENT: Security information and event management software provides quick analysis of the millions of security event logs that are generated every day, allowing us to sort through false positives and focus on correlating interrelated attacks and combating real threats.

EMAIL SECURITY: Our teams stop cyberattacks by filtering emails to remove and stop emails that have malicious links, attachments, or are simply spam.

LAPTOP AND DESKTOP SECURITY: We use advanced encryption, security and antivirus software to protect the vital information stored on all Raymond James equipment.

NETWORK AND APPLICATION VULNERABILITY SCANS: As attackers discover and even create new ways to access systems and hack applications, our teams stay one step ahead by continually scanning all of our systems for possible vulnerabilities.

NETWORK ACCESS CONTROL: In addition to preventing attackers from connecting devices, network access control can disconnect otherwise authorized devices that have become infected with a virus or otherwise compromised.

HOW YOU CAN PREVENT CYBERATTACKS

Maintaining your security is a partnership. With a few preventive measures, including physically securing laptops and mobile devices at all times, you can help protect your assets and personal information from cybercriminals.

- 🔒 KEEP YOUR EQUIPMENT UP TO DATE:** Install the latest updates and patches for your computers and mobile devices and use security software including antivirus, firewalls and encryption. And before selling or disposing of computers and mobile devices, wipe them of data.
- 🔒 USE WIRELESS NETWORKS AND PUBLIC EQUIPMENT WITH CAUTION:** Use virtual private networks (VPN) when accessing sensitive data. Avoid visiting sensitive websites on public Wi-Fi or while using public computers and be wary of unknown flash drives.
- 🔒 PRACTICE GOOD PASSWORD HYGIENE:** Password protect all computers and mobile devices. Online, use complex passwords that contain a combination of upper and lowercase letters, numbers and special characters. When possible, elect for two-step authentication. Do not share your passwords.
- 🔒 REGULARLY REVIEW YOUR STATEMENTS:** Look for signs of unauthorized activity and promptly report suspicious transactions. To thwart mailbox bandits, consider receiving your statements electronically through Client Access.
- 🔒 STAY ALERT FOR ONLINE RISKS:** Never open attachments or click on links in suspicious emails or text messages or from senders you don't recognize. Limit the personal information you share on social media. When online shopping, stick to sites that begin with https.
- 🔒 BEWARE OF SCAMMERS:** Familiarize yourself with popular scam techniques, such as criminals posing as representatives of reputable companies such as your bank or claiming your computer is infected with a virus to gain access to your personal information. Misspellings and grammar mistakes are often a red flag.
- 🔒 PRACTICE SENSIBLE DATA MANAGEMENT:** Back up your data regularly and shred sensitive documents before disposing of them.

PENETRATION TESTING: Penetration testing checks our networks for common loopholes and security exploits to protect against common threats.

TWO-FACTOR AUTHENTICATION: Security tokens, security questions or thumbprints provide an additional layer of security should passwords become compromised.

MOBILE DEVICE SECURITY: Through mobile device management, the applications and access of the mobile devices that connect to our corporate network can be subjected to strict controls that prevent unauthorized access.

DEDICATED THREAT INTELLIGENCE TEAMS: We employ teams dedicated to threat intelligence and are responsible for information gathering, research and testing.

LAYERED SECURITY: Network security can be strengthened by architecting it into multiple layers, each one often taking a different approach. In other words, the chain is no longer only as strong as the weakest link; now an attacker must break all of the links.

OUR PROMISE TO YOU

As a firm that strives to put clients above all else, we want you to have the highest level of confidence in doing business with your advisor and Raymond James. That's why, in addition to offering the comprehensive security measures you expect from a leading financial services company, we're proud to offer you this assurance:



We will reimburse you for losses in any of your Raymond James accounts due to unauthorized access to a Raymond James system that occurs through no fault of your own.

It's important to remember that we reimburse you only for account losses that result from unauthorized online access to one of our systems. That means we do not cover losses caused by individuals who have your permission to access your account. As a reminder, always take care not to share your account information, since doing so implies that you have authorized that person's activities.

**We're committed to preserving your privacy and
financial well-being.**

For more information on how Raymond James
protects your accounts, contact your financial advisor
or visit raymondjames.com/privacy_security

LIFE WELL PLANNED.

RAYMOND JAMES®

INTERNATIONAL HEADQUARTERS: THE RAYMOND JAMES FINANCIAL CENTER
880 CARILLON PARKWAY // ST. PETERSBURG, FL 33716 // 800.248.8863
RAYMONDJAMES.COM

Raymond James will determine the type and amount of any reimbursement, including whether to replace the assets in your account. We may not compensate you for losses for which you are reimbursed, or eligible for reimbursement, through other coverage, such as an insurance provider. This reimbursement requires you to promptly tell us of any unauthorized access to your account and to comply with our requests and procedures during the review of your reimbursement. We may ask you to cooperate with us in connection with any investigation, to take steps to protect against further losses, and to sign documents in connection with any reimbursement. We reserve the right to not reimburse your losses in your retail brokerage account if you have not complied with any of the foregoing.