



How We Protect You

Information Security is a top priority at Baird. We understand that protecting your personal and account information is an essential part of our commitment to our clients. Our Information Security and IT Security teams use advanced technologies and industry-tested processes to protect against electronic fraud.

Maintaining your security is a partnership. For more information on the role you play, please visit our [website](#).

Cybersecurity and the Role You Play

Baird takes great care in protecting your information, but you play a critical role as well. We strongly encourage following these five tips to help improve your online security.

- Keep all of your software up to date**

Install patches for your operating system, applications, and web browser as soon as they're released to reduce your risk of being infected with malware.
- Use a reputable antivirus software**

This will further reduce your risk of a malware infection.
- Think before you click**

Avoid clicking on links or attachments in unexpected emails or texts. Links may direct you to malicious websites that attempt to infect you with malware or harvest your information. Attachments may also contain malware.
- Secure your accounts**

Use a long, strong, and unique easy-to-remember passphrase for each of your accounts. Enable two-factor authentication where available to add another layer of security. Also, consider using a password manager app to help you create and store strong passwords securely.
- Take control of your digital footprint**

Be mindful of the information you share online whether it's for a financial transaction or social media. Do not post about vacations or business trips in real-time. Always log out completely after completing a transaction or sending a message. Log in and review the privacy settings of your online accounts.

For more about how Baird protects your information, contact your financial advisor or visit our Information & Site Security website at <http://www.rwbaird.com/help/safety-security/site-security.aspx>.

To learn more about how you and your family can stay safe and secure online, visit the Department of Homeland Security website at <https://www.dhs.gov/stopthinkconnect>.

TECHNOLOGY

Baird uses layered defenses of industry-standard and leading-edge technologies to address cyber risks and protect our most critical systems and client data:

Encryption

Baird employs some of the strongest forms of encryption commercially available for use on the web today. All Baird Online sessions are encrypted using TSL (Transport Layer Security).

TECHNOLOGY (Continued)

Firewall & Intrusion Prevention Systems

Baird's computer systems are protected 24 hours a day by a powerful firewall that blocks unauthorized entry. We use these firewalls to control who accesses our websites and work with intrusion prevention systems to monitor our network for potentially malicious activities.

Secure Login

Baird Online requires strong passwords and uses risk-based authentication techniques to help secure your login so that only you control who accesses your online account.

Timed Log-Off

The Baird Online system will automatically log you off after a period of inactivity. This reduces the risk of others accessing your information from your unattended computer.

Fraud Detection and Prevention

Baird uses leading-edge technologies that provide strong authentication and anomaly detection to alert us of suspicious events that do not follow normal patterns of behavior.

SECURITY POLICIES AND PROCEDURES

Baird has policies and procedures in place to help prevent the misuse of data and to reduce the risk of fraud. For instance, we will never ask you to verify your account number(s), Social Security number or password(s) via standard email or text messages. Verification of confidential information should only take place in person or via our secure online portal (Baird Online).

If you request that confidential information (e.g., account statements or reports) be shared via email, we will leverage an email encryption service to provide a safe, secure method of sharing such information via email.

PRACTICES AND SECURITY ASSESSMENTS

Baird conducts ongoing, extensive testing of our critical systems, including Baird Online, to proactively find and remediate vulnerabilities. This includes:

- Independent reviews conducted by outside security firms
- Ongoing scanning and monitoring to protect against known security risks
- Application vulnerability assessments
- Internal security assessments and technology to monitor and maintain a safe and stable environment

EMPLOYEE AWARENESS AND TRAINING

We provide mandatory annual training to our employees on information security best practices, security policies, procedures and event handling. We also conduct phishing assessments on our employees with additional required training, if needed.

THIRD-PARTY RISK MANAGEMENT

We have a comprehensive Third-Party Risk Management Department that establishes and maintains risk profiles for Baird's Third-Party Partners. All new Third-Party Partners go through a due diligence process, and existing Partners also undergo routine monitoring and review.

ADDITIONAL SECURITY MEASURES

Baird's layered approach to online security extends beyond a unique username and password, encryption, firewall, technology updates and ongoing monitoring. We have additional security measures that may be activated in response to certain activities or events. If we are suspicious of any behavior, we may restrict online access to accounts, prevent certain types of transactions or contact you to verify the validity of certain instructions. These measures are designed to safeguard your identity and your accounts. Further proof of identity may be required before online access is restored.

Optional:

To learn more about how to protect your personal information in your everyday life, please visit the Insights & Educations on our [Baird Wealth](#) site.