Security Statement

We take securing your data as seriously as growing your retirement.

Our highest priority is keeping your financial and personal data safe and secure. In doing so, we incorporate the most established and robust information assurance concepts in the industry today. Our systems use multiple layers of security controls and our people implement systematic processes and procedures for securing and storing data.

How we protect you

Identity and Access Management

Whether you interact with us online, by phone, or in person, steps are taken to verify your identity before gaining access to any account/s. Our processes are designed to minimize access to your data internally based on the principle of "least privilege," which allows minimal user profile privileges on Financial Engines computers (based on our employees' job necessities). Any time we make changes to a participant account, we send a confirmation via email or through the mail.

Data integrity and availability

We take measures to protect your data from corruption and/or manipulation by performing integrity checks prior to loading or processing. Additionally, we archive secure copies of your data and use procedures to verify that the data is available to be restored if necessary.

Data Loss Prevention

Rest assured, your data is secured during its entire life cycle. We use some of the best available encryption technology to protect your information during transmission and whenever we need to store it on our systems. We ensure your data is encrypted in transit, at rest, and while in use.

24 x 7 Monitoring

Our security solutions are constantly monitoring for anomalies and actively blocking threats all day, every day. We take an active approach to securing your data and employ the proper safeguards to ensure its safety.

Privacy

It is our goal to capture and store only the minimal amount of sensitive data required to provide exceptional services, or as required by law or regulation. Our privacy policy dictates that we are only permitted to share participant data in three limited circumstances: if participants specifically allow it, if it's required to deliver a product or service, or if we're required by law to disclose data. See the full policy online at https://financialengines.com/legal-information.

Credit Card Protection

Under the Fair Credit Billing Act, your bank cannot hold you liable for more than $50 of fraudulent charges. If your bank does hold you liable for any portion of the $50, Financial Engines will cover the entire liability for you, up to the full $50. Financial Engines will cover this liability only if the unauthorized use of your credit card resulted through no fault of your own from purchases made at financialengines.com while using the secure server. Please note that depending on the level of service you are receiving from Financial Engines and whether the service is being made available through your employer, you may not need to provide Financial Engines any credit card information.

How you can protect yourself

Always use strong and unique passwords. This cannot be stressed enough. With computing power at an all-time high, attackers can easily crack weak passwords in seconds and leverage previously breached credentials on other websites. This may sound like a daunting task, but you don't even need to remember passwords anymore. You should use a password manager which essentially keeps all your passwords secure (encrypted) and helps you create different, strong passwords for each one of your accounts. There are many free and very user-friendly versions available.

Keep your devices up to date. Attackers are always finding new and inventive ways to bypass security controls and techniques. Likewise, technology companies are constantly improving security controls and patching newly identified flaws to thwart attackers' future attempts. Updating your devices in a timely manner is the best method to secure vulnerable systems.

Routinely backup your devices. This is a time-honored tradition in the IT field but one that all users should follow. Not only does backing up your device protect you in the event of a malicious compromise, but it will also protect you from accidental failure. Storage devices can and do fail.

Think before you click. You should incorporate the concept of "zero trust" as it pertains to emails and the links contained within them. Attackers have a swath of tools to create legitimate looking emails. It's crucial to investigate unexpected emails and assume all links could potentially lead to a malicious website. Follow industry guideline best practices by opening websites manually to investigate further (if needed); do not use the links within the email unless you are confident the sender is who they say they are.