D A DAVIDSON

D.A. Davidson Companies Information & Cyber Security

D.A. Davidson Companies and its subsidiaries are committed to protecting your privacy and security information. Our technologies follow a security strategy that is designed to utilize industry best practices.

Controls and Protections

Our comprehensive security strategy is designed to protect D.A. Davidson data from threats by using perimeter, network and systems-level protections, data access controls, and third-party partner protections. We also use internal auditing and external consulting resources to test our systems, and participate in securities industry tests.

Risk Management

D.A. Davidson maintains an information and cyber-security program designed to protect confidential information, including clients' non-public personal information. Our firm's program includes a dedicated team of information technology security professionals as well an internal control structures designed to minimize the risks of cyber-attacks or potential compromise of confidential information. In addition, we engage third parties to periodically test our external defenses, and auditors periodically review our control environment. Our firm maintains an Incident Response Committee, Plan, and regularly test in the event of a security breach.

Account Security

At D.A. Davidson, we use several layers of security designed to protect your information. We use technologies designed to keep your data secure when you review your account online. We employ industry best practices to help ensure the integrity of our systems and the safety of your information. Additionally, we encourage our clients to proactively take precautions to keep their information safe and secured.

Employee Training

Each D.A. Davidson employee is required to complete annual information security training. Training topics include: prevention of data loss, detection of fraudulent activity, and procedures for verifying the identity and authenticity of a client request. We believe in providing every D.A. Davidson employee with the knowledge to help protect client information.

Leadership Commitment

D.A. Davidson's leadership team is focused on security matters through active participation in numerous industry programs, including the SIFMA security roundtable. Members of our leadership team serve on the company's Response Committee, and the executive team is apprised regularly of security audit updates. By working closely with D.A. Davidson leadership, we are able to offer exceptional service to our clients.

Privacy and Security

D.A. Davidson is committed to protecting your privacy and security. The information below highlights how we protect your privacy and security, as well as ways you can protect yourself.

Privacy notice

- Our privacy notice explains how D.A. Davidson collects, shares and protects your personal information.

How we safeguard your information — online and mobile

- Passwords
  - D.A. Davidson requires you to choose a unique user name and password to access your account information online or through a mobile device. This is one way we can verify your identity to prevent unauthorized account access.

- Information access
  - D.A. Davidson computer systems are protected by layered security devices that block unauthorized access. This means that no one without the proper web browser or mobile application configuration can view or modify information contained on our systems. Only authorized people – employees, advisors, approved contractors, etc. – can use D.A. Davidson computer systems. Only people who need to know confidential client information have access to that information.

- Information we may request from you
  - When you initiate contact with D.A. Davidson by phone, to safeguard accounts and verify your identity, we may ask you to confirm certain personal information. Your advisor will not call and ask for personal information on an unsolicited basis. Additionally, we will not request your personal information in an email and will not send emails requesting you to reply in the body of an email with personal information, such as a password, your Social Security number, account numbers, mother's maiden name, etc. Do not respond to, open an attachment, or click on a link in an email if you suspect the message is fraudulent or unsolicited.

- Secure Web/Internet sessions, encryption and security questions
  - D.A. Davidson uses a variety of security features, including the features listed below, to help protect your account information:
    - **Secure sessions and encryption**
      - We require that a secure session be established any time you supply or access personal or confidential information, such as when you log in to view your accounts. A secure session is established using Transport Layer Security (TLS) technology, which encrypts the information sent between your computer and D.A. Davidson. Only computing devices with web browsers that are compatible with SSL Technology and support encryption can be used to access your account information online.
      - Here's what to look for online to ensure a secure session has been established:
        - Address bar: Secure pages on our sites will start with https (rather than http).
        - Padlock symbol: Secure pages on our sites will display a small padlock icon in the bottom right corner of the browser window.
        - When you have finished using a secure area of D.A. Davidson, make sure you log out to end the secure session. To further protect your personal information, we will automatically log you off after a period of inactivity.
    - **Security questions**
      - If you use our online sites to access your accounts, we require you to select three security questions and create answers that only you will know. If we ever need to verify your identity, we'll ask you to answer one of these questions. These questions and answers provide another layer of protection for your accounts.

- Secure email messaging
    - Mimecast is an email application that D.A. Davidson employees use to securely send messages to clients. It offers built in security and privacy features that allows your financial advisor and members of his/her staff to send you sensitive information in a secure manner.

Protecting yourself

- Passwords
    - Consider these password tips to take extra measures to protect your accounts:
        - Create passwords that include numbers, symbols and special characters, and use longer passwords to make them harder to crack.
        - Avoid common words because some hackers use programs that try every word in the dictionary.
        - Don't use your personal information, your login name, or adjacent keys on the keyboard as passwords.
        - Change your passwords regularly and don’t use the same password more than once.
        - Don't use the same password for each online account you access.
        - Don’t share your password and don’t use the “remember my password” option on any computer that is not used solely by you.
    - Creating a strong password
        - One way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers or symbols that resemble letters.
- Be aware of spyware
    - Spyware is software that may be installed on your computing device without your consent to monitor the way you use your computing device. It can be used to display pop-up ads, send you to websites you did not mean to visit, monitor the websites you visit or even record keystrokes. By recording keystrokes, spyware may be used to record your usernames and passwords.
    - Clues that spyware may have been installed on your computing device are:
        - Onslaught of pop-up ads
        - Your browser taking you to sites you did not enter in the address box
        - A change to your Internet home page that you did not make
        - New toolbars are on your browser
        - New icons in your browser window
        - Keys that don't work properly
        - Random error messages
        - Slow performance when opening programs or saving files
    - Tips to help protect your computing device from spyware
        - Update your operating system and web browser software to make sure you have the latest protection.
        - Only download free software or applications from sites you know and trust.
        - Don't install any software without knowing exactly what it is.
        - Set your security setting to at least “medium” to avoid unauthorized downloads.
        - Avoid links in pop-up windows.
        - Don't click on links in spam that claim to offer anti-spyware software.
        - Install a personal firewall to stop uninvited users from accessing your computer.
    - How to get rid of spyware
        - If you think your computer might have spyware on it, follow these steps:
            - Get anti-spyware software from a vendor you know and trust, choosing one that can undo changes spyware makes to your system.
            - Set it to scan on a regular basis — at least once a week — and every time you start your computer, if possible.

        - Delete any software programs the anti-spyware program detects that you don't want on your computer.
- Anti-malware and firewalls
    - Anti-malware software and a firewall can help protect you when you make financial transactions online.
    - Anti-malware software works by removing or quarantining suspected viruses. It is best to choose a solution that updates automatically so you don’t have to worry about ensuring the software is up-to-date.
    - A firewall functions much like a fire door in a building by preventing unauthorized parties to access your computer or network. It is important to set up your firewall properly.
- Personal information and phishing
    - Phishing refers to the unlawful and fraudulent attempt to acquire sensitive information, such as usernames, passwords, Social Security numbers and credit card information. Phishers send email or create pop-up windows posing as reputable companies, such as Internet service providers (ISP), banks and online payment services, and ask consumers to update, validate or confirm account or other personal information on a website that looks legitimate.
    - **Consider these tips to help you avoid phishing scams:**
        - Don’t reply to or click on links in email or pop-up messages that ask for personal information. Legitimate companies will not attempt to collect personal information outside of a secure website. If you are concerned about your account, contact the organization mentioned in the email or pop-up.
        - Use anti-malware, anti-spyware software and a firewall. Some phishing emails contain software, such as spyware, that harm your computer or track your activities on the Internet. Anti-virus software and a firewall can help protect you from inadvertently accepting such unwanted files.
        - Don't email personal or financial information. Regular email is not a secure method of transmitting personal information. Some companies, including D.A. Davidson, offer a secure email service that you can use when you need to exchange sensitive information.
        - Use caution when opening attachments or downloading files from email. These files can contain viruses or other software that can weaken your computer's security.
    - **Providing personal information to aggregators**
        - Other companies offer aggregation websites and services that allow you to consolidate your financial account information from different sources (such as your accounts with us and/or with other financial institutions) so you can view all your account information at one online location. To do this, an aggregation provider may request access to Personal Information, such as financial information, usernames and passwords. You should use caution and ensure the aggregator company has appropriate policies and practices to protect the privacy and security of any information you provide or to which they are gaining access. D.A. Davidson is not responsible for the use or disclosure of any Personal Information accessed by any company or person to whom you provide your Client Access username and password.
        - If you provide your Client Access username, password or other information about your accounts with D.A. Davidson to an aggregation website, we will consider that you have authorized all transactions or actions initiated by an aggregation website using access information you provide, whether or not you were aware of a specific transaction or action.
        - If you decide to revoke the authority you have given to an aggregation website, we strongly recommend that you change your password to Client Access to ensure that the aggregation website cannot continue to access your account.
- Keeping your accounts safe – For additional tips, FINRA has published a document entitled “Keeping Your Account Safe – Tips for Protecting Your Financial Information” on its website at www.finra.org: FINRA.

Report lost or stolen Checks/ATM/debit cards or credit cards
Contact United Missouri Bank (UMB)
Credit Cards - 800.821.5184
Debit Cards and Checks - 800.842.8950