GHP Investment Advisors, Inc.

Personal Wealth Management | GHP Global Markets

www.ghpia.com

11 Ways to Protect Your Accounts from Fraudsters

GHP Investment Advisors and our custodians have a variety of safeguards in place to monitor and protect your accounts. However, fraudsters often access personal information directly from individuals. But you can take simple steps to thwart scammers seeking to harvest your data.

Do Not Click Links in Phishing Emails. These emails may appear to be from a trusted source. They create a false sense of urgency to scare you into entering login credentials or clicking on a link. Never enter secure information through an email link or click to open attachments. Access your account via your browser using the URL address you normally use. Fake emails may contain spelling or grammar errors, addresses from strange domains, or names of companies where you don't have accounts.

Avoid Fake Websites. These websites look like sites you visit frequently, and the URLs may be close to the authentic address. They often contain links that may prompt you to enter usernames, passwords, or payment information. You should access all websites directly by typing the URL address in your browser.

Establish Login Credentials Immediately. Even if you prefer not to manage your account information online, by not setting up login credentials, you provide an opportunity for a fraudster to beat you to it. If you choose not to manage your account online, contact the provider to determine if you can freeze online access.

Establish Two-Factor Authentication. Many websites now use this security method, which involves a unique, one-time-only code (usually sent to your phone via text) along with your login credentials before granting access to your account. This is an extra layer of security that makes it difficult for anyone to access your account even if they obtain your credentials.

Use Longer Passphrases. Technology has made it easier to crack 8- to 10-character passwords. And scammers can crack common passwords, such as pet names, children's names, or even the word "password," without the use of technology. A longer passphrase that includes punctuation, capitalization, and spaces adds complexity and may be easier to remember. "My favorite vacation spot is Disneyland!" is easier to recall than "2Qa5aTFP!", reducing the likelihood that you will write it down.

Use Different Passphrases for Each Account. People tend to use the same password for multiple accounts. Using the same password for your email, bank account, and gym membership may make your passwords easier to remember, but it also means that if someone hacks into your gym's system and steals your username and password, you may have handed them the password to your bank account.

Keep Login Credentials Free of Personal Information. Avoid using personal information, such as birthdays or Social Security numbers, when setting up usernames and passwords. A fraudster with access to pieces of your personal information has a better chance of accessing your accounts if the information is incorporated into your credentials.

Avoid Common Passwords. If your password is 123456, qwerty, password, 1111111, abc123, 123123, 0, iloveyou, 1q2w3e4r5t, Monkey, Dragon, or other common variations on these, change it today.

Monitor Alerts. Charles Schwab and Fidelity Investments, the custodians of your investment accounts with GHPIA, send out real-time email alerts to notify you of any activity or changes made to your account If you receive an alert notifying you of a change or money movement transaction you did not authorize, please contact our Client Relations team as soon as possible.

Regularly Update your Security. Be sure that all your mobile apps and web browsers are upgraded to the most recent updates. You should also run regular virus scans in order to detect any potential malware you may have installed unknowingly.

Avoid Public Wi-Fi. Public internet connections are unsecured and have become another tool fraudsters use to try to obtain your information. Be sure you are connected to a private, secure Wi-Fi connection before accessing any sensitive accounts online.

If you believe you've received an email from a fraudster posing as a custodian of your accounts (such as Charles Schwab), please contact GHPIA immediately. Please do not hesitate to reach out to us with questions.

For more tips on how to combat identity theft and data breaches, read our July 2019 post (https://ghpia.com/worried-about-the-capital-one-data-breach-heres-how-to-protect-yourself/).