TRUSTCORE

illuminate the possibilities.

Preventing Cybercrime and Identity Theft

Unfortunately, cybercrime continues to rise, and criminals continue to evolve in their craft. Here is some information to help you avoid being a cybercriminal's next victim.

What TrustCore does to help protect your identity:

- ✓ When processing a request for you, we may reach out to you to verify information regarding that request with you verbally.
- ✓ We use dual-factor authentication extensively across our technology platform.
- ✓ We limit access to your information by only granting permissions to persons who require this information to process transactions, open accounts or secure other services for you.
- ✓ We utilize standing instructions for our clients' accounts held by Charles Schwab & Co., Inc. for wire transfers, ACH money transfers or check requests.
- ✓ When utilizing DocuSign for an electronic signature, we utilize dual-factor authentication via a mobile phone number on file for you.
- ✓ We may use steps to verify your identity if you call our office and request balance or asset information on any of your accounts.

What steps you can do to help protect your information:

Logins and Passwords:

- ✓ ***Never share your login or password information with others!***
- ✓ If you have a *smart phone,* be sure to have a ***passcode*** on the ***device***.

- ✓ *Don't reuse passwords* across accounts or websites that contain sensitive personal information that could be used to impersonate you or steal your identity.
- ✓ Whenever possible, use a *dual-factor authentication choice*, rather than a single password login to accounts or websites that contain sensitive personal information.
- ✓ Keep your passwords secure – don't use a word processing file, contact file or notes program on your phone, tablet or computer to keep your list of passwords. Consider an *encrypted password protector* program to provide an extra layer of security for your password information.
- ✓ If your password protector program will automatically prefill your password for you, *copy and paste* it instead to prevent keystrokes from being monitored on your device.
- ✓ ***Avoid*** logging into any site that maintains personal information about you *when using public WiFi.* Use your smart phone's hotspot instead.
- ✓ Use a combination of upper-case letters, lower-case letters, numbers and special characters when creating your passwords. *Don't use common words found in the dictionary*
- ✓ ***If you suspect any suspicious activity in your investment accounts, please contact our office immediately.***
- ✓ ***If you discover your e-mail has been compromised, please let us know. This will allow us to use alternate methods to contact you while you resolve your e-mail issues.***

E-mail

- **Phishing**
  - Phishing e-mails attempt to obtain sensitive information, like usernames, passwords or credit card information by looking very much like they are originating from a trusted source.
  - These e-mails will generally request you ***"click on the link"*** and complete the information.
  - Unfortunately, the link is taking you to a sight that looks legitimate but is not. Once you click the link, you are giving away your information.
  - If you receive a request like this, ***DO NOT click on the link***. Instead, go directly to that sight and see if there are any issues with your account.

- **Spear-Phishing**
  - Spear-phishing utilizes extra information to make the e-mail look legitimate.
  - Spear-phishers will *use information they find out about you*, often from a social network (Facebook, LinkedIn, Twitter, etc.) and send you a document or file that needs ***IMMEDIATE ATTENTION.***
  - Once you ***"Click on the link"*** malware or spyware can start downloading on your device. Often, these programs run in the background and log keystrokes and enable the hacker to get to know you.

Telephone

- When you receive a call from a number you do not know, or an unidentified number, the caller or automated system may ask, "Is this John Doe?"
- You naturally want to say "Yes," ***but don't!*** Criminals can use your "Yes" against you by trying to impersonate you on the phone to steal your identity or your money.
- Ask the caller to identify themselves before you go any further.
- If a ***service representative*** calls you, especially an unsolicited call, hang up and call the company back at a number known to you.