Keeping Clients Cyber Safe

December 14, 2018

Cyber fraud is on the rise, with high net worth individuals natural targets due to their wealth and the level of exposure that attracts. More so than other, high net worth individuals have broader circles of “Associated Persons” e.g., financial advisors, accountants, lawyers, etc. to whom they transmit financial information over emails and other communication channels. While Associated Persons don’t have direct responsibility for their client’s cyber protection, sharing best cyber practices with your clients is at best assisting with your fiduciary obligations and at a minimum, demonstrating your interest in helping to protect their identity and confidential information.

You may wish to share these five tips with your clients to help them keep safe:

1. Enlighten clients on the impact of sharing on Social channels.

Social media has provided a platform to share personal information with nearly no limits. Over exposing personal infomration enables criminals to keep track of activities which can be used to perpetrate fraud or create profiles that mimic a clients’ persona.

2. Advise clients to consider layered controls. You may not be able to influence how frequently your clients change passwords or other basic safeguards, but providing common sense tactics might resonate well. Examples of layered protection may include encouraging clients to only use a designated home-based computer for logging into financial sites. Another example is creating a throw-away email account for one-off online interactions to reduce SPAM (and phishing attempts) in a primary account. Or paying for online transactions with a low limit credit card only vs. a debit card, can also reduce liability. Encouraging these types of actions can raise awareness and provide a layered approach to being cyber safe.

3. Guard home network connections. Phones, PCs, and even appliances are susceptible to cyber crimes. Networks like Bluetooth and WI-Fi are common and especially vulnerable. Securing networks with passwords only is not enough; it is advisable to encrypt them with firewalls and also make them undiscoverable.

4. Avoid public WI-Fi networks for sensitive data transmittal. Unencrypted networks allow hackers unrestricted access to any unsecured devices. Everything you do can be tracked, and passwords, as well as credit card and financial details, may be easily stolen. Resist the need to check bank balances until back on a secure network or VPN.

5. Recognize children are most vulnerable. Monitoring and restricting their social media use, limiting what they post online as well as having a good understanding of the applications used in the household are necessary steps to curb these concerns.

It’s important for your clients to recognize that as technology continues to evolve, so does cybercrime. Most fraud is aggravated by the use of poorly secured networks and poor human awareness and lack of proper decision making.