Cyber Security

October 14, 2016

We live in a world that is more connected than ever before and the internet touches almost all aspects of everyone's daily life, whether we realize it or not. Over the past several years there have been numerous cyber breaches of personal information. This is a trend that will continue to grow as the worldwide use of technology expands. Some notable companies that have been hacked recently include Yahoo, Home Depot, EBay, Target, Adobe, and JPMorgan Chase. The Department of Homeland Security and the FBI, two agencies that are charged with the task of protecting Americans from cyber-crime were hacked and sensitive personal information of about 29,000 employees was posted online[1].

Cyberspace is particularly difficult to secure due to a number of factors including the ability of criminals to operate from anywhere in the world, the large amount of information online, and the difficulty in reducing all vulnerabilities in computer networks. Cyber-attacks have increased 48% since 2013[2]. Odds are that you or someone you know has had their personal data compromised. Usually the breached company will provide a complimentary credit monitoring service for a limited amount of time, but this in many cases is just a short-term solution as the data has already been disseminated. Unfortunately we are living in a world now where personal information is available for those who know how to access it. However, you can be proactive and protect your personal information as human error can pose a significant risk to having your information compromised.

Privacy and safeguarding your information are of paramount importance to Carmichael Hill. We have a continuing obligation to respect the privacy of our clients and to protect the security and confidentiality of client nonpublic personal information.

Here are some protective measures that Carmichael Hill has implemented to keep your personal data and information secure:

- We do not provide your personally identifiable information to vendors or solicitors for any purpose (unless required by law).
- We have a secure office environment; only employees have access to client data.
- We have a secure encrypted in-house server with no "cloud" access.
- Our employees are trained to recognize cyber security threats.
- We verify money movement directly with clients and will probe any unusual requests.

Schwab, the custodian of your assets, takes a number of measures to protect you as well:

- Offers a Security Guarantee – under most circumstances Schwab will cover 100% of any losses in your accounts due to unauthorized activity. Beware that you as the client must safeguard your account access information and report any unauthorized transactions as quickly as possible
- Complies with federal laws regarding security measures including computer safeguards and secured files and buildings while continually monitoring systems and working with law enforcement to address potential threats
- Uses encryption technology and dual authentication login requirements
- Implements advanced analytical systems that continuously adapt to detect suspicious activity
- Makes sure that their employees are trained and well-informed

Listed below are some additional measures that Carmichael Hill is taking that you can take as well to protect yourself from cyber-crime:

- Make sure your virus protection, spyware/malware programs, and firewall are active and up-to-date.
- Maintain your operating system updates to close vulnerabilities.
- Make sure your passwords are complex. Using 12 characters instead of 6 significantly increases the chances that a hacker will be discouraged and go for an easier break-in. Change your passwords at least every 90 days. Do not give your login credentials to anyone and find a secure spot offline to keep the passwords private.
- Password protect or encrypt personal data when sending it over the internet.
- Do not open emails, links, or attachments from strangers.
- Be alert for scammers especially strange 'phishing' emails asking for personal data or for you to click links and open attachments.
- Don't download software that you are unfamiliar with.
- Lock your computer, tablet, and cell phone when you are away.
- Make back-ups of all of your important work and keep them in a safe or safe deposit box.
- Report any suspicious activity on your accounts immediately.

You should also make sure that you are:

- Not oversharing on social networking sites
- Being very cautious on public networks and public Wi-Fi – we recommend against joining these networks since they are not secure
- Reading privacy policies for companies that have your personal information to see exactly how they are protecting you

The Carmichael Hill Privacy Policy is available upon request. Please contact us for any questions about how we are safeguarding your personal information.

- Jeff Grodsky, CFP®, QKA

Footnotes

1 – nbcnews.com - 2/9/2016

2 – FPA Conference Baltimore – Snow, Christensen & Martineau "Data Security In Financial Services: How to Stay Protected" 9/16/2016