1919 INVESTMENT COUNSEL
Complexity to Clarity
100 YEARS

# Data Point

## Online Security

**December 11, 2018**

Recently, the disturbing news of yet another high-profile data security breach broke across all major news outlets. Specifically, Marriott was hacked, exposing the sensitive personal data of approximately 500 million guests.

We realize that news such as this is of grave concern to many of our clients, which is why we want to share insight into those things you can do to minimize your risks as you travel through an increasingly complex digital landscape.

While it is impossible for you to completely insulate yourself from hackers, it is possible to be prudent and follow best practices that work to make you less vulnerable online.

As with other recent large data breaches, some of the data exposed often includes usernames and passwords for websites. With this in mind, please remember that you should never use the same password across multiple websites. You should never use your corporate network or email password, for example, for any external websites you use for personal banking, shopping, etc. Using the same password across multiple websites can easily make your entire personal network vulnerable in the event of a single initial data breach.

Consider a data breach such as the recent ones with Marriott or Yahoo takes place and usernames and passwords are compromised. Assume your username is bobjones@gmail.com and you have a password of “Autumn1989”. A hacker will immediately go to Gmail and attempt to log in with these credentials. If successful, they will have access to all of your emails and contacts. They will also attempt to use these stolen credentials at major banking institutions, such as Bank of America, Wells Fargo and Chase, as well as retail outlets such as Target, etc. A single data breach could expose your accounts at other places that were not part of the initial hack.

Our recommendation is to do whatever you can to create longer and more complex passwords with combinations of letters, numbers and symbols. Best practices also include changing your passwords on a periodic basis. Generating and remembering all of these passwords can be extremely difficult, but applications such as Lastpass, Dashlane and Keeper are all appropriate solutions that provide a secure vault for all of your passwords and ensure they are unique across the websites you log into during your online sessions. A simple internet search for any of these applications can provide details on the services offered and their cost.

With so many facets of our daily lives now including online interactions with people, institutions and systems, this may all seem challenging to manage, but at the same time makes it critically important that you follow these recommendations. The time, effort and money you spend looking into these solutions can be among the best investments you make to help protect yourself online and allow you to rest more comfortably when data breaches such as the Marriott instance happen in the future.

Please know we are vigilant on the topic of data security and take our role and responsibility of protecting the private information you share with us very seriously. To learn more about how to safeguard yourself from hackers, please feel free to contact us.