CYBERSECURITY:
The "Other" Financial Planning Topic

Often in the wealth management industry, discussions with clients tend to focus on investments, insurance and planning for retirement. Commonly overlooked, however, are steps taken to safeguard those planning elements, as well as making sure personal information and records are kept away from nefarious characters or those who would seek to utilize your private information for their own personal gain. Potentially the most important aspect of that protection in the present day is recognizing the need for strong personal cybersecurity for you and your family.

Just 20 years ago, personal cybersecurity was only starting to come into existence with the advent of the dotcom boom. At the time, crimes like identity theft were largely comprised of individuals diving through dumpsters trying to find bank statements. Computer viruses had only just begun making their way onto home devices. Times have changed dramatically, and in our now internet connected society, the need for individuals and businesses to be mindful of the risks associated with cybersecurity, and to take proactive measures to ensure they are protected, is more important than ever. Given that in 2017 alone there were 1,579 data breaches exposing roughly 158 million records and social security numbers, it's no coincidence that 78 percent of companies view cyber risk as the largest threat to the broader economy.[1]

At first glance, those numbers can seem daunting, leaving the average consumer feeling a bit helpless in finding how best to protect his or her information. So what can be done to keep yourself safe? Here are a few tips to get you started.

First and foremost, staying informed is key. Threats can come from a variety of different places and are changing all the time. There are some general rules and practices you can follow to significantly reduce the odds of an attack on you or your family. Making sure you utilize different passwords for your accounts, that they are kept in a safe location and that they meet the complexity requirements typical of websites and institutions are good first steps.[2] Password vaults are a great way to handle this task as you can keep all of your passwords in one secure place and only have to remember one password to get into the vault (just make sure you don't forget that one).[3]

Second, when it comes to ongoing protection, there are two simple steps that can help you be better protected while online. Turning on automatic updates for your browsers, systems, and applications is an easy way to make sure the software you are using reflects the most recent iteration from the developer.[4]

Mariner WEALTH ADVISORS

It's not uncommon for web and app developers to include bug fixes and new security protocols with each update. Making sure those changes take place automatically is key. Another easy step to staying continuously protected is installing an ad-blocker onto your browser.[4] This can reduce the risk of accidentally clicking on an advertisement or email attachment containing malicious software, also known as malware.[5] Similar to a computer virus in causing slower processing speeds and even the covert transmission of your private information to outside parties, malware is certainly something to be avoided.[5] In one of the more recent additions to the realm of cybersecurity threats, ad-blockers can even prevent your computer's processor from being used to mine cryptocurrency without your knowledge, either by visiting certain websites or having a hidden pop-up on your screen.

A third important tip in maintaining good cybersecurity practices is being aware of where you are accessing the internet. Coffee shops, libraries and other public places now commonly offer free WIFI internet for patrons, thereby encouraging people to visit. While convenient for those with limited data plans or hoping to save battery life, public WIFI networks that don't require a password can be a significant security risk for those who use them. Because there is no restriction to accessing the network, a hacker can virtually place themselves between you and the actual internet connection, gaining access to anything you transmit in the process.

For those who travel regularly, this can present a significant problem because you may not have access to protected networks. To overcome that problem, you should consider investing in a mobile hotspot or contacting their phone carrier to activate it as a mobile modem, thereby creating a WIFI hotspot. While there are additional costs involved in both options, the resulting internet connection is much more secure and may be worth the cost for heightened protection.

With a topic so complex, the points discussed only scratch the surface of the many considerations in keeping your online presence and personal information secure. Thankfully, there are a variety of resources you can access to learn more about the steps you can take to be better prepared, including our Your Life, Simplified podcast. You can listen to our episode on cybersecurity by clicking HERE.[6]

[1] https://www.nytimes.com/interactive/2018/09/12/business/the-next-recession-financial-crisis.html?rref=collection%2Ftimestopic%2FComputer%20Security%20(Cybersecurity) & https://www.experian.com/blogs/ask-experian/identity-theft-statistics/
[2] https://www.cnet.com/how-to/how-to-check-the-strength-of-your-passwords/
[3] https://www.cnet.com/news/the-best-password-managers-directory/
[4] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
[5] https://us.norton.com/internetsecurity-malware.html
[6] http://www.marinerwealthadvisors.com/insights/cybersecurity-is-your-personal-financial-information-protected

Mariner WEALTH ADVISORS