Finance

by Clarissa Krinsky, MD< CFP®, ClariFinancial
www.clarifiplanning.com

ClariFinancial

A Guide to Safe and Secure Online Banking

Are you ready to go paperless? There are many benefits of online banking, including access to your financial documents, decreased fees, less postage, automatic bill pay and integration with other software programs for taxes or budgeting, environmental benefits of less paper use, and less clutter.

Hard copies carry the risk of identity theft through stolen paper statements in the mail or in your home, car, etc. Electronic copies carry the risk of identity theft via hacking or online scams. Financial institutions are vested in protecting your (and their) money and have created significant safeguards. In addition, there are many steps you can take to maximize your online security.

For secure online banking, you should not use public computers or wireless (wi-fi) access and should password protect your own wireless network at home or work. If you are logging in on your phone, use your cellular data rather than wi-fi.

Other safety measures include maintaining antivirus software on your computer at home, keeping as little secure information on your desktop as possible, using encryption software for any data you do store on the computer, and always using safe and secure passwords.

Since most financial institutions keep your statements available for up to seven years, you can always pull them off the websites if you need them. For the long-term storage of other documents, they should be backed up and stored in a separate physical location to protect them from fire, theft, or other hazards. Of course, cloud-based storage solutions can be wonderful alternatives to keeping documents in your home or on your computer.

We all know we need safe and secure passwords. But how? There are excellent password apps for your mobile devices that store passwords with secure encryption. This is likely a safer alternative to having passwords in writing or kept elsewhere. This helps you keep track of passwords. These tools also encourage complex and regularly updated passwords. I also recommend using different passwords for your financial log-ins than those you use for other places where security may be less stringent, such as your email or online shopping sites.

Another security measure is to request 2-factor authentication, which is offered by most banks. This may include having a unique code sent to your phone to provide extra confirmation of your identity. While it may add a little time (seconds) to your log-in, it is much less time than you will spend on the aftermath of identity theft.

Lastly, never send financial data via regular email. Most financial advisors or professionals will have encrypted emails or secure portals for you to use in lieu of email. And, of course, never provide any financial information in response to an email that seems to be from your bank. Many scams operate this way to get your bank information. If you get such an email, report it to your bank immediately.

It can be a little work upfront, but once you go to online banking, you'll likely never go back. Good luck!