Cyber Security in an Insecure World

I recently attended the annual educational conference put on by my broker dealer, Commonwealth. It is an event that I look forward to every year as the speakers they engage and topics that are addressed are always timely and excellently presented. This year was no exception as I was able to hear directly from individuals like David Gergen, a Senior Political Analyst with CNN and former Federal Reserve Chair Ben Bernanke.

As good as the presentations were, the moment that I will remember most from this conference was standing in my hotel room that Friday night watching the live coverage of the Paris Terrorist attacks. Events like that tend to be understandably etched in our brains and, standing in a downtown Washington DC hotel as I was, the reality of the threat took on extra resonance.

In the wake of the attacks in Paris and the more recent tragedy in California, security is on the forefront of many people's minds. Unfortunately I suspect this is an issue that we will continue to face for some time as the types of threats continue to evolve. While there are things that each of us can do to help be vigilant and aware of what is going on around us, the heavy lifting of keeping us physically safe rests with those who work in the various branches of protective services and they clearly deserve our gratitude.

While threats of physical violence are in the headlines, don't forget that there are other types of threats that we face every day. Cyber security is a very real concern, both for our national infrastructure and the safety of our personal information. There are things you can and should be doing to help safeguard yourself.

Most of us tend to hear stories about things like identity theft and credit card fraud and think that it will never happen to us. We see stories about celebrities having their email hacked and think that no one would ever do that to us because we aren't famous. Why would someone want access to our email? Predators prey on attitudes like that to take advantage of people every day.

About a month ago I received an email from a client requesting that I send money to a vendor for her to pay off a recent purchase. She asked that I email her the paperwork so she could fill in the instructions for where the money was to be wired. The request was very plausible for this particular client but we have strict procedures in place that require a verbal authorization any time money is going to be sent somewhere other than directly to the client. When I relayed this the response I got indicated that she was at a funeral and not going to be available to talk.

I immediately picked up the phone and called the client. She answered on the first ring, at home, exactly as I suspected. Her email had been hacked and the perpetrator had read through enough of her prior correspondence to learn that I was her financial advisor and that I commonly send her money.

Sadly, this is the second time I've had an experience like this with a client. Fortunately, Commonwealth has protocols in place to foil these attempts but not all firms do. While I would suggest that that you check with your bank and other financial institutions to see what type of security procedures they have in place, there are also a number of steps that you should be taking to proactively keep yourself safe.

The first line of defense is often your password. We may find it irritating to constantly have to set up passwords and to try to keep track of them all but they really are important. A good rule of thumb is that passwords should be hard to guess but easy to remember. A good password should be at least eight characters long, contain both letters and numbers, not be a word and not be based on personal information like the name of a family member or a birthdate.

Be suspicious of unsolicited emails, especially if the email tries to scare you into action by threatening to close an account or report something to a credit rating service. As many of these types of attempts originate outside of the United States you may be able to identify them by things like grammar and spelling errors. Don't be fooled into thinking it is legitimate just because it looks the part though. If you are ever sent an email asking you to follow a link and then enter personal information like social security or account numbers follow the same procedure that we do for clients. Pick up the phone and contact the institution directly.

The prevalence of mobile devices like smart phones has opened a new potential opportunity for cyber predators. Make sure that you keep your mobile operating system and any apps that you have up to date by taking care of any updates when they come out. Most systems will make it easy by notifying you when a new update is available. Often those updates are related to security issues so make sure that you do them.

For the first time ever, more people shopped online this Black Friday than did in stores. Shopping online can be very convenient and more and more people are doing it, but make sure that you use safe practices. Make sure that your browser is updated and that you have current security software in place. Try to only shop on reputable sites that you are familiar with and when entering payment information ensure that you are on a secure site by checking for the "https://" before the "www".

Sadly, security threats are likely to continue so it is important to remember that you are your own first line of defense. For more tips and tricks to stay safe online, visit the National Cyber Security Alliance at www.staysafeonline.org.

Trisha Arndt, CFP®, is President of Wealth Strategies of Wisconsin Ltd, 901 Kimball Lane, Suite 1400, Verona, WI 53593, 608-848-2400. Securities and Advisory Services offered through Commonwealth Financial Network, member FINRA/SIPC, a Registered Investment Adviser.