Take it to eleven with two factor authentication (2FA)

April 4, 2018 2FA, Cyber Security

In a prior post I talked about how your need to up your game in terms of password management. In this post I will talk about taking the management of your online identities to the next level. I'm not going to dance around on this issue – in addition to a solid password, you really should be using two factor authentication whenever possible.

The next level of sophistication in password management is called "two factor authentication" (referred to hereafter as 2FA). This essentially requires a password as your line of security, and then an additional and unrelated level of authentication, in order to access a web site or resource.

Some common examples of 2FA include, in roughly ascending order of security:

- Security questions (example: what was your high school mascot?)
- Sending an email to you with a onetime use code.
- Send a text message to your cell phone with a onetime use code.
- A code generator application.
- Voice recognition / Face recognition

The security question method has been around for several years. The weakness of this system is that there are a limited number of questions in the world. These types of questions are easily "socially engineered". For example, "what was your high school mascot?" adds a false sense of security given that this information can be reverse engineered for most people with a profile on LinkedIn, FaceBook, and other social networking web sites. In addition, if you have unique question and answer combinations that you use, and those become compromised, you are vulnerable and may not even realize it.

The email method has numerous weaknesses, including but not limited to the fact that email is itself fairly insecure. Many hacks start with taking over an email account, and then doing password resets (which send the reset to the email address of record). If you lose control of your email account, it can be chaotic process to get control back.

The use of text messages to cell phones have become popular as a means of 2FA. Please know that there is a risk associated with this. Cells phone accounts have a number of vulnerabilities, the most serious of which is called a "cellphone hijack". In this scenario, someone uses social engineering to take over your cell phone, and then use 2FA to access your accounts. (The hack goes something like this: the hijacker calls your cell carrier to say "I lost my cell phone, and I'm desperate, can you transfer my cell number to my new phone?")

The most secure / widely used method of 2FA is the password generating application. This is sometimes in the form of a small device you carry with you (companies like RSA SecureID and Symantec VIP Access have been providing this service to corporations for years). This is sometimes in the form of a proprietary application that is tied only to that one service – for example Yahoo Mail, GMail, and

basic premise is that a unique code is generated (and constantly recycled) that is unique to you and your device. It is much hard to hijack this type of 2FA.

There is a 1984 movie called "This is Spinal Tap". It was one of the first "spoof documentaries", and chronicled a hard rock band. There is a memorable scene in which one of the lead characters discusses the amplifiers that they use, which have a unique feature: volume nobs that go to 11 instead of the normal 10. I realize that it's a goofy clip, from a goofy movie. What I'm hoping is that the reference is just memorable enough to drive home this one idea: it is time for you to up the level of your online security. It is time to take it to eleven with 2FA.

Your Password Stinks

April 3, 2018 2FA, Cyber Security

Don't take this personally, but your password stinks

Please don't take this the wrong way, but the passwords you use on the internet every single day probably stink. Do not despair, read on because there is a fix.
Let's face it, passwords are a major pain in the backside to keep track of. Every web site that you visit will ask you to create a new user id and password. It quickly becomes daunting. All too often we take the easy way out.

The most common crutch that we use is reuse. We use the use the same password. Again. And again. Rinse, lather, repeat. The problem with this approach is that once that password becomes compromised, the bad guys may have access to your bank accounts, your investment accounts, your online shopping accounts. The list goes on. Anywhere that you used the same combination of user id and password, you are vulnerable. Say for sake of argument that you have a Yahoo! email account that was compromised. (Oh wait, that actually happened.) Now the hackers have a combination of user id and password that they can, with minimal effort, try to use on an infinite number of web sites.

There are other crutches that we use: we write down our passwords (FYI: don't do this!), we use short

words that you can find in the dictionary (FYI: definitely don't do this), we never change our passwords (FYI: you should change your password regularly). The list could go on and on.

I am speaking from personal experience. Full mea culpa: I used the exact same user id and password for years. I used it on name brand websites such as Yahoo! Mail. I used it on fly by night websites where I thought to myself "this web site probably won't be here a year from now". I've used it on "once and done" transactions on web sites that I knew I would only visit once in my lifetime. Eventually this behavior came back to haunt me. Someone used those reused credentials on an eCommerce site, and ordered themselves a laptop. I had forgotten that I even had a login to that web site, so you can imagine my surprise when I received an email with an order confirmation for a new laptop. When I went to go and reset my password, the web site actually sent me an email with my "old" password. This was painful confirmation that it was the same user id and password that I used…everywhere.

There is a better mousetrap. Password management systems.

I'm not a big fan of the Firefox, Google Chrome, and Internet Explorer password mechanisms. However, there are a number of well-regarded solutions that will track your passwords, regardless of how you're accessing the internet.

There are 2 primary functions that these services provide: first, they are a master repository of your passwords, and secondly, they allow you to generate long and completely random passwords.

I personally have used LastPass (www.lastpass.com) for several years (ever since the hacking mentioned above). There are a number of other well regarded services such as 1Password (www.1password.com), Dashlane (www.dashlane.com), RoboForm (www.roboform.com), as well as about a dozen others.

There is one final gotcha with password management systems. You need to create a "master" password to get into that system. Some of these systems add extra security by having no password recovery mechanism for the master password. If you forget your master password, you are completely locked out. The method that I have found to work is to have a long pass phrase, that only you know, and that you abbreviate into the password. For example, you can start with a quote such as "If not us, who? If not now, when?" You might turn that into "if<>Uwif<>Nw?3000". The key is to make it personal, something that you will remember, but that is impossible to guess.

Summary

There is no other way to explain it, you simply need to do a better job of creating and managing your passwords. We often use shortcuts of various forms to help manage our passwords, to our own detriment and peril. Know that here is a better way. A password manager can help.

My "Why" Story – Circa 2010

April 2, 2018 Uncategorized

My "Why" story, circa 2010: The story of a career change

I am fond of saying that I rarely do something for only one reason. My decision to change careers and become a financial advisor is no exception. After 15 years in the tech world, I recognized that my chosen career path was not fulfilling in the way that I wanted it to be. Through long soul searching

In a parallel and serendipitous set of events, I was approached by a family member that was aware of my affinity for the financial markets. It was early in 2008. The markets had been falling since late 2007, and had further to go. My family member had fairly simple questions and needed honest answers: Am I doing well? (In my opinion, no.) Am I getting sound advice? (In my opinion, no.) Am I well diversified and holding the right types of investments? (In my opinion, no.) Could I be doing better? (In my opinion, yes.) Do I have enough money to support my retirement? (Most likely, yes.)

That portfolio belonged to my grandparents. They were my first client, and I am eternally grateful for some of the lessons that I learned from them. They modeled some incredible behavior (personal, and as well as financial), and from who I developed my first mantra for thinking about client advice: *is this something I would do for my grandparents?*

This project I embarked on with them, finding and framing answers to important questions, was a pivotal moment for me. I found the experience to be thoroughly rewarding. For me, it was as if a light had been turned on in a dark room. I realized that by basing a financial advisory business on honest and relevant advice, I could deliver significant value and develop meaningful relationships with the people I worked with while having a positive and sometimes dramatic impact on their lives. I also realized that in a time of uncertainty and sometimes turbulent markets, that these services were relevant to almost everyone I knew.

I believe in a few fundamental principles of personal finance and investing: live below your means, revisit your goals regularly, invest wisely and for the long term, re-balance and reevaluate your investments at regular intervals.

These might seem like simple concepts on the surface, but in everyday life they are often difficult to implement and live by. *Simple, but not easy.*

I strongly believe that my number one priority is to give honest and accurate advice that always serves the best interests of the client. I enjoy helping people plan and invest to achieve their financial goals.

If that is the kind of relationship you would like to have with a financial advisor, I look forward to talking to you.

Chris Duke
August 31, 2010