Phishing scams, credit card skims, and computer hacks. The cyber criminal is flourishing. While it may be impossible to completely protect yourself from cybercrime, there are few steps that should always be in your toolbox. One of the main problems that can lead to compromised personal information is poor use of passwords. This includes using the same password for all (or many) of your logins, too simple of a password, and not changing passwords regularly. I know it's a pain in the neck (believe me as I have some 200+ sites with user IDs and passwords) but it's important enough to put up with the inconvenience (the alternative is a much bigger pain, and much lower). A couple of tips for passwords:

- They should be at least 8 characters long
- Include both letters and numbers
- Include both upper- and lower-case letters (if able)
- Include special characters such as @$!& (if able)
- Have a password keeper to keep track of your current (and old) passwords
    - This can be either written (please don't store it in the open next to the computer) or an app.

Already been compromised? Contact a reputable technology provided to look over your computer for viruses, contact your credit agencies, and call your financial advisor if you feel your investment account is at risk.
----Chuck

Cybersecurity

Protecting yourself from potential calamity.

Provided by Charles D. Vercellone, ChFC

Cybercrime affects both large corporations and private individuals. You've likely read about the large data breaches in the business world. These crimes are both expensive and on the rise. The U.S. Identity Theft Resource Center says that these corporate data breaches reached a peak of 1,632 in 2017. The response to the growing need for data protection has been swift and powerful; venture capitalists have invested $5.3 billion into cybersecurity firms.[1]

That's good news for the big companies, but what about for the individual at home? What can you do to protect data breaches to your personal accounts?

For most private individuals, the key idea is to both:
* Know what to do if you've had a data breach.
* Know what you can do that might help prevent a data breach.

Total cybersecurity for your financial matters isn't something that can be strategized in a single short article like this one, but I would like to offer you two suggestions that can help you get started. Both can be done from home and represent *reactive* and *preventative* measures.

Credit Freeze. By *reactive*, I mean that a step that you can take after the fact. In many cases, a credit freeze might be a reaction to identity theft or a data breach. What it specifically does is restrict access to your credit report, which has information that could be used to open new lines of credit in your name. The freeze prevents this, but it will not prevent a criminal from, for instance, using an active credit card number, if they've discovered it. For that reason, you still have to monitor for unauthorized transactions during the freeze.[2]

While the freeze is in place, you can still get your free annual credit report. You also won't have issues with credit background searches for job or renter's applications or when you buy insurance – the freeze doesn't affect those areas of your credit history. You can even apply for a new line of credit during a credit freeze, though that requires a temporary or permanent elimination of the freeze during the process. This can be done through either a call to the big three credit reporting agencies (Equifax, Experian, and Transunion) or a visit to their respective websites.[2]

Password Manager. This is a *preventative* measure. Yes, we all know the poor soul who uses "Password" as their password. While you are probably not that far gone, the truth is that there are many tricks that cybercrooks use to learn or intuit our passwords. In fact, 20% of Internet consumers have experienced some sort of account compromise. That comes at a time when about 70% of consumers operate 10 or more accounts. A few, against best practice, will use the same password across each of those accounts. A good security measure against that is password manager software – applications that allow us to keep all our numerous passwords encrypted in a vault and drop them into our browsers when requested. While yes, there are options to save these passwords, encrypted on most browsers, these security measures are limited. Password managers are focused solely on security and are more frequently updated than the browser security features might be. That attention might be difference between a criminal obtaining access to your sensitive personal information or being blocked in the attempt.[3,4]

While this is a very basic pair of tips, they are worth thinking about and may prove to be helpful in your efforts to prevent identity theft. There are, however, additional, more-advanced choices for you to explore. Talk with your trusted financial professional about other cybersecurity best practices that you might consider.

any investment or insurance product or service, and should not be relied upon as such. All indices are unmanaged and are not illustrative of any particular investment.

Citations.

1 - forbes.com/sites/forbestechcouncil/2019/10/09/the-need-for-a-breakthrough-in-cybersecurity/ [10/9/19]
2 - consumer.ftc.gov/articles/0497-credit-freeze-faqs [9/2019]
3 - wired.com/story/best-password-managers/ [9/25/19]
4 - digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic [12/18/18]

Charles D. Vercellone, ChFC
Wealth Strategies Group, LLC
200 E Big Beaver, Troy MI 48083
248-680-4622
chuck@wsgllc.net
www.wsgllc.net