SEPTEMBER 2019

Cyber Theft: The Modern-Day Pickpocket

CONTRIBUTOR
Ryan Stuart
Business Director

WEALTHMANAGEMENT
WHITE PAPER

The past 12 months have been marred with a number of high-profile cyberattacks (CapitalOne, Facebook, First American Corporation, and even the credit reporting agency Equifax). With the number of attacks on the rise, many cybersecurity experts believe it is not a matter of if you will be exposed to a cyberattack, but when. In this article, we aim to educate you on the types of fraud being perpetrated and some simple precautions you can take.

Fakebook: A cyber-story

Beverly Beauregard sat quietly in her usual spot near the front of the bus on her way home from playing pickleball with her social club. Her eyes were glued to her tablet as she scanned her social media feed for new pictures of her grandkids or tweets from her favorite political pundits. She noticed a message from a name she remembered from childhood… one she hadn't heard in years.

Jillian Friedman had been her next-door neighbor and best friend as an adolescent. Beverly and Jillian had lost touch over the years, but Beverly was pleasantly surprised by the contact and anxious to reconnect. After some messaging back and forth, Beverly learned that Jillian had come down with some serious medical issues and could not afford proper treatment. Beverly had accumulated a modest nest egg to fund her retirement and wanted to help her long lost friend any way that she could. The funding gap was $75,000 and although this was a sizable chunk of change for Beverly, she wanted to help.

Beverly insisted on meeting face to face with Jillian to catch up and go through the details. Jillian agreed to meet, but said that she needed the funds immediately and pushed the meeting back until after the procedure. Jillian provided the bank account information for the generous donation and Beverly quickly worked with her financial advisor to raise and transfer the funds.

The operation day came and went and Beverly had not heard from Jillian. Beverly began to fear the worst. When she called the hospital, she was told they had no record of Jillian Friedman as a patient. She then called Jillian's bank to inquire about the account and learned that all funds had been withdrawn and the account was closed. Just like that, Beverly fell prey, like countless others, to a sophisticated and deftly executed "social engineering" cyberattack.

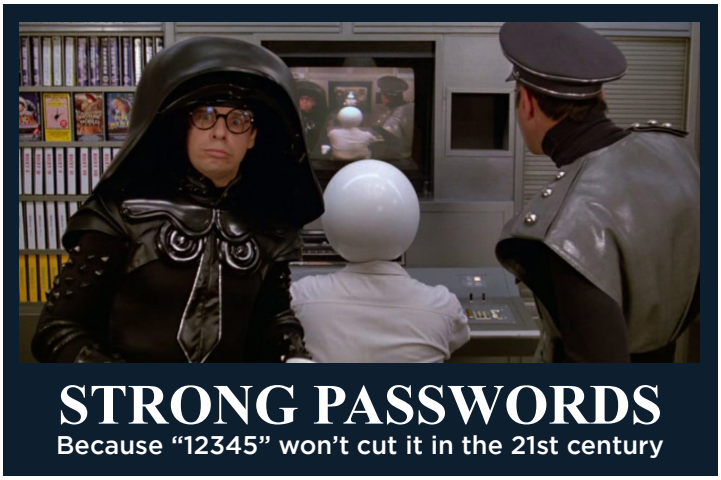
Global Cyber Risks: "The combination to the air shield is 12345"

In the 1987 Mel Brooks Star Wars parody, "Spaceballs", the evil Spaceball empire, who over-polluted their planet, is seeking to steal all the fresh air from the peaceful, neighboring planet Druidia. The Spaceballs ransom the Druish princess, coercing the King to divulge the secret password to the planet's air shield...

"The combination to the air shield is 1 2 3 4 5" [King Roland]

"That's the stupidest combination I've ever heard in my life. That's the combination an idiot would have on his luggage!" [Dark Helmet, Spaceballs General]

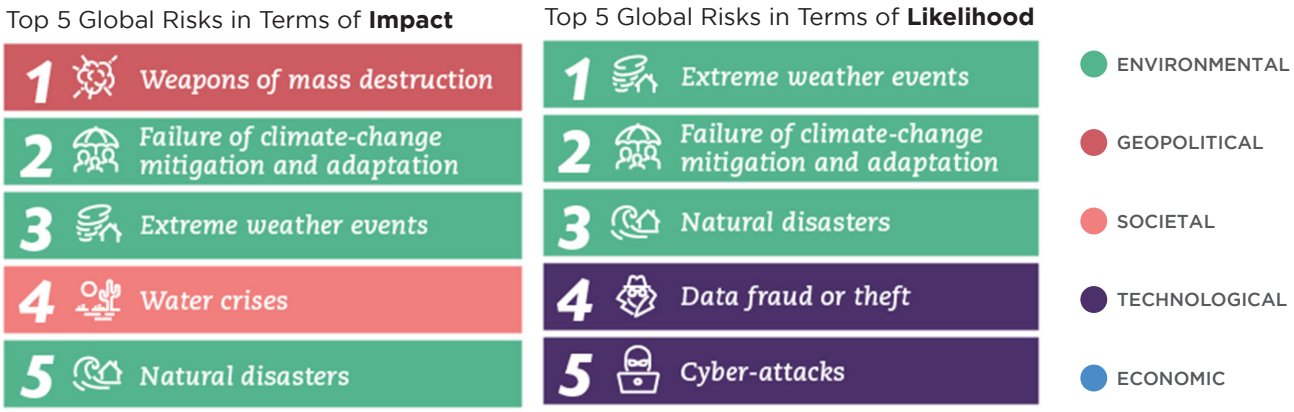
"1 2 3 4 5? Amazing! I have the same combination on my luggage." [Spaceballs President]



Coincidently, or perhaps even presciently, thirty years later exposing weak passwords and waging ransom-based attacks remain common tactics for cybercriminals. CNN Business reported on the top 10 most frequently used passwords. Not surprisingly, five of the ten are consecutive numbers, with others involving sequential letters or the word "password". While a weak, easily guessed password may not lead to loss of the Earth's atmosphere, it could certainly lead to exposure of sensitive information or financial ruin.

The 2019 Global Risk report, published for the World Economic Forum in Davos, Switzerland, recently cited technological risks as two of the top five global risks in terms of likelihood, trailing environmental risks only. A decade ago, negative impact from economic events was viewed as the most likely risk. It wasn't until 2012 that technological risk even made an appearance. This observation highlights the societal paradigm shift that accompanied our growth and reliance on technology. Indeed, Gartner, Inc estimates that "internet of things" devices will reach 20.4 billion by 2020, each being a potential entry point for a data breach[1].

The Global Risk Outlook for 2019



SOURCE: World Economic Forum – Global Risks Report 2019

www.visualcapitalist.com/top-global-risks-2019/

Closer to home: It's getting personal

Cyberattacks are real and are happening more than most of us realize. There have, of course, been some high-profile data breaches in the news, such as Equifax, Facebook, and most recently, CapitalOne. Odds are that one or more of these affected you. In fact, 60% of Americans report they or an immediate family member have fallen victim to a scheme to defraud, according to research from The Harris poll and the American Institute of CPAs.[2]

Financial institutions are obvious targets for cyberattacks. According to Boston Consulting Group, financial services firms are targeted 300 times more than any other type of company.[3] Then why be concerned by data breaches on social media platforms such as Facebook or Reddit? It is probably not so the assailant can log on to your Facebook account and change your status or post an embarrassing picture.

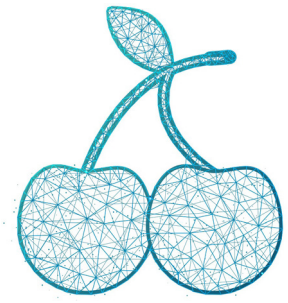
It's more likely to be a scheme such as "Credential dumping" - when a hacker uses stolen username and password combinations to systematically test logins to hundreds or thousands of online platforms (usually financial) using automated computer algorithms. The hope is that the victim uses the same login credentials across multiple accounts. Here is a good place to pause and self-evaluate. Would credential dumping work on you? If the answer is yes, your homework is to update any repetitive or easy to guess passwords to unique, secure passwords. We give some practical advice on setting strong passwords and managing credentials later.

Cyberattack strategies are constantly evolving and can take many forms. The figure below illustrates some of the broad categories of cyber threats. If you are not up to speed on the cyber-lingo, see the National Institute of Standards and Technology's computer security glossary. According to the Financial Conduct Authority, phishing and ransomware attacks are the most reported types of cyberattacks on financial services firms comprising 52% and 20%, respectively.[4]

Financial gain, of course, is the primary goal of these attacks. According to a 2018 study by Dr. Michael McGuire, who works in the Criminology department at Surrey University, a conservative estimate of the global cybercrime economy is $1.5 trillion annually.[5] With that sort of financial incentive, we don't expect cybercrime to go away any time soon.

COMMON CYBER THREATS

SOLUTIONS 2019
Charles Schwab Advisor



Don't be the low-hanging fruit

Last year, Ginni Rometti, IBM's CEO, stated that "cybercrime is the greatest threat to every company [and in the next the five years, every person] in the world." While this sounds like a phrase that could be written on the cardboard sign of a psychotic street-side apocalyptist, the statement holds some merit. Cybercrime damages are anticipated to reach $6 trillion by 2021. This number "represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."[6]

DON'T BE THE LOW-HANGING FRUIT CONTINUED

Misappropriation of data from a major financial firm might be the "holy grail" for cybercriminals, however companies which house large amounts of sensitive data also have the best defenses. According to an estimate from cybersecurity experts, IT security spending could hit $124 billion in 2019, up 8.7% from last year.[7]

Cybercriminals have therefore discovered other more accessible targets. In 2019, the FBI issued a warning to raise awareness that the elderly demographic makes up the majority of successful cyber scams.[8] The warning is based on an observation that seniors are more susceptible to attacks as they are more likely to have cognitive impairment, health issues, and generally be less sophisticated with technology than younger generations. Coupled with the fact that many seniors have amassed retirement savings, you can see why they are prime targets.

Fortunately, there are some simple precautions everyone can take to identify and abate these attacks. According to Cybint, a cyber solutions company, 90% of cyberattacks are due to human inexperience or error and could be avoided.[9]

- **Do not use the same password for multiple logins.** A password manager (e.g. LastPass) can help you organize your credentials.
- **12 characters minimum on passwords,** including numbers, symbols, and upper and lower case characters. Password managers have a handy feature that will automatically generate a random password of a given length and complexity.
- **Periodically change your passwords.** If you have been using the same password for over a year, it is time to change it.
- **Use two-factor authentication.** You should have this enabled on all accounts where this option is available (e.g. your Schwab, TD Ameritrade, Client Portal accounts, etc.). Please contact us if you need help setting this up. We are happy to assist.
- **Use good judgement when opening unknown emails.** If you do not recognize the sender, or the domain name, ignore and delete the email. If you do recognize the sender, but weren't expecting a message from them – especially if they are asking you to open an attachment or follow a link – ignore and delete the email. If it is a legitimate message, and it is important, they will contact you by phone or some other method.
- **Never give out username, password or personal information over email.** Financial firms, mortgage/title companies, the IRS, etc. will never ask for your social security number, username, password, date of birth, etc. over email. If you receive a message requesting this type of information, it is likely a phishing attempt.
- **Use anti-virus and anti-malware software.** Fortunately, if you are running Windows version 10 or later, the operating system has Windows Firewall and Windows Defender automatically built in. Similarly, MacOS includes Gatekeeper, XProtect and malware removal tools.

- **Consider purchasing identity protection.** If you feel you are a particularly high-risk target or simply want the comfort of some added defense, you might consider purchasing identity protection (such as LifeLock). These services monitor transactions at banks, wireless carriers, payday lenders, and black-market websites to alert people when there is suspicious activity or if fraudulent accounts are opened.

- **Regularly check your credit score and financial accounts.** The three credit reporting agencies (TransUnion, Equifax and Experian) will issue a free credit report at least annually. Be aware of what appears on your credit score. If you find an error, work with the agencies to correct it. You should also regularly examine bank or investment account statements, credit card statements and other financial information to be sure all transactions are recognized. If you find anything amiss, notify your financial institution immediately.

WT Wealth Management's commitment

According to the SEC, 74% of advisors have experienced cyberattacks either directly or through one or more of their vendors.[10] It is no longer a question of if an attack will happen, but when. According to an IBM report examining the financial impact of data breaches, an average breach involved 25,000+ computer records, $8.19 million in costs and took 279 days for the company to become aware of the breach. Moreover, the study found that small and midsize businesses (fewer than 500 employees and annual revenues of less than $50 million) suffered the worst financial consequences on a relative basis at an average cost of $2.5 million per breach. Further, companies are 31% more likely to experience a data breach today than in 2014.[11] With all of that in mind, here are some things that WT Wealth Management is doing to protect your information:

- All client data is housed on off-site cloud computing platforms and datacenters using fully redundant data storage, internet and power infrastructures. All data is transmitted securely using 256-bit SSL and is encrypted.

- All firm computers are protected and monitored by state-of-the-art firewall, anti-virus and anti-malware protection.

- All employee logins to platforms holding client data require two-factor authentication.

- Vulnerability scans are performed at least annually by all third-party software vendors.

- Firm policy requires verbal confirmation of any move money request.

- Incoming emails are screened using industry best practice techniques, such as IP block lists, to filter messages containing phishing and other types of scams.

- Staff are trained annually on cybersecurity best practices and developments.

- WT Wealth Management specifically insures for cyber risks and periodically reviews this coverage to ensure it is sufficient and appropriate.

CONCLUSION

As we continue to increase our reliance on technology and the interconnectivity of our digital lives, it is clear that cybercrime will continue to grow as a key global threat. Fortunately, there are measures you can take, and measures WT Wealth Management is already taking, to decrease the chances of falling victim to cyberattacks. Protection of your sensitive information is a top priority for us and we are dedicated to ensuring that our policies, processes and systems keep your information safe.

As we learned in this article, cybersecurity is a two-way street. We hope that you take advantage of the simple steps described herein to avoid falling prey, like Beverly and countless unsuspecting others, to a costly, yet avoidable, cyberattack.

If you need help with your security settings or would like more information on how we keep your information safe, please do not hesitate to contact us.

Info@WTWealthManagement.com • 800-825-0616

SOURCES

[1]*www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016*

[2]*www.aicpa.org/press/pressreleases/2018/nearly-half-of-americans-say-id-theft-likely-to-cause-them-finan.html*

[3]*www.ciodive.com/news/cyberattacks-hit-financial-services-300-times-more-than-other-sectors/557372/*

[4]*www.zdnet.com/article/phishing-ransomware-are-top-cyberattacks-on-financial-services-firms/*

[5]*www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/*

[6]*www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf*

[7]*www.darkreading.com/2019-security-spending-outlook/d/d-id/1333826*

[8]*www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-elder-fraud-in-arizona-top-five-cyber-crimes-targeting-arizona-seniors*

[9]*www.cybintsolutions.com/employee-education-reduces-risk/*

[10]*www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf*

[11]*www.dailyvoiceplus.com/westchester/westchester-business-journal/latest-news/ibm-average-data-breach-costs-us-companies-819m/773320/*

DISCLOSURE

WT Wealth Management is an SEC registered investment adviser, with in excess of $100 million in assets under management (AUM) with offices in Flagstaff, Scottsdale, Sedona and Tucson, AZ along with Jackson Hole, WY and Las Vegas, NV.

WT Wealth Management is a manager of Separately Managed Accounts (SMAs). With SMAs, performance can vary widely from investor to investor as each portfolio is individually constructed and managed. Asset allocation weightings are determined based on a wide array of economic and market conditions the day the funds are invested. In an SMA, each investor may own individual Exchange Traded Funds (ETFs), individual equities or mutual funds. As the manager we have the freedom and flexibility to tailor the portfolio to address an individual investor's personal risk tolerance and investment objectives – thus making the account "separate" and distinct from all others we manage.

An investment with WT Wealth Management is not insured or guaranteed by the Federal Deposit Insurance Corporation (FDIC) or any other government agency.

Any opinions expressed are the opinions of WT Wealth Management and its associates only. Information offered is neither an offer to buy or sell securities nor should it be interpreted as personal financial advice. Always seek out the advice of a qualified investment professional before deciding to invest. Investing in stocks, bonds, mutual funds and ETFs carries certain specific risks and part or all of an account's value can be lost.

In addition to the normal risks associated with investing, narrowly focused investments, investments in smaller companies, sector and/or thematic ETFs and investments in single countries typically exhibit higher volatility. International, Emerging Market and Frontier Market ETFs, mutual funds and individual securities may involve risk of capital loss from unfavorable fluctuations in currency values, from differences in generally accepted accounting principles or from economic or political instability that other nations experience. Individual bonds, bond mutual funds and bond ETFs will typically decrease in value as interest rates rise. A portion of a municipal bond fund's income may be subject to federal or state income taxes or the alternative minimum tax. Capital gains (short and long-term), if any, are subject to capital gains tax.

Diversification and asset allocation may not protect against market risk or investment losses. At WT Wealth Management, we strongly suggest having a personal financial plan in place before making any investment decisions including understanding personal risk tolerance, having clearly outlined investment objectives and a clearly defined investment time horizon.

WT Wealth Management may only transact business in those states in which it is registered, or qualifies for an exemption or exclusion from registration requirements. Individualized responses to persons that involve either the effecting of transactions in securities, or the rendering of personalized investment advice for compensation, will not be made without registration or exemption. WT Wealth Management's website is limited to the dissemination of general information pertaining to its advisory services, together with access to additional investment-related information, publications, and links.

Accordingly, the publication of WT Wealth Management's website should not be construed by any consumer and/or prospective client as WT Wealth Management's solicitation to effect, or attempt to effect transactions in securities, or the rendering of personalized investment advice for compensation, over the internet. Any subsequent, direct communication by WT Wealth Management with a prospective client shall be conducted by a representative that is either registered or qualifies for an exemption or exclusion from registration in the state where the prospective client resides.

A copy of WT Wealth Management's current written disclosure statement discussing WT Wealth Management's registrations, business operations, services, and fees is available at the SEC's investment adviser public information website (www. adviserinfo.sec.gov) or from WT Wealth Management directly.

WT Wealth Management does not make any representations or warranties as to the accuracy, timeliness, suitability, completeness, or relevance of any information prepared by any unaffiliated third party, whether linked to WT Wealth Management's web site or incorporated therein, and takes no responsibility therefor. All such information is provided solely for convenience purposes and all users thereof should be guided accordingly.

Bloomberg® is a trademark of Bloomberg Finance L.P. (collectively with its affiliates, "Bloomberg"). Barclays® is a trademark of Barclays Bank Plc (collectively with its affiliates, "Barclays"), used under license. Neither Bloomberg nor Barclays approves or endorses this material, guarantees the accuracy or completeness of any information herein and, to the maximum extent allowed by law, neither shall have any liability or responsibility for injury or damages arising in connection therewith.

MSCI does not approve, review or produce reports published on this site, makes no express or implied warranties or representations and is not liable whatsoever for any data represented. You may not redistribute MSCI data or use it as a basis for other indices or investment products.

The S&P 500 Composite Index ("Index") is a product of S&P Dow Jones Indices LLC and/or its affiliates and has been licensed for use by Capital Group. Copyright © 2018 S&P Dow Jones Indices LLC, a division of S&P Global, and/or its affiliates. All rights reserved. Redistribution or reproduction in whole or in part are prohibited without written permission of S&P Dow Jones Indices LLC.