Forward Share Tweet Share

EMPYRION™

WEALTH MANAGEMENT

Creating Wealth by Intentional Design

August 5, 2021

Monthly Insight

Why Cyberattacks Increased During the Pandemic, and What It Means for Your Online Safety

As if the COVID-19 pandemic hadn’t already caused enough problems, experts are warning that the public health crisis and the resulting move to remote working has created another type of crisis: online security. Hackers and cybercriminals, always swift to respond to any change that could potentially create vulnerabilities in online defense systems, have raced to exploit the chinks in corporate, governmental, and other networks that have resulted from the practically overnight migration to the internet for processes and workflows that were formerly handled either in-person or on closed networks.

As millions of workers began using home wifi, unsecured laptop and desktop computers, personal mobile phones, and other “home remedies” for their jobs, hackers quickly moved in to take advantage of the many opportunities this offered to penetrate the online defenses of various entities, including some of America’s largest corporations and even governmental agencies around the world.

In a recent special report by the Wall Street Journal, global IT leaders indicate, by a vast majority, that the move to remote working and the so-called “hybrid workplace” has made them more vulnerable to cyberattacks. By margins well over 80%, they say that practices of remote-working employees such as allowing others to use their work devices, use of software not approved by the company’s IT department, and the simple use of personal devices for work have greatly increased their risk of a security breach. A May 2021 report released by Verizon Communications indicated that attacks against cloud-based email, remote desktop applications, and similar technological services increased markedly during 2020.

Several reasons contribute to the increased vulnerabilities present in the remote and hybrid workplace. One of the most prominent is the fact that remote workers often don’t stay current on installing patches: the software updates regularly sent by developers to strengthen the weak spots in programs that hackers use to gain unauthorized access to data and systems. Not only do remote workers tend to pay less attention to newly released patches, but as many people began returning to the office after the first of the year, they were firing up machines that had been sitting idle for months—time during which many vital patches were not being installed. Also, as they work remotely, many individuals connect work devices to public wifi networks, which are notoriously ripe for exploitation by hackers. For example, a March survey of 3,000 workers by AT&T found that over half had used work devices for personal business such as online banking, and many performed these activities on public, unsecured networks.

Evidence of increased activity by hackers is easy to find. Johnson & Johnson, the pharmaceutical and healthcare giant that developed one of the three primary COVID-19 vaccines, has estimated that its cybersecurity systems and processes handle something like 15 billion potential attacks each day. This includes malware that is automatically detected and disabled, attempted logins that are flagged as potentially problematic, so-called "phishing" attempts, and others. And last December, the Scottish environmental protection agency fell victim to a ransomware attack that required them to completely overhaul their software system.

What does this mean for consumers and others who may work for a company that could be targeted, who use its products or services, or whose data could be compromised if one of these companies experiences a security breach? As usual, the answer—for the time being, at least—lies in taking greater personal responsibility for keeping safe online.

A good place to start is by remembering how much anyone—including cybercriminals—can learn about you simply from public internet sources. Your social media profile on sites like Facebook, Twitter, Instagram, and others can tell hackers things they need to know in order to construct an online snare for you and even for the company you work for. Did you post an image showing you and your colleagues back in the office for the first time since the shutdown? How about that cute puppy picture you "liked"? The news article you retweeted? Hackers can use all these bits of information to devise ways to trick you or someone you know into giving them information. You might get an innocent-looking email that references details of your recent experiences, asking you to click on a link—which then implants spyware or other malware on your computer. Be cautious about posting details on travel, personal matters, or other information that could make it easy for online bad guys to impersonate you or someone close to you.

Another obvious—and under-utilized—line of defense is maintaining good password practices. It's still easy, even now, to walk into someone's office and spot yellow sticky notes bearing letters and numbers that are obviously passwords to internet sites. The easy solution to keeping your passwords out in the open is twofold: use passwords that are hard to guess—like those generated automatically and randomly by your software—and manage your passwords with a secure program. The main objection that many people have to using strong passwords—
"I can't remember all those numbers and special characters"—is alleviated by the use of a secure password management program. When using a password manager, you only have to remember your master password, and the program does the rest of the work for you. And many password management programs do more than just keep up with your passwords; they can also alert you if a site you use has experienced a data breach, so you can change the password for that site; they can remind you to update passwords on sites with mandatory password change requirements; and they can perform other tasks on an automated, secure basis, relieving you of many of the tasks that can make using a password manager seem like a hassle.

Finally, it's a good idea to use two-factor authentication whenever possible. This involves not only entering your username and password when logging in, but also responding to a prompt on another device, such as a security code sent as a text message. Multi-factor authentication makes it much more difficult for hackers to gain access to your company's email account, databases, or other sensitive sites. Additionally, most sites now require some form of multi-factor authentication when you reset a password or even when you log in using your existing credentials. It takes a little extra time, but it's worth it when you consider the time and expense involved in recovering from a data breach.

Your financial safety and security—online or otherwise—is my chief concern. To learn more about how I help clients build and maintain sound financial strategies to accomplish their most important goals, please click here. And to read more about staying safe online, read my recent article by clicking here.

Stay Diversified, Stay YOUR Course!

SOCIAL MEDIA DIGEST

In case you missed them, here is a roundup of my latest posts on social media:

In my latest blog, I share some thoughts on the personalization of medicine, and remind you that your #financialplan will continue to be central in affording access to the latest developments in healthcare and other vital areas of life.

With the EWM Digital Investing platform, you'll see all of your investment goals in one place and always know how your investments are performing. Designed with usability in mind, test it out for yourself! #DigitalInvesting.

There are essentially three methods that companies use to sell their stock to the public: initial public offerings (IPOs), special-purpose acquisitions companies (SPACs), and direct listings. In my latest blog, I walk you through each of them. #investing

Can market volatility be your friend? In my latest Fox 40 appearance, I discuss how to take advantage of market dips. #marketvolatility

KIMBERLY FOSS

President, CFP®, CPWA®,
CFT-I™ Candidate

"We understand that every person we serve has distinct values and ambitions, and they each need their own plan for wealth management."

Empyrion Wealth Management ("Empyrion") is an investment advisor registered with the U.S. Securities and Exchange Commission under the Investment Advisers Act of 1940. Information pertaining to Empyrion's advisory operations, services and fees is set forth in Empyrion's current Form ADV Part 2A brochure, copies of which are available upon request at no cost or at www.adviserinfo.sec.gov. The views expressed by the author are the author's alone and do not necessarily represent the views of Empyrion. The information contained in any third-party resource cited herein is not owned or controlled by Empyrion, and Empyrion does not guarantee the accuracy or reliability of any information that may be found in such resources. Links to any third-party resource are provided as a courtesy for reference only and are not intended to be, and do not act as, an endorsement by Empyrion of the third party or any of its content. The standard information provided in this blog is for general purposes only and should not be construed as, or used as a substitute for, financial, investment or other professional advice. If you have questions regarding your financial situation, you should consult your financial planner or investment advisor.