July 2021

LAWYER ALERT

Stopping Medical Injustice

How to Stop the Cyber Thief DEAD in Their Tracks

There's a good chance you've been hacked.

Most lawyers are not protecting the information that they have been entrusted with, but any information that you retain is subject to being hacked. Your fiduciary duty to your clients is the highest standard of care. Cyber security is constantly evolving and cyber criminals are continually becoming more innovative. Yet most lawyers are poorly prepared for a cyberattack.

Statistics that Should Scare You

According to the American Bar Association, 26% of all law firms have been subjected to, or experienced some form of data breach involving hackers. An additional 19%, or one in five firms, admit that they don't know if they have been breached. For the remaining 55% of law firms, some have been compromised without knowing it or simply decided not to report it.

According to the American Bar Association's TechReport 2020:

- Only 43% of lawyers use encryption
- Only 39% of lawyers use email encryption
- Only 39% of law firms use two-factor authentication (authentication that requires both a password and a code to access your account)
- 65% of people reuse the same password for multiple or all accounts (Google Security Study, 2019)

If you think "it won't happen to me", you are sadly mistaken.

6 Rules for Avoiding Cyber Crime for Your Law Firm

Rule #1: Never Wire Money: Avoid wiring money—always write a check when sending money to your client. Wiring money is the most dangerous thing you can do. Do not wire money from your escrow account, as this will subject all of the money to a cyber theft.

Rule #2: ENCRYPT EVERYTHING! (or Avoid Public Wi-Fi): Free public Wi-Fi is dangerous and it's easy for a hacker on the same network to read your personal data. You should use a VPN (virtual private network) every time you connect to the internet.

Without a VPN, third parties can see your internet traffic. Public Wi-Fi connections are usually unencrypted, which means hackers and identity thieves can potentially gain access to valuable personal and company data. A VPN (virtual private network) encrypts your data and keeps it out of the wrong hands, allowing you to work safely and securely no matter where you are.

As you connect to a secure VPN server, your internet traffic goes through an encrypted tunnel that no one can

(continued on page 2)

(continued from cover)

see, including hackers, governments and your internet service provider.

"Encryption works. Properly implemented strong crypto systems are one of the few things you can rely on."

Edward Snowden

Using a VPN on your devices keeps you safe with strong encryption. With ExpressVPN, your online activity is anonymous and private and their best-in-class AES (Advanced Encryption Standard) 256 encryption means that your data is as secure as it can be. It's the same encryption standard adopted by the U.S. government and used by security experts worldwide to protect classified information.

Lost or stolen laptops are a top cause of law firm data breaches. If the laptop is encrypted, even if the laptop is lost or stolen, the information will not be accessible. Make sure every laptop used by you and your team members has encryption from ExpressVPN. Download the ExpressVPN app at www.ExpressVPN.com/setup.

Rule #3: If You Have to Wire Money: If you wire money to a client, always pick up the phone and confirm with your client the wiring instructions. You need to verify where the money is coming from and where it is going. This alone will stop the cyber-criminal.

Never receive wiring instructions via email.

Rule #4: Log Out of All Devices at the End of the Day: Log out of your email and all devices at the end of the day.

As soon as you get hacked in 1 account, the hacker knows your passwords and can access other accounts. If you suspect you've been hacked, change the password on your computer and every connected device.

Rule #5: Use a Password Manager: Use a password manager (e.g., Keeper or LastPass) to manage passwords. A password manager provides a secure way to store and find all of your passwords and only requires you to remember a single, master passphrase to gain access.

Do not use the same password or user name in multiple devices. Use difficult passwords, the longer the better. A unique password for each site can go a long way if one site gets hacked, your stolen password can't be used

on other sites. You're basically creating your own security feature.

Rule #6: Do Not Open or Respond to Suspicious Emails: Do not open any attachments in an email until you are 100% sure the sender is legitimate.

Cyber criminals find you by searching for the most successful lawyers. You have an obligation to protect your email. The cyber-criminal reads your emails and looks for emails to your clients about a settlement.

A phishing scam involves sending fraudulent emails that appear to be from a friend or a reputable company, with the goal of deceiving you into either clicking on a malicious link or downloading an infected attachment, usually to steal financial or confidential information.

Inspect all unsolicited email with a careful eye. Phishing scams are one of the most common ways that hackers gain access to sensitive or confidential information and is involved in 70 percent of data breaches (Verizon's 2018 Data Breach Investigations Report).

The 6 Most Common Cybersecurity Mistakes Made by Lawyers

Mistake #1: Failing to Buy Cybersecurity Insurance: General liability and professional liability policies usually do not insure you against cyber theft. Invest in cyber security coverage. Cybersecurity insurance requires specific written procedures.

If you inadvertently breach your fiduciary duty, don't assume that you're covered by your errors and omissions professional liability policy. When this happens, you are not practicing law. Many professional liability policies have exclusions for breach of fiduciary duty.

Cybersecurity coverage can help your law firm cover the costs related to a data breach, including privacy breach notification expenses, litigation, loss of income, and regulatory fines and penalties. Given the potentially devastating impact of a data breach, cybersecurity insurance can mean the difference between your law firm surviving a data breach unscathed or not surviving at all.

Mistake #2: Failing to have Data Prevention Policies, Software and Training: Only 34% of law firms have policies for records retention.

Does your law firm have:

- Data retention, destruction and recordkeeping procedures?
- An incident response plan to respond to a network intrusion?
- Annual privacy and information security training for employees?
- Intrusion detection software (IDS)?
- Intrusion prevention system (IPS)?
- Data loss prevention software (DLP)?
- Multi-factor authentication for remote access to email?
- Procedures for terminating user access rights as part of the employee exit process?

When you apply for cybersecurity coverage, you will need to answer these questions "YES".

Mistake #3: Failing to Educate Your Clients about Cybersecurity: Share your records retention policy with your clients and let them know what you are doing to protect their confidential and private data.

Talk about cyber security with your clients, e.g., "You will never receive an email from me asking for money."

Mistake #4: Failing to Monitor the Internet Activity of Your Employees: Even if you follow meticulous practices for encrypting email and online activity, your law firm won't be safe from cybercrime if your employees are violating your cybersecurity policies. Especially for employees who work remotely, there are plenty of opportunities for hackers to steal your firm's confidential data.

Monitoring your employees' internet

(continued on page 3)

activity is the best practice to ensure that your employees are not violating your cybersecurity policies.

Mistake #5: Failing to have a Business Recovery Plan: Your law firm should prepare for the possibility of disaster by having a business recovery plan in place and test it at least annually. Additionally, routinely back up your data and maintain a copy at an off-site, secure location.

Mistake #6: Failing to Give Bad News to Clients Immediately: If you have a cyber security breach, do a Zoom meeting with your clients and explain what happened. ABA Model Rule 1.4 requires that you give bad news to your clients ASAP. This will help you avoid a legal malpractice case.

American Bar Association's Formal Opinion 483 entitled: "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" states:

> When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach….

A data breach means a data event where material client confidential information is misappropriated, destroyed, or otherwise compromised. A data breach may belong or relate to the representation of a current or former client.

Cybersecurity Policy for Email Messages

What This Is: This is a policy dealing with email messages that you may receive to maintain our law firm's cybersecurity.

Why We Do It This Way: Email creates vulnerabilities for our law firm's security and we must be mindful of it. If our security systems are breached, a cyber thief can access our clients' private information, including dates of birth, social security numbers, etc. Additionally, a hacker can acquire information that will give them access to our banking information and steal money from our law firm.

Hackers do this in number ways: Email may contain a virus that allows the hackers to infiltrate the firm's data and access confidential information, with their presence unbeknown to us. A hacker may lay in wait until a substantial amount of money is received by our law firm, and then act.

How We Do This: Careful email management is critical to cybersecurity. Even if you have regular email communication with someone, BE ALERT.

If you suspect that there might have been a breach, power off your computer and IMMEDIATELY notify John Fisher. Shutting off your computer should stop access to portions of the data.

Think before you click or open an email.

DO NOT OPEN any Word, Excel or other attachments unless you are expecting it from the sender and you are certain that it is safe.

If an email seems suspicious or odd—DO NOT OPEN OR CLICK ANYTHING—check with John Fisher. Read the following website page in its entirety: https://bit.ly/2Stw44B. If you think you clicked on a phishing link, report it to John Fisher as soon as possible. We all make mistakes, but we need to fix this as soon as possible.

The longer you wait, the longer we cannot properly address the potential issue and the more potential damage we have in our system. The sooner you report, the faster we can respond to a potential threat.

Thank you, Alex Bainov, Esq., for sharing this policy!

THE MASTERMIND EXPERIENCE

...Returns to Our Nation's Capital on September 10th

Washington, DC.:
September 10, 2021

The next *Mastermind Experience* will be held on Friday, September 10, 2021 in Washington, D.C. at the Courtyard Marriott in downtown D.C., 901 L Street NW, Washington, DC.
The Courtyard Marriott opened in 2018 and has brand new accommodations, amazing rooftop views of the Capitol and is located in DC's vibrant and historical Shaw neighborhood. The Courtyard Marriott has a signature full service restaurant and a 1,700 square foot rooftop terrace and bar and 4th floor courtyard terrace.

As a member of the *Mastermind Experience*, we have a discounted room rate of $119/night for Thursday, September 9th and Friday, September 10th. To book a room with the discounted rate, call 202-408-5300 and ask for the special rate for the "*Mastermind Experience*". Our point of contact is Dominic Sanchez, head of group sales, 202-469-6355.

...Comes to an Island Paradise in the Sun-Kissed Waters of the Caribbean on February 18th, 2022

Curacao (Southern Caribbean)
February 18, 2022

On Friday, February 18, 2022, the *Mastermind Experience* will take its first

(continued on page 4)

JOHN H. FISHER, P.C.

278 Wall Street • Kingston, New York 12401
Phone 845-802-0047 • Cell Phone 518-265-9131
Fax 845-802-0052 • Toll Free 866-889-6882

Email address:
jfisher@fishermalpracticelaw.com

THE MASTERMIND EXPERIENCE

(continued from page 3)

trip to the Southern Caribbean at the stylish, elegant Curacao Marriott Beach Resort, an undiscounted gem in Curacao.

Set on 6 oceanfront acres near historic Willemstad, this all-new Curacao Marriott Beach Resort offers warm, dedicated hospitality. This tropical hotel oasis is a cultured paradise in a charming and friendly island.

Curacao has some of the most incredible beaches in the Caribbean and is home to some of the world's best scuba and snorkeling spots. You can enjoy the vibrant nightlife in the historic town of Willemstad, just 15 minutes from the Curacoa Marriott Beach Resort.

Only 15 minutes from historic Willemstad, we will have a special private catamaran tour to one of the prettiest beaches you will ever see in Klein Curacao as well as a fun ATV tour that will take you along the coast of Curacao. The Curacao Marriot Beach Resort has 2 18-hole golf courses.

There are direct flights to Curacao from New York, Boston, Atlanta, Washington, DC and Miami.

If you'd like to extend your stay beyond Thursday, February 17, 2022 and Friday, February 18, 2022, our discounted group rate of $207/night is an option.

The Mastermind Experience and The 7 Figure Lawyer Join Forces in the Big Apple!

April 7, 2022: The 7 Figure Lawyer

April 8, 2022: Mastermind Experience

(above) The world's worst golfer (me) takes to the links with my boys, Tim and Alek

If you can make it there, you'll make it anywhere. The Mastermind Experience once again joins forces with the 7 Figure Lawyer for 2 very special events in New York City on April 7th and 8th, 2022.

These 2 special events will be held on consecutive days at the Knickerbocker Hotel in Manhattan. The 7 Figure Lawyer will be held on Thursday, April 7, 2022 and the Mastermind Experience will be held on Friday, April 8, 2022.

If you've never been to Craig Goldenfarb, Esq.'s, The 7 Figure Lawyer, you need to attend this event. The 7 Figure Lawyer is special. Craig and his management and marketing team take the cover off and show you exactly how the Law Offices of Craig Goldenfarb went from 1 lawyer and a secretary to a thriving 70 employee plaintiff's injury law firm in West Palm Beach, Florida.

If you've ever wondered how a 1 lawyer firm became a powerhouse in a highly competitive market of South Florida, Craig will show you the way. On the day after The 7 Figure Lawyer, the *Mastermind Experience* will be held at the same hotel, Knickerbocker Hotel.

We are once again grateful and privileged to join forces with The 7 Figure Lawyer for these 2 special events in the Big Apple. I hope you can join us for both of these special events!