Cybersecurity 101:

Top 10 Ways to Keep Your Firm Safe

rocket matter

Introduction

Cybersecurity is more critical now than ever. Not only are law firms storing more data, but as we all become increasingly mobile it's even more of a challenge keeping clients' sensitive information safe.

So what can you do? There's a saying in the computer security business that you can live in a concrete house with no doors and no windows, but it's not going to be very useful. Well, it turns out this is a perfect analogy for what's going on with computer cybersecurity: If you wanted to ensure that your computing environments were 100% safe, then you wouldn't have very useful tools at your disposal. Think about it: You wouldn't be connected to networks. You couldn't use email or the internet. You couldn't attach to any drives used by any other system.

Obviously, this isn't an option. So, the question then becomes, "How do you pragmatically live in a digital world with appropriate levels of safety, but still not reduce your ability to work?"

This guide will help you do just that.

Just remember your firm is only as strong as your weakest link. So if you've got ten employees, then all ten people need to be on board with adopting all security measures. Share this guide with each and every one of them, and you'll be on your way to making your firm as safe as possible.

Larry Port
CEO and Founder of Rocket Matter

Train Your Staff

Training your staff is the most basic step in avoiding a cyberattack at your law firm. In October of 2017, a study conducted by the ABA GPSolo Solos & Small Firm Summit concluded that only 33% of law firms had implemented employee cybersecurity training.

One of the primary ways that a hacker can gain access to your firm's network is through an unintentional act by employees. Most of the time, they may not even realize that they've made a mistake. This is why it's imperative that each member of the team knows the severity of a possible attack and receives training on how to avoid one (including everything we cover in this guide!) In other words, it's extremely important to develop a culture of awareness.

Firm employees need to be trained to identify red flags and suspicious activity to prevent hackers from gaining access to important data. According to Mark Rasch, a lawyer and former

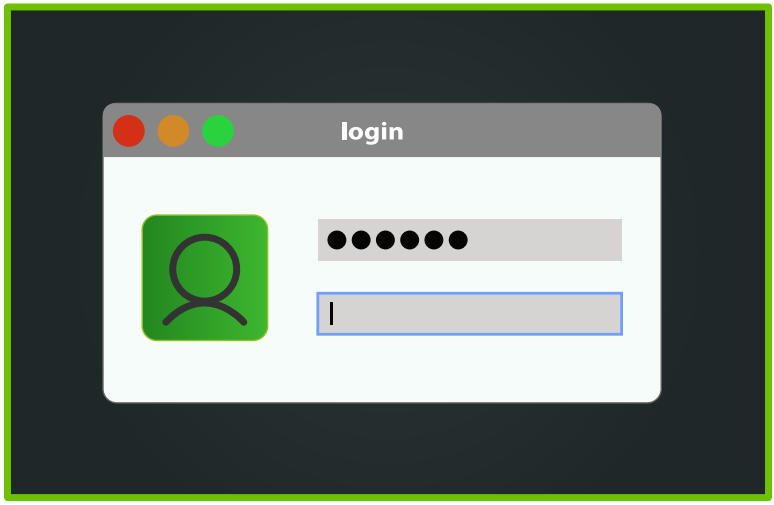
computer crimes prosecutor based in Washington, D.C., “Phishing is the No. 1, No. 2, and No. 3 threat for law firms.” Having employees who know how to spot these attempts and report them to the correct people in your company can make a world of difference.

Here are four things your cybersecurity training policy needs to address:

1. The information you care about and why it needs to be protected
2. How the information will be protected
3. Who is in charge of enforcing your policies and procedures
4. To which employees do the policies and procedures apply

More specifically, your cybersecurity policy needs to address topics such as acceptable internet usage, device and machine usage, the physical security and location of devices and machines, and contingency planning.

Only Choose Safe Passwords



So you probably know by now that having “password” or “123456” as a password is not a good idea. (Those are sadly still the two most common passwords in the U.S.!) However, any word you’d find in the dictionary really isn’t safe either. Hackers trying to break into a server or a password-protected computer sometimes use what’s called a “brute force attack” or a “dictionary attack” where they automatically enter every word in the dictionary as a password. Of course, using your dog’s name or your birthdate isn’t a good idea either—it’s too easily guessable.

Instead, best practice is to use a combination of punctuation and numbers. Try catchy phrases with numbers, and use punctuation that looks like letters. Here are two examples: Salad2E@t (salad to eat) or Dog8Hom3work (dog ate homework). Also, have different passwords for different sites. Usernames are bought and sold on the black

market, so if access to one of your sites is compromised, all of your logins are vulnerable if you use the same password.

However, there's a caveat: If you choose different "safe" passwords for all of your sites, and they're all super-complicated with lots of letters, symbols and numbers, chances are you'll never remember them. So maybe you write them on a sticky note or pad near your desk. Well, that's not very safe either.

The good news is there's a way to have multiple complex passwords without having to remember them: Use a password manager such as 1Password. 1Password is an application installed on your computer and mobile devices that stores all of your passwords. It will help you generate and store strong, unique, and secure passwords for each of your online accounts. And here's the real magic: Instead of having to dig through a vault when you need to recall a password, your manager will summon it for you automatically! Gone are the days of having to keep track of every single account and login. The only thing you are required to remember is the master password. That's it. Nothing else. One. Password.

Another huge benefit of 1Password is your ability to safeguard your entire firm. The business edition allows you to manage passwords for your team across all of their machines and devices. This gives you the ability to not disclose passwords to staff. A 1Password file is made available to employees, who are then able to log in to your critical systems. And if you have to fire someone, you don't have to tell everyone to change their passwords. You or an IT admin can do this from a centralized location.

Always Update Your Operating System

In early 2017, computers around the world were held hostage by a series of particularly aggressive ransomware attacks known as the WannaCry and Petya attacks.

What's very unfortunate about these attacks—where viruses exploited vulnerabilities in the Windows operating system—is that they were entirely preventable. Months before those attacks, Microsoft issued security fixes for those exact vulnerabilities. However, consumers needed to then apply their Windows security updates. Those who did had nothing to worry about. However, far too many people didn't update their systems.

When the WannaCry attack happened, Microsoft released a statement saying that the attack demonstrates the degree to which cybersecurity has become a shared responsibility between tech

companies and customers. The company said, “The fact that so many computers remained vulnerable two months after the release of a patch illustrates this aspect. As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems. Otherwise they’re literally fighting the problems of the present with tools from the past.”

In other words, we’re in this together. It’s up to Microsoft and Apple to harden their defenses, but they can’t help you if you don’t help yourself. It’s critical that you update your software anytime there’s a security update, regardless if you’re using Windows or a Mac. Keep in mind, if a software company comes out with an update, chances are they have discovered a vulnerability. So if you don’t update, you’re leaving yourself wide open.

How do you update your operating system?

If you’re on a Mac, go to “App store” under the Apple icon as often as you can and look for updates. Accept them. If you’re on a Windows machine, go to “Settings” and click on the Update and Security logo. You can also turn on automatic updates for both systems, which is ideal. However, if you’d rather control when the updates occur, do it manually at least once a week, but no less than once a month.

Bottom line: On your Mac, PC, iPad, iPhone, or Android, always perform the recommended updates and periodically check for new ones. Remember, your operating system is separate from your apps and software. Those need to be updated through the respective app stores.

Be Aware that Physical Security is a Greater Risk for Data Theft

Many people are surprised to find that cyberattacks are often physical in nature as opposed to electronic. In other words, it's not always some mysterious person hacking into your computer and stealing your data. Instead, it's more likely that someone will actually steal your actual computer or smartphone, such as a landlord, a disgruntled employee, janitorial staff, or a shady character on the bus or train ride home.

If you recall some of the largest cyber-thefts of our time, many of them were performed by insiders with access to systems. This was the case with the Edward Snowden leaks as well as the Sony Pictures attack in 2014.

Of course, if you're running a firm that stores confidential client information and other critical business details, you must first make sure that any and all computers and servers are locked away so others can't access them. The good news is that if you're using a cloud-based software such as Rocket Matter, you don't have to worry about locking down servers as they are not on your premises. However, if your servers are on-premise (or "on-prem", as it is frequently referred to by IT professionals), then physical security is especially paramount. Make sure your servers and any computers are in a room to which only a few people have the key.

Also, make sure that if someone does wind up getting access to your computer or your smartphone—which is a mini-computer that can contain all your sensitive data as well—that you're not giving them the keys to the kingdom. In other words, make sure that a third party who finds or steals these devices can't log in and access your information.

For instance, all computers (desktop and laptops) need to be locked or either put to sleep or shut down after a period of inactivity. You must also lock your cell phone with a password or touch id. Sensitive apps you use on phone such as Rocket Matter also need authentication after inactivity of more than a few minutes. Also, if you have cell phones with your work data on them, you might want to make sure that you can remotely wipe them if you need to do so. Apple has built-in tools that allow this.

Don’t Click Links in Emails

So called “phishing attacks” are when as perpetrator sends you an email that looks to be legitimate from an institution you trust such as your bank or insurance company. You click a link in the email, go to an imposter site that looks identical to the institution’s site, and hand over your username, password, and other authentication information to a bad actor. Those people now have all your login information to that site. (This might sound familiar because phishing attacks are what got John Podesta and Colin Powell in email trouble during the 2016 Presidential election.)

Another danger of phishing attacks: The link can take you to a site that infects your computer with malware.

So how do you prevent this? First, make it a rule to never click on links in emails unless you’re expecting the email. For instance, if your

friend texts you and says, “I’m emailing you the funniest cat video!” then by all means open the email.

If you are not expecting the email, however, then type the internet address directly into the address bar of the browser instead of clicking on it. So, if you receive an email from, say, Chase bank, don't click on the link. Do this instead: Type chase.com into your address bar yourself and log in from there. It’ll only take a few seconds, but it can protect you from hackers looking to steal all of your financial information (or worse.)

There are companies that will train you and your colleagues on how to look for phishing email attacks. For instance, Wombat Security will send your organization emails, and they'll see who's clicking on what, and then they'll give you a report on which employees are not being very careful. Such information can be invaluable—it’s better to nip bad habits in the bud and learn from a fake phishing attack before your firm is subject to a real one.

Consider Two-Factor Authentication

For another layer of protection, two-factor authentication is a great choice (in a couple of years it may be standard and not a choice at all). Here's how it works:

1. You log into a web application via your username and password.
2. You then type in a dynamically generated code that is sent to your smartphone (or a key fob).

With two-factor authentication, a malicious actor would need to have your username, password, and smartphone in order to access your account. It's a very strong extra lock on the door.

To understand this a little bit better, let's take a look at our favorite legal practice management software, Rocket Matter. Here's how it works:

If you want to use two-factor authentication in Rocket Matter, you need to download an app to your smartphone called Google Authenticator. Once you log in to Rocket Matter, a dynamic code is sent to the app. You enter that code into Rocket Matter, and then you're able to log in.

For more specific step-by-step instructions, take a look at our FAQ here.

If you're using WordPress, take a look at locking down your website and blog with an app and plugin called Duo. The last thing you need is for someone to deface your website. Duo is available across many applications and a wide variety of industries, with WordPress being one of the more common applications.

When Duo is configured on WordPress, you first log in to your site with a simple username and password. You then get a Duo notification on your cell phone. The service can call you, in which case you can pick up the phone and hit a number. It can alternately text you a code or even open the Duo app on your phone, in which case you have to click a green checkbox.

The tradeoff with two-factor authentication is convenience: It's a lot easier to log in to something without needing to answer a call or other second step. However, considering the world we live in, some extra precaution is extremely prudent and worth a little hassle.

Install Anti-Virus Software

Whether you're using Mac or PC, you should absolutely always have the latest antivirus software installed on your computer. It protects your computer from incoming threats by scanning for and removing any unwanted applications. These can include malware, viruses, Trojans, worms, spyware, ransomware, and other attacks.

Windows 10 comes with antivirus software called Windows Defender, and you can open the security center and run scans. When you first download antivirus software, it runs an initial scan on your system, and then it runs differential scans as time goes on. Ideally, do this at night so the scans don't interfere with your workday—the scans can significantly slow down your computer. Continue to make sure that you update your antivirus software and check that it continues to run scans.

Mac users also need antivirus software. A lot of people on Macs are lulled into this sense of complacency because so many of the attacks we hear about are happening on Windows machines. Apple does have a security feature called Gatekeeper that verifies downloaded apps before they run to prevent people from running malware on their systems. However, that's not enough: As more people use Macs, these computers increasingly become targets as well. You're putting your firm at great risk if you don't have anti-virus software in place.

Which antivirus software should you choose? There are a lot of options. For instance, there's Webroot which works on Macs and PCs and claims to protect customers from the Petya-based ransomware. Another option is Bitdefender, one of the leaders in this space. Of course, even if your computer comes with such software already installed—as Windows 10 does—you can install additional layers of security. It's not necessary, but it's definitely an option.

Use Encryption on the Web

Encryption works like this: Imagine you have a blender and you add in yogurt, bananas, and strawberries to make a smoothie. Now pretend there's a separate magic blender that can take the resulting pink slop and reconstitute it back into yogurt, bananas, and strawberries.

This is what encryption does. It is a complex mathematical trick that can turn your data into unrecognizable gobbledygook and then unscramble it later.

When you send data over the internet, you want it to be encrypted for security reasons. Sensitive data sent over the web should always be sent via HTTPS, indicated by a lock icon in the address bar of your browser.

With HTTPS, your data is scrambled inside the browser itself, passed down through the computer and then out over Wi-Fi networks. It eventually makes it to the server, where the data is unencrypted. When the server responds to your browser request, the round-trip undergoes the reverse process.

This means that if you're at Starbucks or the airport on a public Wi-Fi router, your data is safe from snooping. Your true risk there is a physical one: Someone looking over your shoulder at your screen.

Most responsible websites use HTTPS when sensitive data is being sent through a browser. Your bank does this, Amazon does this on payment pages, and Rocket Matter does this on every page of the application to protect client data.

Mobile apps on your phone are a bit trickier than using a browser because you don't know if your traffic is over HTTPS or not. There is not an address bar or lock symbol, but apps do use the web to communicate with servers. The problem is that the traffic is hidden. If you're concerned about whether or not the app you're using employs encryption to talk to its servers, it's your responsibility to get in touch with the software provider and understand if their mobile app communicates securely. (FYI, Rocket Matter does.)

For the extra-paranoid web browse user, you can also use HTTPS Everywhere, a browser extension from the Electronic Frontier Foundation that encrypts all communications with websites, making your browsing more secure. This extension works on Firefox, Chrome, and Opera.

Back up Your Data

You always need to think about business continuity and how you're going to access your files in case something terrible happens. And since attorneys are really in the worst-case-scenario business to begin with, there's no excuse for not anticipating disaster and coming up with a plan.

For instance, if your law firm is paperless and all of your documents are scanned onto hard drives in your office, what will you do if your office burns down? You missed an easy layup to continue operating uninterrupted. Well, the same is true if a ransomware attack destroys all the data on your computer by encrypting it forever. You can sidestep such a threat by performing regular backups on your data. If you do so, then even if you are victim of such an attack, you can quickly restore your work to the most recent version saved and move on with your life.

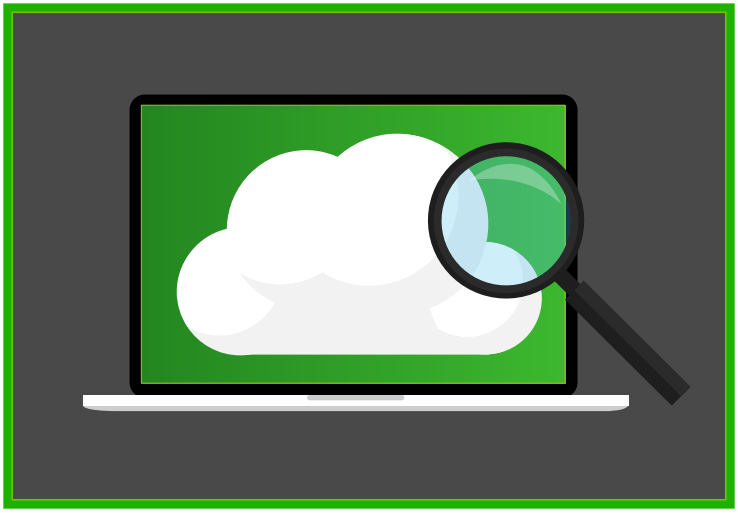
Here are three different approaches to backing up your data:

Use a dedicated cloud-based document management system.
These solutions abound in the marketplace. For instance, Dropbox, Box, OneDrive, Google Drive, ShareFile and many others compete in this space. Legal-specific ones include Worldox and NetDocuments, which are more sophisticated and include robust workflow and metadata support.

Save money by leveraging a cloud-based practice management program with built-in document storage.
Products such as Rocket Matter have document storage built in to their legal workflows. Typically, digital files stored in these applications can be shared with clients through portals. Additionally, you should be able to leverage document automation features (such as Rocket Matter's document assembly) that allow you to quickly produce your standard documents.

Employ a straight-up digital backup storage device.
Services like Mozy, Crashplan, or Carbonite can monitor your folder structures and continually back up your files. If you want to mostly work with files inside your computer network and are looking for a passive backup, this might be the easiest way to do things. Keep in mind, storage is very cheap these days. It may be the most commoditized aspect of computing. You shouldn't have to spend a lot of money for your business continuity plans.

Vet your Cloud Vendors



It used to be perceived as more secure to keep all of your data on-premise. But at this time, what sounds safer to a client: That you secure the data yourself in your office or that you're using cloud storage at an Amazon or Rackspace data facility? Unless you're skilled in cybersecurity or have specialized rooms and security systems in place, storing data on-premise is now perceived as less secure.

The problem is, not all cloud providers are created equal. Some, like Rocket Matter, have stood the test of time and have responsible security protocols. However, this is not the case with all vendors, and it is your responsibility to figure this out. State bars, in their ethics opinions on cloud computing, have issued "reasonable care" guidelines that instruct attorneys to learn about the security practices of their vendors.

In order to give guidance to law firms and bar associations in terms of best security practices for cloud vendors, Rocket Matter, along with other leaders in the legal technology space, formed the Legal Cloud Computing Association and issued a set of security guidelines to help you make decisions. There's a lot to know, but the biggest items you need to determine are the following:

- You should own your data. The cloud provider should not own it.
- You should be able to get your data out of a cloud system at any time in a usable format.
- Encryption should be used to safeguard client information.
- The cloud provider should be able to spell out their backup policies.
- You need to determine who at the cloud provider has access to see your data and under what circumstances. You must be comfortable with the answer.
- Find out if the company has had a breach before. If so, how did they respond to it?
- What measures does the cloud company take to ensure cybersecurity on an operational level? In other words, aside from the application you're spending money on, is the organization itself safe? Do they conduct background checks on employees? How do they manage passwords internally?
- Does the application limit attempts to log in to prevent brute force and dictionary attacks?
- Can you use two-factor authentication?
- How does the company handle data destruction? It is important when you leave a service that copies of your data are not lying around.

Many state bar associations publish their own list of due diligence questions for bar associations, but the points listed above are the major ones to consider.

About Rocket Matter

Rocket Matter helps law firms offer better client service and also increase revenues by more than 20%. The company was the first cloud-based legal practice management software on the market, landing its first client in 2007. It has been a leader ever since.

Rocket Matter has the most powerful, easy-to-use time and billing software in the industry. Also, when law firms want to make more money, go paperless, or increase confidence in their trust accounting, Rocket Matter helps them achieve those goals. With award-winning customer service based in the United States, it's no wonder thousands of law firms swear by Rocket Matter.