LEGAL workspace
Your Law Office in the Cloud

2 easy ways to TIGHTEN SECURITY

Learn how your firm can implement barriers to protect against online threats.

LEGAL workspace
Your Law Office in the Cloud

Two Easy Ways to Tighten Security

Law firms have an obligation to keep client data secure. As hacking becomes an ever-increasing threat to businesses of all sizes—especially those that store and transmit sensitive data—two options, Two-factor Authentication and Email Encryption, can help put up barriers.

Two-factor Authentication (2FA)

2FA simply verifies a user's identity a second time to make sure that the person making the request to enter a system is the actual user.

Often, it works in such a way that you enter your log-in credentials as usual, then the system sends a code to your cell phone that you enter to verify your identity a second time before you can access the system.

2FA is quickly becoming more prevalent in the business world. Some companies that currently use it include Google, Apple, Facebook, Twitter, Dropbox, Paypal, and Citibank. Many colleges and universities, including Penn State and the University of Chicago, are also adapting their systems to incorporate 2FA. Because these organizations understand that the data they house is precious to their users, they know that extra security is necessary to protect that data. It's only a matter of time before 2FA becomes the standard.

What advantages does 2FA offer?

It can be frustrating to come up with a unique password for every single account—and that means that many people duplicate passwords across accounts or use simple and easy-to-remember passwords and passphrases. That may make it more convenient for the user—but it makes hacking more convenient, as well.

Even a strong password might not be enough because hackers sometimes use tools that repeatedly guess passwords. Such a tool was used to hack Apple's iCloud in 2015 [link to: http://www.businessinsider.com/icloud-hack-idict-patched-by-apple-2015-1]; many high-profile users were affected. One way Apple responded was by improving 2FA.

Whether users employ weak log-in credentials, their information gets stolen, or they repeat passwords across accounts, 2FA adds an extra layer of protection that protects law firms' data.

How does 2FA work?

Legal Workspace offers 2FA as one of the many security options so its clients can experience greater peace of mind around data security. When a Legal Workspace user logs in, he or she can automatically receive a one-time code on his or her Smartphone app. Then the user enters the code in the Legal Workspace environment and gains access to their workspace. The whole process takes five seconds or less.

Most users find the process painless, but if any issues arise, Legal Workspace offers complimentary technical support for assistance.

Email Encryption

Email encryption protects content from being accessed and read by unauthorized parties. When an attorney sends a sensitive document to a client, he or she probably assumes that no one but the client will be able to see it. However, most email can easily be accessed by hackers determined to get the information, and the device where email is retrieved and stored—whether that's a laptop or a Smartphone—is also at risk.

What advantages does email encryption offer?

Attorneys know it's their duty to perform due diligence to protect client privilege. Sending unencrypted documents puts client data at risk—especially since email is one of the most vulnerable and targeted areas for anyone.

When a user opts to send encrypted email, the sent document is never stored on that user's email server or computer. That means that the information is safe in the event of a computer or email server hack. It also protects information in case laptops or other devices are stolen or lost.

How does email encryption work?

Legal Workspace uses a system that works as follows: An attorney who is sending something to a client types the word "encrypt" in the subject line. Instead of the email server sending the email to the other party directly, it instead sends a link that informs the client that he or she has been sent an

encrypted email. The client clicks the link, goes to the website, and can access or download the sensitive document from the website, bypassing the email system completely so the files are never stored on the recipient's email server.

2FA and Email Encryption considerably help law firms battle ever-increasing threats to security. It's no longer enough to cross your fingers and hope that hackers won't attack your firm. If you store and transmit sensitive information, you are at risk. These two offerings mitigate that risk by giving you extra layers of protection.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more at legal-workspace.com.