LEGAL workspace
Your Law Office in the Cloud

HOW TO

SECURE SENSITVE DATA

Learn more about today's cloud computing solutions for law firms.

LEGAL workspace
Your Law Office in the Cloud

Hackers Ignore Attorney-Client Privilege: How to Secure Sensitive Data

Attorneys go to great lengths to keep attorney-client privilege sacred. But some attorneys may inadvertently be opening their communications to threats. Hackers don't observe attorney-client privilege, and the highest value target is a law firm's email.

When hackers attack a law firm, they seek out email correspondence that might reveal strategy. For example, a large law firm handling a merger might be targeted by someone who wants insider information in order to buy or sell stock. On the other end of the spectrum, a smaller law firm might be handling a divorce--and the other party works in IT and has the skills to discover what the representing attorney has planned. That could be a reason to worry. Firms of every size should take steps to keep their high-value data safe.

Make sure your IT department or email provider has these email security measures in place. Do they:

1. *Log failed attempts?*

   Your network administrator should keep track of failed log-in attempts, and those logs should be regularly monitored and brought to your attention. That way, the administrator will discover if someone is guessing passwords and trying to break into your network.

2. *Enable account lock-out?*

   If hackers have the ability to guess passwords over and over again, the chances of them successfully logging into your network are much higher. Make sure they have enabled account lock-out after three to ten failed attempts to help stop hackers.

3. *Perform a quarterly external vulnerability scan?*

   Performing an external scan is a great way for your IT department to double-check that they have the latest patches, service packs, and other vulnerabilities covered.

4. *Have an attachment policy?*

Most malware and viruses come across as an email attachment, such as a .zip or .exe file. Blocking those and other high-risk file types can help protect against an attack.

5. *Have SSL certification and SPF records*?

   Without an SSL certification, your remote users make easy targets for even the most junior hackers. Also, make sure you added an SPF record when you purchased your domain name. If you neglected to do this, the next email your clients receive might not actually be from you.

Security best practices everyone in your law firm should follow:

1. *Use a complex password*

   Don't fall victim to a popular shortcut that can get you hacked: choosing something too simple--such as a word with no numerals or symbols--or too easy to find, such as your spouse's or pet's name. Complex passwords are strong passwords.

2. *Consider using two-factor or multi-factor authentication (MFA)*

   MFA provides an extra layer of protection by requiring that users confirm their identity through two or more channels. For example, you might enter your password, then receive a code via text message that you must enter in order to access the network. Especially if your law firm is high-risk--for example, if it works with health care providers or other clients who must follow HIPAA regulations--MFA is an important security measure to take.

3. *Unique network password*

   Almost everyone uses passwords for multiple purposes: over multiple platforms and for multiple apps and websites. It can be difficult to remember all of those passwords, so some people take shortcuts and use the same one over and over again. That's not a good idea.

If someone figures out your password for your personal email, for example, they can use that information to attack you in other areas of your life. Keep your work data safe by not using your network password for any other accounts.

Protect all of your privileged data, not just email

Hackers target email because of the high-value information it contains. But they don't stop there. Document exchange portals, your firm's servers, and cloud-based third party document and practice management systems could all pose risks.

Select your document-sharing portal carefully. In order to stay secure, do your research. Some of the most popular applications are the least secure. Dropbox is the **number one most banned application** according to one recent report. The reason? Poor security.

Make sure your law firm's file servers--whether they are local or in the cloud--are adequately protected. Important questions to ask vendors and your IT team include: Who really has access to the data? What controls do you have in place for security? Do you have an intrusion prevention/detection system? What type of firewall are you using?

Those same types of questions can also be asked of your cloud-based third-party document management or practice management system vendors.

Take several steps to better data security—or take one step

If you and your firm have the time and technical resources, you can do it yourself. You can make your email much more secure by taking the several steps outlined above. They also work as great talking points with both vendors and IT departments to ensure that your data is protected.

Or, you can take one step: Legal Workspace's environment is set up for security. Working with Legal Workspace eliminates the headaches associated with IT and security because they take the steps for you. Our trained and qualified employees constantly monitor and protect your data, and Legal Workspace uses the latest and greatest security features to halt potential breaches.

Protect your privileged data and keep hackers out. Whether you do it yourself or let an expert do it for you is up to you.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more or arrange a free demo at legal-workspace.com. Click here to watch our video.