LEGAL
workspace
Your Law Office in the Cloud

The true cost of
SPAM EMAIL

Learn more about how your firm can bolster security and reclaim 69 billable hours by implementing the right spam tools.

Reclaim 69 Billable Hours This Year

Everyone gets spam emails. It's a part of life, so you deal with it. But do you realize how much time your employees spend reviewing and deleting spam emails?

The average worker receives 121 emails per day, and nearly 50 percent of those emails are spam. It takes some time to differentiate spam from the real thing—about 16 seconds per email on average—which doesn't seem like a whole lot of time until you start doing the math:

If your employees are anything like the average worker, your employees and attorneys spend 16 minutes each day, 80 minutes each week, 5.5 hours each month, and 69.3 hours each year managing spam email. That's over one and a half 40-hour work weeks per year spent just dealing with spam.

Worrying about spam is a waste of time and money when your staff should be concentrating on more productive and strategic initiatives, such as workflow management, assisting clients and maximizing billable hours. Free or included spam tools, such as Microsoft 365's spam filtering, are not advanced enough to unburden your employees and protect your network.

Not just wasted time: Spam can be dangerous

Law firms store trade secrets, protected health information (PHI), and other high-value data which makes them valuable targets for cyber criminals. Some junk emails might be easily identifiable as spam, but others are more nefarious. For example, hackers have become increasingly clever when it comes to email spoofing and phishing. Both email spoofing and phishing look very much like the real thing and attempt to fool recipients into either giving away their information or downloading hazardous software.

Ransomware can be another issue for law firms if employees and attorneys aren't properly trained to recognize malicious emails. An employee might receive an email with a seemingly benign attachment and open it—only to unleash a Cryptolocker virus in your network. The virus systematically enters and locks files on the infected computer (including network files), and the user can only regain access by sending money to the hacker, who may or may not release the information. Spam has the potential to directly compromise attorney-client privilege.

Get those hours back

Implementing the right spam solution is imperative to reclaiming billable hours and securing your law firm's network. Technology is now available with advanced features such as opening attachments in a "sand box" to check for malware before sending the attachments to the end user's inbox.

The time, effort, and expense it takes to set up a system for reducing junk email offsets the time, effort, and expense individuals sink into managing it on their own—and you'll spend a lot more time, effort, and expense if a user in your firm finds itself the victim of a malicious cyber-attack.

Legal Workspace regularly implements spam solutions and provides end-user training to improve law firm efficiency and protect firms from email threats. We are serious about protecting data in a world where hackers and spam purveyors continually invent new ways to penetrate defenses. Get serious about stopping spam, and reclaim those hours back.

Reach out to Legal Workspace to learn more about spam filtering options.

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