

Five Ways Law Firms Can Immediately Improve Their E-mail Security

By Hal Licino

August 2010

Given the severe consequences that can result from an online security breach, all law offices need to address these steps to better protect their systems.

The average cost to organizations for a security breach continue to rise, according to statistics from the Ponemon Institute, with serious financial consequences resulting for the organization <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf>. With these overwhelming costs and the obligation for law firms to maintain attorney-client confidentiality, it is staggering is that the 2009 *ABA Legal Technology Survey* of law firms found that:

- 14 percent did not use spam filters
- 25 percent did not use anti-spyware software
- 29 percent did not use firewalls
- 37 percent did not use antivirus software
- 45 percent did not use mandatory passwords

Given these statistics it is not so surprising that 54 percent of all law firms reported that a virus, spyware or malware had infected their systems. Here are recommended steps to protect your firm.

1. Vaccinate Systems Against Viruses

Viruses, spyware and malware hidden in e-mail attachments are particularly troublesome for a law firm because they can contain keyloggers that transmit confidential information to third parties. The latest releases of antivirus utilities, fortunately, consume far less CPU resources than earlier versions, which slowed down even fast systems. You need to run antivirus, malware utilities and firewalls continuously in maximum security mode, and firm e-mail policies must meticulously outline the prerequisites for launching e-mail attachments.

2. Don't Disclaim: Encrypt

The majority of law firms rely on confidentiality disclaimers on their e-mails. In most cases a disclaimer is definitely better than nothing, but it can create a minefield for a firm in the case of a disciplinary proceeding or a malpractice suit, for several reasons:

1. A disclaimer essentially verifies that the sender was aware that the e-mail message was unsecured and determined to send it anyway.
2. The disclaimer is placed at the end of the e-mail; therefore the content of the message has already been read by the time the recipient arrives to the disclaimer.

3. Any prospective client of the law firm might read the disclaimer and understand it to mean that the confidentiality of the attorney-client relationship has already taken effect.

By far a better alternative is full encryption of all client-related e-mails. Not only is it a much more secure means of communication, but when a client becomes aware that the firm is offering encrypted its information, it broadcasts that the firm is taking the appropriate precautions to protect all communications.

Be aware, however, that encryption can also have a downside in that it can be fairly expensive for solo and small firms, your clients generally have to have the identical software resident on their PCs to decode the message and, if the firm does business internationally, encryption is illegal in some countries.

3. Scrub That Metadata

Metadata is the embedded data in virtually every computer file that includes information such as the author, creation date, changes made by whom, and comments in the content. While metadata is usually largely irrelevant, in some cases it can contain confidential, sensitive or privileged information, and thus can present a considerable problem for adherence to confidentiality restrictions.

The American Bar Association's Standing Committee on Ethics and Professional Responsibility has concluded that law firms should eliminate metadata when they are "concerned about the possibility of sending, producing or providing to opposing counsel a document that contains or might contain metadata" under the general duties of client confidentiality.

Remarkably, many smaller law firms do not even possess metadata removal software. It needs to be part of every law office's e-mail security arsenal.

4. Beware of Phishers

The FBI regularly warns of various sophisticated phishing attempts aimed at attorneys and intended to defraud the recipient. Although there are various software solutions that claim they can stop phishing attacks, the best precaution is to be extremely careful whenever clicking on any link received in an e-mail.

Phishers have become very adept at fooling recipients by addressing them by name and seeming to have a great deal of what should be confidential information on them, but what phishers can't fake is the URL domain name of the company that is being "spoofed." If an e-mail link must be clicked on, hover on it first and view the URL that is displayed in your e-mail client. If it does not match the company it's supposed to be from, delete the e-mail immediately.

5. Leave Spam in the Can

Law Practice TODAY

THE MONTHLY WEBZINE OF THE ABA LAW PRACTICE MANAGEMENT SECTION

Many law firms have chosen to route their e-mail through an enterprise application that filters spam on a dedicated company's remote servers. Any e-mails deemed not to be spam are then directed to the lawyers' inboxes.

The best way to avoid spam, however, is to avoid becoming a spam target. If the law firm has its e-mail address properly masked on its Web site, and the attorneys do not register at questionable sites, post on a wide range of forums or ever reply to spam-mail, the amount of spam will be held to a minimum.

By implementing a strong set of e-mail policies, including those outlined here, law firms can help minimize the huge risks caused by porous e-mail security.

About the Author

Hal Licino is the author of two books and an e-mail marketing advocate for Benchmark Email www.benchmarkemail.com, an e-mail marketing service.
