NJSBA PRACTICEHQ Affinity CONSULTING

EMAIL ENCRYPTION AND SECURE CLIENT

By: Barron K. Henley and Jeffrey R. Schoenberger

WHAT THE EXPERTS SAY

Here are a couple of quotes to consider:

> "A secure email account that the attorney is assured protects the content of correspondence. No attorney should use Gmail or other free services that in fact admit that they use personal information from email content. They should encrypt their client correspondence. Before sending sensitive correspondence, they should check by phone or text with the client to see what method of delivery is preferred."[1]

> "The level of encryption may vary based on practice areas or, more importantly, the firms' clients. At a minimum, emails and attachments that contain confidential data should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."[2]

> "It's all about encryption of the 3 main risk areas for data held: data in transit, at rest and in backups. It doesn't matter if it's email, Instant Messages, case files, discovery or 3rd party expert communications, the principle of encryption is the ONLY way you can really satisfy due diligence requirements."[3]

ENCRYPTING DATA ON THE INTERNET

BACKGROUND

We all know how convenient email is. With smartphones and tablets, we can read and respond from anywhere at a time of our choosing. Email is also one of the oldest internet technologies, predating HTML (*i.e.*, web browsing), by 28 years; 1971 vs 1989 for you history buffs. Old technologies are not ipso facto bad. Generally speaking, they are robust and adaptable; that's how they survive. But old technologies, particularly computer technologies, were developed "among friends." Neither Ray Tomlinson (who sent the first email) nor Tim Berners-Lee (the father of the world wide web) thought much about internet security. In both decades, the internet was the province of governments, academics, and other trusted individuals and institutions.

In the intervening 25 years, security has taken an infinitely more prominent role in networked computing. There's very little human interaction or business service that isn't replicated to some degree on the internet. The core technologies of HTML and email have adapted to meet those needs. With HTML, security came in the form of SSL and then TLS, the technology represented in your browser's address with a padlock when you access your bank or other private site. Indeed programmers wrote a browser plugin, HTTPS Everywhere, to ensure you always get a website's secure version, if one exists. Email underwent similar, but less dramatic and less consistent, changes.

---

[1] Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data, by Nate Lord, DigitalGuardian, October 13, 2015, quoting Robert Ellis Smith. See https://digitalguardian.com/blog/law-firm-data-security-experts-how-protect-legal-clients-confidential-data.

[2] Ibid., quoting Marco Maggio.

[3] Ibid., quoting Steve Santorelli.

EMAIL ENCRYPTION SERVICES

While the transition to a more secure internet for websites is well underway and nearly invisible to end users who "just want to get things done," the same is not true for secure email. A substantial roadblock to an easy, seamless transition lies in the fact that no entity controls both ends of an email exchange. In the case of secure web browsing, one can guarantee that a site visitor is using one of four or so potential browsers (Apple's Safari, Google's Chrome, Microsoft's Edge, and Mozilla's Firefox). Across all platforms (desktop, mobile, and tablet) those four account for 95% of browser usage. The shares vary based on platform and region (*i.e.*, continent or country). But in no case does a browser move from a rounding error to a front runner. Run your own tests here. If those four browsers adopt a security protocol, you can implement it on your website confident that 95% of visitors will use it without a problem.

In the case of email, there's no such unity. Email runs on three potential protocols: IMAP (Internet Message Access Protocol, an open standard), Google's Gmail (which is IMAP-like with a bunch of Google customizations), and Microsoft's Exchange. They each of advantages and disadvantages but they all talk to each other. When I exchange emails with someone, I don't know what their backend email protocol is. Furthermore, I could access email through a myriad of devices, programs, and even web browsers. My company uses Microsoft 365, which includes Exchange. I use a MacBook laptop. I could access my email via Apple's Mail desktop mail program, its iPad or iPhone companions, Outlook for Mac, or any web browser that runs on a Mac. Add in Windows and the number of potential endpoints more than doubles. Including Android devices (smartphones and tablets) increases the number further. That doesn't even include third-party email clients on the desktop or mobile. Unlike web browsers and websites, it's not a matter of getting four companies to agree. That leaves email communication at the lowest common denominator, in plain text and unsecured.

This security gap has led companies to develop their own utilities or add-ins that ride on top of existing email protocols. These tools, which usually come with subscription fees, encrypt the email message and attachments before it leaves your device. The message recipient receives an email, but not the email you sent. What the recipient gets is an email with a link (usually HTTPS-secured) that sends them to a website to read your message, download attachments, and reply to the message.

The options listed below are inexpensive and easy. They encrypt both the emails and any attachments to the email. In most cases, a password must be entered by the recipient to open the email and any attachments.

A. ECHOWORX ENCRYPTED MAIL: https://www.echoworx.com/email-encryption-platform/

B. HIGHTAIL: https://www.hightail.com/ - this service was formerly known as YouSendIt.com. It's designed for sending enormous attachments, but also offers encryption for those attachments. Incredibly easy to use and inexpensive. It does not encrypt the text of an email, only the attachments.

C. HUSHMAIL: https://www.hushmail.com/plans/legal/

D. IDENTILLECT: https://identillect.com/ - many bar associations offer discounts on this service.

E. MICROSOFT 365 E3 & ABOVE: https://www.microsoft.com/en-us/microsoft-365/enterprise/e3 - Despite the name, you do not have to be a large organization to subscribe to E3 ($36/user/month). It's more expensive, but includes several niceties beyond the "standard business" plans and, for an additional cost of $12/user/month, you can add Microsoft's Purview Message Encryption (part of the Microsoft 365 E5 Compliance add-on), which allows email encryption from within Outlook without any extra plugin. It's also one of the easiest for message recipients to use too. As of this writing, combining Microsoft's E3 plan with the E5 Compliance add-on costs more ($58/user/month) than simply subscribing to Microsoft's E5 plan ($57/user/month), which includes the E5 Compliance features within it.

F. RMAIL: http://www.rmail.com/ - registered email service which can prove delivery + encrypted email

G. SENDITCERTIFIED: http://www.senditcertified.com/ and note that they offer discounts through several bar associations.

H. SHAREFILE: https://www.sharefile.com/

ENCRYPT EMAIL ATTACHMENTS

Word, WordPerfect and every good PDF program including Acrobat offers file encryption. This functionality is built-in so you only have to learn how to use it. With file encryption, the file simply cannot be opened without a password. You email the encrypted attachment while the body of your unencrypted simply says "Please see attached." That attached file containing the sensitive information would be encrypted on its own. The recipient needs a password to open the encrypted attachment. But remember, do not include that password in the email. Text or call the recipient with the password. Alternatively, the password could be something you and the client decide in advance, perhaps noting it in the engagement agreement.