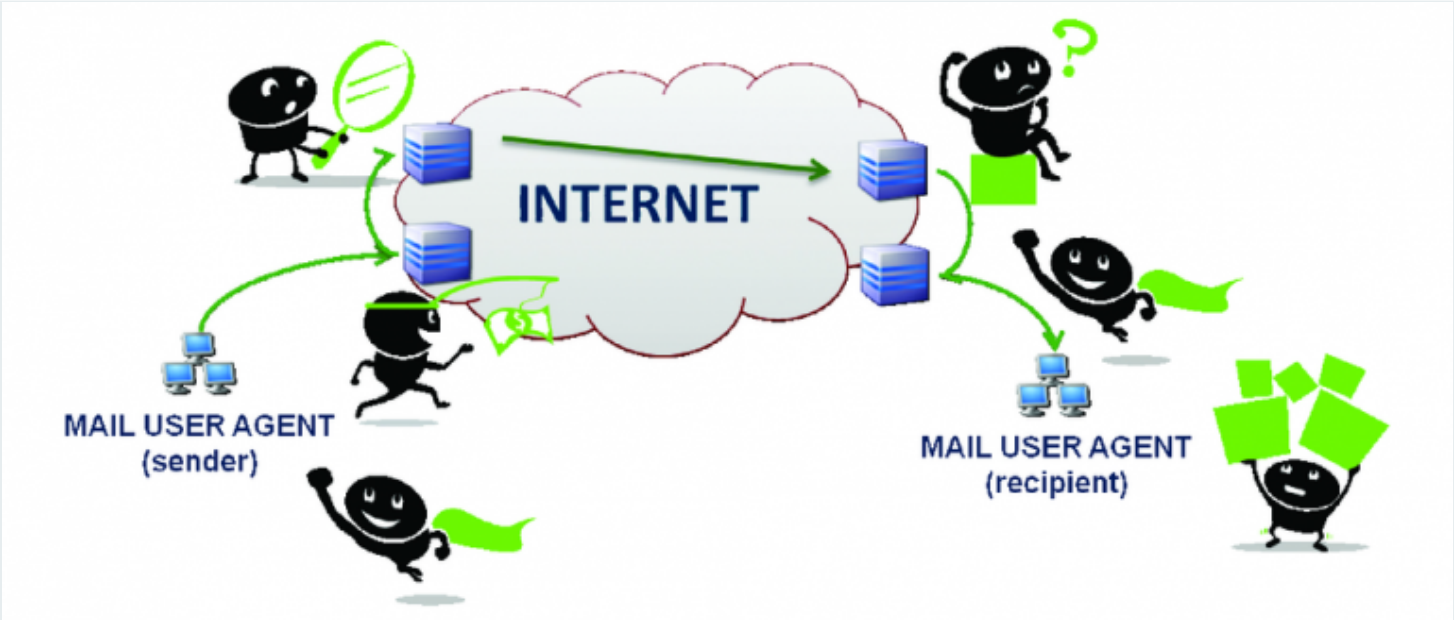
TECHNOLOGY

The Insecurities of Email

Eric Pulaski • Sep. 05, 2014



Email has been around a long time and has evolved into a mission-critical resource to deliver documents and communicate with clients. It's the default for most businesses — convenient, easy and mature — and has all but replaced time-consuming faxing and manual delivery of documents. However, while email has been a trusted delivery tool for year, you should ask yourself, "Is it safe?"

Security v. Privacy

Security and *Privacy* have significant importance in the accounting profession. Unlike the recent trending topics, such as *paperless* and *workflow*, the measure in which firms assure data security and privacy has been a focus for accountants for decades. And

now with new state and federal mandates hitting the profession at warp speed, ensuring the security of data and the privacy of client information has a renewed significance and has elevated to Job 1.

First, it's important to understand the difference between security and privacy if firms are to comply with mandates geared toward client data protection. Consider each separately:

Security is comprised of three primary elements: authentication, authorization and audit.

Authentication refers to the ability to authenticate the person signing on. In other words, making sure an individual is who she says she is, typically via a unique user name and password.

Authorization determines a user's access to various resources, based on the user's identity. This has to do with setting permissions — what an individual can and cannot access. In a document management system, a user would be granted 'rights' to access certain documents.

Audit refers to the mechanism for tracking access and activity of a system or service — in short, who did what and when. In a document management system, an audit log would allow you to generate security and compliance reports of which users uploaded, accessed or changed the properties of a document, and when.

Privacy is really a subset of Authorization. It centers on ensuring that an individual's privacy is protected during the course of sharing data with others, whether that data is shared online or stored in file cabinets in the office (who has access to those files?). When we are talking about sharing and collaborating over the Internet, it's easiest to think of security as the padlock — no one gets in without the right combination. Privacy is the shield that protects a person's identity while actively sharing information via the Web.

Second, it's critical that firms understand why they should care about security and privacy.

The Internet is the foundation of communication in most businesses, including accounting firms. Accountants send hundreds of emails every week. Without worry, financial statements, tax returns, and other common reports and forms are attached and sent. A few may send email links to documents, which are secure, but don't require the user to have an email and password to access the document. And without user authentication, there is no way to verify that the person accessing the document is the intended recipient.

Some firms have advanced to using encryption as a means to protect documents, which can add a lot of complexity to managing hundreds of passwords for the documents encrypted. You also have to think about how you are getting the password to the recipient. If you are emailing it, that could be a security risk. And if the password is lost or expires, the document is effectively "dead" and unable to be opened by the sender or the recipient. The result is that you end up duplicating your efforts in order to recreate and send the information again.

The bottom line: Most firms are riding on the hope that email is safe.

But what if it's not? It only takes one time, one breach of a client's data, and your firm's reputation is at stake. In fact, consider all that you are risking — your clients' business privacy, your firm's privacy, and civil and criminal penalties. Also consider that as the topic of data privacy continues to garner attention, clients may look to you as an expert, seeking education on how they can protect themselves against potential data breach. These are all good reasons to care and give security and privacy their due attention.

The Journey of the Standard Email

Now for the big question: Is email safe for sending sensitive documents? The truth is that if most people were aware of the multiple stops an email makes en route to its final destination, they might think twice about sending private information.

Email doesn't simply move from your inbox to the recipient's. It is transported across multiple servers, and at each stop point 'sits' unprotected. IT experts refer to this as "data in the clear." While in the clear, emails are open game and at the mercy of the server administrator, who can alter or even delete a message. Below is a simplified illustration of the typical email journey.

Email will most certainly continue to be a primary delivery tools for firms. But as new data privacy mandates continue to emerge, firm leaders may want to look at alternatives for delivering sensitive financial data.

A Resolution to Email Insecurities — the Cloud (Portals)

A better solution for exchanging documents that contain private client data is through secure portals. Other industries, such as banking and healthcare, have converted to portals as a primary delivery tool. And clients within these niche markets have come to expect this level of service. Think about it. Would you even consider using a bank that didn't offer online banking?

No one is saying email should be abandoned completely. Email will continue to be a firm's primary communication source. It's only when sensitive information like tax returns, social security numbers or financial statements are attached within an email that firms should consider a better alternative like portals. The best portal solution also offers the ability to use email as the core communication tool. However, via portals, sending a link to a document is secure because the document is stored online, not attached in the email.

Exchanging and delivering documents using portals eliminates the need to send complete documents as attachments in emails. It also alleviates several other pain points associated with emailing client information, such as encrypting files and creating, managing and communicating hundreds of passwords. Portals allow firms to store sensitive documents within a secure, personalized online space. Firms can then simply provide a link to a secure location where clients can log in and access current versions of their financial documents at any time and from anywhere with an Internet connection.

Email + Portals = Easy + Safe

A key reason why portals are fast becoming a popular document delivery tool is their ease of use for clients. The newest document portals offer the best of both worlds: You can use your own email system to send emails to your clients, but send them a link to a document in a secure portal, rather than attach the document itself to the email. This can be as easy as sending a friend a link to an interesting article on the Web, but it is secure, auditable and compliant. Clients really don't even need to understand what a portal is. To access the document, they simply click on a link in the email.

Portals are also exceptionally secure, offering advanced, built-in security features. They require recipients to log in using a unique user ID and password to access documents. This ensures authentication and authorization in one fell swoop. Most portals also automatically provide an audit trail that enables administrators to view and set user permissions and track usage, and support automatic back up of data. Even better, portals teach your clients a safer way to communicate, as well — no more sending your firm sensitive information, like SSNs, via email. Everything can be exchanged in the portal. It's a win-win.

For sensitive documents, it's important that you do this with a secure portal, which requires your clients have a username and password. While some portals let you share documents using "anonymous" links, whereby users are not required to have a username/password, those links are not secure and are vulnerable to discovery over

the Internet. That's why such products put these documents in a temporary folder that is deleted after a short period of time, usually 30 days or less. You can password protect these documents for safety, but communicating the password over email is not safe, and access to these documents is not auditable.

Keeping Up

Firms have a lot to keep up with these days, and privacy and security of client data should be at the forefront. The good news is that technology can make securing clients' data easy. Portals provide a secure platform for exchanging sensitive information and files, alleviating firms of having to deal with time-consuming document encryption, password creation and general management of a complex delivery process.

Sending links to documents via email offers clients a familiar communication channel, while leveraging secure portal technology. Portal technology is defined by built-in security and offers one of the safest and most intuitive platforms for exchanging data and documents with clients. Why take the risk of breaching client privacy by sending documents via email when portals offer a solution with all the security and privacy functionality built in? The insecurities of email are complex. However, with advancements in cloud technologies like portals, the answer to this very real and very difficult issue has gotten much simpler.

You might also be interested in "6 Steps to an Effective Client Portal Strategy" at www.CPAPracticeAdvisor.com/10248304.

About the Author – Eric Pulaski, CEO and Founder of SmartVault Corporation

With over 20 years of experience in network security systems and a focus on cloud computing, Eric founded SmartVault Corporation in November of 2007, and currently serves as the company's Chief Executive Officer. Eric has made it his mission to deliver a simple, low-cost document management solution that uses cloud-based technology (low cost) but is centered around integration with applications customers already use, such as QuickBooks® (simple). Eric can be contacted at eric@smartvault.com.

Technology

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.