users to transmit data to a remote user, regardless of the computing platform or internet connection method used by the recipient. There are many ways that data ...

Brian Tankersley • Sep. 10, 2022

Note: This is part two of a series of articles on basic tools used to encrypt confidential data to protect it from unauthorized access. Last month's column discussed practical methods to encrypt data "at rest", this month's column details some ways to protect yourself when accessing data remotely by encrypting data while it is "in transit" with secure portals and encrypted messages.

Protecting data in transit is harder than encrypting data at rest, since it must allow

office. An unprotected message or an unencrypted data transfer on the internet is like a postcard sent through the post office in that it may be read by anyone who handles it along its journey, and senders and recipients have no expectation of privacy when using these insecure methods. We use three different techniques to protect messages in transit – encrypted portals, e-mail encryption, and file-level encryption, and a brief summary of each approach follows.

Encrypted Portals

Also called "client portals" in our industry, these are websites which are designed to allow you and your clients to securely exchange data through these password-protected portals, which use Transport Layer Security (TLS) to secure data while it is transmitted between a computer or device and the portal. There are literally hundreds of tools which can be used as a secure portal, including offerings from Sharefile, XCM, Doc-It, CCH, Thomson Reuters, TaxCaddy, Box, Microsoft, and others.

E-Mail Encryption

Sending normal e-mail outside of your organization is like sending the message and any attachments in a postcard – they can be intercepted, retrieved, modified, and forwarded to others with impunity. While e-mail servers use TLS security when transmitting messages to each other, the servers (and their administrators) have access to the unencrypted data, and can do with it as they like. There have been a number of attempts at applying encryption to individual e-mail messages – SMIME, PGPMail, GPGmail, and others. While all of these methods work, all have proven to be too difficult for the average end user, and are rarely used in practice.

There are a wide range of services which use a combination of technologies to protect e-mail and attachments in transit. Some of the more popular approaches

include the following:

365 Message Encryption, and additional solutions are available which work with e-mail hosting from Google, Zoho, and others.

- **Webmail-Based Solutions** – Some solutions use a combination of webmail, PGPmail, and portals to secure data transmission to others like Switzerland's ProtonMail and Canada's HushMail. Unfortunately, these solutions can't be used to store or transmit client tax data since their servers are not based in the United States.
- **File level encryption** – A final approach used by some is file level encryption using tools like AESCrypt, 7-Zip, or the password protection built into Microsoft Office and Adobe Acrobat and then attach the file to an unencrypted e-mail. While this is not a good solution for many reasons which I won't address here, I've seen some users take this approach, which could subject you to liability under relevant data protection laws and regulations.
-

Regardless of which approach you and your firm take to securing messages and file transfers, it's crucial that you consult your cyber insurance and malpractice vendors to learn what methods are accepted/recognized by your policies. You should also review your strategy with your attorney, and train your staff and clients on how to transmit files to and from your firm with directions, videos, and admin staff who can walk clients through the process. No file transmission method is perfect, and once you've implemented a solution, your admins may want to enable Data Loss Prevention settings to prevent users from sending e-mail attachments without using the appropriate methods.

We will continue our discussion of encryption next month when we will cover securing Wi-Fi and accessing data over a virtual private network (VPN).

Brian F. Tankersley, CPA.CITP, CGMA (@BFTCPA, CPATechBlog.com) advises firms

CPA Practice Advisor 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.