PLF *in*BRIEF

ISSUE 138 | SEPTEMBER 2019

*Malpractice Prevention Education for Oregon Lawyers*

LAW PRACTICE

# Protect Your Data by Using Encryption

***By Hong Dao***

This article is a continuance of our cybersecurity series. It focuses on encryption as a way to protect your data from physical loss or cyberattacks.

Encryption is a critical step in adopting and implementing a security policy in any law office. It transforms information so it is unintelligible to an unintended recipient. It uses specific algorithms to scramble the data into jumbled unreadable codes. The recipient needs to unscramble the data using an encryption key in order to decrypt the information.

You do not need to know how encryption technically works to use it. Your "usage" of encryption typically involves turning on the native encryption program built into your computing devices. Or it may involve downloading and following instructions to install and set up a third-party encryption software program. You may need technical assistance with implementing both types of usage.

Encryption protects two types of data: in transit and at rest. Data in transit refers to data moving between browsers, via emails, and through the cloud. Data at rest is data stored on computer hard drives, servers, databases, and mobile devices. Lawyers deal with both types of data. This article will focus on hard drive, file/folder, smart device, cloud, and email encryption.

## FULL DISK ENCRYPTION – ENCRYPTING COMPUTER HARD DRIVE

Your computer contains client information as well as your personal information that you want to protect from unauthorized access. If the computer is lost, stolen, or hacked, there is a high risk that the data will be compromised if it's not secure. Encrypting the entire hard drive on your computer (called full disk encryption) ensures that no one can access anything on it. The encryption makes all data on your computer unreadable unless it is decrypted with a key (password) that only you have.

Computers running on Microsoft Windows have a free built-in full disk encryption program called BitLocker Drive Encryption. They also have Bitlocker to Go that can be used to encrypt external drives like USB flash drives and other portable hard drives. However, both Bitlocker programs are only available in the Professional or Enterprise editions of Windows 8 or 10, or the Ultimate version of Windows 7. (Beginning January 14, 2020, Microsoft will no longer support Windows 7. Computers running on unsupported operating systems are more vulnerable to malware and other types of attacks.)

Instructions to turn on BitLocker are available on the Microsoft website here: *https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption*. Once BitLocker is enabled with a strong password or passphrase, the contents of the hard drive are automatically encrypted when the authorized user logs off and are decrypted when the user logs on.

Most of us buy PCs with the Home edition of Windows, which does not have BitLocker encryption. Check to see which version you have. If you need help with this, go to the Microsoft website here: *https://support.microsoft.com/en-us/help/13443/windows-which-version-am-i-running*.

For those using the Home edition, consider using a third-party encryption software program like VeraCrypt, DiskCryptor, or BestCrypt to encrypt your hard drive. Common computer security vendors like Symantec and McAfee also have their own lines of encryption software.

Mac computers with OS X Lion or later have a full disk encryption program called FileVault 2 available in the System Preferences. Instructions to turn on FileVault 2 are available here: *https://support.apple.com/en-us/HT204837*.

## LIMITED ENCRYPTION—ENCRYPTING FILES/FOLDERS

Encryption can also be performed on a limited basis — at the individual file or folder level on your computer. Limited encryption provides another layer of security on your encrypted hard drive. It addresses a concern with the full disk encryption: the hard drive is not always encrypted. When a user turns on the computer and enters the decryption key (password), the entire drive is decrypted. It remains decrypted until it is turned off or logged off again. During the time the computer is turned on and in its decrypted state, your data is vulnerable if left unattended. Limited encryption helps make those files inaccessible during that period.

For those looking for extra security by encrypting selected files and folders, you have a few options.

- Windows Users
  Windows has an encryption method called "encrypting file system" (EFS) that allows users to encrypt files or folders. EFS is only available on Professional and Enterprise editions of Windows. More information on how to use this feature is available here: *https://www.thewindowsclub.com/encrypt-files-efs-encryption-windows-10*.

- Mac Users
  Mac OS Disk Utility tool can encrypt files and folders. More information on how to use this function is available here: *https://tinyurl.com/y7wshet4*.

- Encrypt Office documents and Adobe PDFs
  If your computer doesn't have any built-in file/folder encryption program, you may consider putting a password on the document as a way to encrypt it. Microsoft has instructions on encrypting Office documents here: *https://tinyurl.com/yyf64c29*. Instructions for encrypting Adobe PDF documents are available here: *https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html*.

- Paid programs
  Paid file/folder encryption software programs offer the capability to encrypt only parts of a file or the entire file or folder. A list of paid file/folder encryption software is available here at PC Magazine: *https://www.pcmag.com/article/347066/the-best-encryption-software*.

If you have to choose between full disk or limited encryption, go with full disk encryption. With full disk encryption, you don't have to think about what files to encrypt. Everything is encrypted automatically. Make sure you set your computer or laptop to log off automatically after a period of inactivity so unencrypted data is not exposed.

## DEVICE ENCRYPTION – ENCRYPTING SMARTPHONES AND TABLETS

All smartphones and tablets, which are essentially small computers, should also be protected with encryption, as they can be easily lost or stolen.

Newer versions of Android devices have encryption enabled by default. Other versions require the user to set up a password or PIN to enable the encryption program. More information on how to do this can be found here: *https://www.androidauthority.com/how-to-encrypt-android-device-326700/*.

All iPhones and iPads have encryption built into their operating systems, but they need to be enabled by setting up a lockscreen password: *https://support.apple.com/en-us/HT204060*. Once you set a password, all files are automatically encrypted when the device is locked and decrypted when it's unlocked.

## CLOUD ENCRYPTION—ENCRYPTING BEFORE UPLOADING TO THE CLOUD

Some lawyers also store files and other types of

data on the cloud through providers like Dropbox, OneDrive, and Google Drive. Although your data is encrypted by the provider against hackers, it is not encrypted against the provider itself. This means that the provider has the ability to access your files or give backdoor access to the government in response to a subpoena or warrant.

Programs like Boxcryptor, ODrive, and Cryptomator allow users to encrypt their files first before uploading them to the cloud. This makes the data unreadable by the provider because it doesn't have the encryption key. Those programs create an encrypted drive on your computer. When you transfer files to the encrypted drive, those files will be automatically encrypted and then uploaded to your cloud provider through file synchronization.

If you're looking for a more secure alternative to Dropbox or other common cloud storage providers, consider these "zero-knowledge" providers: SpiderOak, Tresorit, Sync.com, pCloud, or MEGA. All your files are encrypted on your computer first before they are transferred to the provider's servers. You keep the encryption key and a copy is not shared with the provider, so it has "zero knowledge" of your key. Without knowledge of your key, the provider cannot access your data stored on its server.

## EMAIL ENCRYPTION – ENCRYPTING BEFORE SENDING EMAILS

Emails are by default not encrypted. If you're sending confidential or sensitive client information, you may want to take steps to secure the message and its attachments. Below are a few options to secure emails.

- For Gmail and Outlook users
  Gmail Confidential Mode does not use encryption but still provides a little bit of security for your emails. It lets you put an expiration date on a message and lock it with a password sent to the recipient's phone via SMS messaging (text). Emails sent with Confidential Mode cannot be forwarded, copied, downloaded, or printed, but recipients can still take screenshots. Those emails are automatically deleted from the recipient's inbox after the expiration period but remain in the sender's Sent folder. To learn how to use Confidential Mode: *https://support.google.com/mail/answer/7674059?hl=en&co=GENIE.Platform=Desktop*.

Outlook users can encrypt Outlook emails using Digital ID. The process to create a Digital ID can be cumbersome, but once it's created, you can use it to encrypt your email message or prevent it from being tampered with. More information is available here: *https://support.office.com/en-us/article/get-a-digital-id-0eaa0ab9-b8a2-4a7e-828b-9bded6370b7b*.

- Email encryption software
  Third-party email encryption services like Trustifi, Citrix ShareFile, TitanFile, Zix, and Virtru can be purchased and downloaded as an add-on to most existing email programs. It's fairly easy to encrypt an email and attachments using any of these programs. Users just click on the encryption icon whenever they want to encrypt a message. How the recipient receives and opens the encrypted email will depend on the program.

- Encrypted webmail
  An encrypted email service is an easy way to secure your emails without having to download and set up anything. Web-based email services like Hushmail, Protonmail, and StartMail let you send encrypted emails to anyone. They have the added benefit of providing anonymity because the provider cannot read the messages in your inbox. These services can be used on any computer browser or iOS and Android devices.

## PASSWORD IS IMPORTANT

Most encryption programs are tied to the password or passphrase you choose. Make sure it's strong, complicated, yet still easy to remember. Our *inPractice* blog has tips on how to create strong passwords available here: *https://www.osbplf.org/inpractice/passphrases--an-enhanced-level-of-security/*. Make sure you keep your password in a secure location, as a forgotten password means complete loss of your data.

*Hong Dao is an attorney and practice management advisor at the PLF.*