What is Encryption?

Encryption is the process of converting data into a code. To read encrypted data, the receiver must have a key to "unlock," or convert, the data into a readable form. Without the key, the data is unreadable. Encryption doesn’t lessen the frequency or likelihood of a cyberattack, but it can help minimize the impact of a successful attack by preventing the hacker from reading the information they have accessed. For example, many sites encrypt information such as your credit card number, name, and address when it is transmitted during the course of purchasing products and services online.

Data can be encrypted when it is in transit, such as a document attached to an email, or when it is at rest, stored on a network drive.

Encryption can also be applied at the device level. For example, by encrypting a laptop’s hard drive, all the data contained on the machine is encrypted and protected from inadvertent disclosure, even from some forensic tools. If disk-level encryption is applied to a laptop, a password will be required before the boot process begins. Entering the disk password is the equivalent of using a key that decodes the information on the drive.

Confidentiality Statements and Disclaimers

Many firms include confidentiality statements and disclaimers in transmitted information. However, those measures rely on the “honor system” and that any unintended recipient will do the right thing and not read or distribute the confidential information. Encryption is preferred as it does not rely on the “honor system” and removes the human element from the equation.

ABA Recommendations

In accordance with American Bar Association Model Rule 1.6(c), encryption programs are recommended for email, laptop and desktop systems, mobile devices, and storage solutions. Unless implemented, though, these encryption methods will be useless.

Encryption Best Practices

* Familiarize yourself with any policies in place at your firm that require the use of encryption when working with confidential information.
* Avoid using unencrypted USB drives in firm computers, or saving client data or work product to an unencrypted USB drive. If you’re unsure of the contents of a USB drive, contact the appropriate person at your firm to assist you with viewing the drive’s contents.
* Become familiar with the regulatory compliance encryption requirements that apply to client work and follow firm practices for encrypting client data.
* Whenever possible, use a secure, password-protected Wi-Fi connection rather than an unsecure, open connection. Secure connection methods, such as VPNs, encrypt data transmissions and help to protect confidentiality.