4.7. Security Toolkit: Encryption

What Everyone Needs to Know

Encryption is the conversion of data into an unreadable form that helps prevent unauthorized use of such data. Encryption helps ensure confidentiality and keep information secret from those not entitled to see it.

To encrypt data, you need software that uses a key or password to scramble the data, and you need that same key or password and compatible software to decrypt it as well. Most business websites encrypt their data with what is called public key encryption technology. When you see a website URL that starts with https://, the site is using public key encryptions. Encryption is used to help identify an entity such as a website, server, or user.

Encryption technologies are used to protect data and files that are stored in one place (data at rest) and data that is sent from one place to another (data in transit). The legal aid community is moving to more encryption of both data in transit (e.g., email, voice calls, video calls, web meetings, chat) and data at rest (e.g., hard drives, desktops, file servers, cloud servers, backups) to help protect the data against accidental or intentional access or dissemination of data in an unauthorized manner. (Legal Aid providers should also talk to their cloud service providers (e.g., case management, document, fundraising, accounting, HR, telephone) to understand how they encrypt data in transit and at rest.)

Data in transit includes confidential email, voice, or video communications. Lots of messaging services already include encryption (such as WhatsApp, iMessage). Email communications are typically not encrypted by default, but most email solutions either have options to encrypt emails or are compatible with technology to encrypt them. Google's email and Microsoft 365's email solutions both have options for encryptions from Google and Microsoft as well as from third parties.

Data at rest includes data on USB storage keys, hard drives, laptops, smartphones, servers, and backup files. Protecting data at rest is key for any office that wants to prevent data loss when equipment is lost or stolen. A stolen laptop that is encrypted is functionally the same as an empty laptop to a thief.

What IT Needs to Know

When thinking about Encryption, you need to protect the data at rest and the data in transit. Data at rest means data that is housed physically on computer data storage in any digital form. This includes servers, desktop computers, laptops, smart phones, and tablets. Data in transit is data actively moving from one location to another, such as across the internet or through a private network. This includes email, web, collaborative work applications such as Teams, and remote access technologies.

When possible, use services that already include encryption (e.g., web applications that use HTTPS instead of HTTP. Messaging applications with end-to-end encryption). If your technology does not include encryption built in, you can find secondary tools for encryption, both across applications and for sending specific encrypted messages.

Solutions to Consider:

- Proofpoint (email security and protection): Website
- Office 365 (Built in tool): Website
- BitLocker for Windows: Website

Resources

- "Azure data security and encryption best practices" (Microsoft)
- "What is encryption? Data encryption defined" (IBM)
- "What Is Encryption?" (Proofpoint)
- "What Is Data Encryption: Types, Algorithms, Techniques and Methods" (Simplilearn)

Printed:December 2, 2022
http://www.lsntap.org/node/382/47-security-toolkit-encryption