Encryption Basics for Programs Serving Survivors of Gender-Based Violence

Encryption helps to protects information from unauthorized and unwanted access. Options for encryption are available on most smart devices and online platforms.

Victim Service Programs should use encryption to protect data, communications, and websites whenever possible. Survivors can also use it to help protect their devices and communications. This handout will provide an overview on what encryption is and how it can be used by survivors and victim service providers to protect sensitive communications.

What is Encryption?

Encryption protects data so that only authorized people can view it. In simple terms, encryption scrambles the data in such a way that only people who have the right electronic key can unscramble it. The original content could be a message or other information that your computer is sending over the Internet. To read encrypted content, someone must provide a decryption key to prove that they are authorized to view the content. This key might be in the form of a password, or in some other form. It's all simple to the user; you do not need to understand how the technology works in order to use encryption. If you have sent a WhatsApp message or used a mobile banking app, you have used encryption.

There are different kinds of encryption for different needs. Some types protect information stored on your computer. Some types protect information that is moving between different computers. If a product or service says it "is encrypted," it might still not be using the right type of encryption to meet your needs.

Why is Encryption Important for Programs?

Encryption is important for confidentiality. Storing unencrypted personal information about survivors creates a risk. So does sending unencrypted messages with survivors' personal information. In both cases, people outside your organization could obtain that information. Encryption does not stop all breaches of survivor information. However, it is necessary for reducing risk.

Why is Encryption Important for Survivors?

Secure Communications

Encryption allows survivors to use technology strategically and securely. Survivors can use tech to make plans, store and send evidence, and seek help. To do these things safely, survivors need to prevent eavesdropping on their communications. This means they need access to secure online communication channels. They need access to tools – for file storage, sending email, connecting to Wi-Fi, and more – that provide encryption. It's important to note that although encryption can offer some important security, it is not a full solution for survivors seeking safe communications. For example, it does not prevent an abuser from coercing a survivor to give them a password or stop them from using stalkerware on a survivor's device. It also does not stop them from checking how a survivor is using a device if they have physical access and the survivor is logged in. Encryption can be one of *many* useful tools in a survivor's tech safety toolbox.

Protection from Data Breaches

A data breach occurs when private information is accessed by someone without authorization. Nearly all of us, including survivors, have been affected by a data breach at some point. Data breaches are common and they create many risks for survivors. A stalker or abuser could find this information online or buy it from a data broker to locate someone. They or someone else could use sensitive information to steal the survivor's identity. In the case of a breach where the data

is encrypted, the unauthorized person still will not be able to read or access the information without the keys to decrypt it. Encryption is a critical tool to help mitigate the harms that may be caused by breaches.

How Should Service Providers Use Encryption?

Confidentiality requirements for victim service programs are strict. Programs may only share a survivor's personally identifying information (PII) with written, informed, and time-limited direction from the survivor. Because survivor PII can leak through tech-based eavesdropping or data breaches, programs need some tech-based precautions. When choosing and implementing tech, programs should look for the most secure options. Our Selecting a Database resource explains how this applies to database selection. The following are encryption best practices:

Client-side, Zero-Knowledge, and No-Knowledge Encryption

A confidentiality best practice is to store survivor PII in a database or file-sharing system with a form of encryption called *client-side, zero-knowledge,* or *no-knowledge* encryption. These terms refer to encryption that is designed so that no one except authorized people (i.e. people in your organization) can access the information, even including the tech company providing the service if it is cloud-based. This guards against several risks:

- Abusive people or stalkers (or their friends) who work or contract for a tech company misusing their access to the company's resources to obtain survivor data.
- Survivors' PII appearing publicly online because the company's servers were hacked and the data published online.
- The tech company sharing survivor information from the database with law enforcement or other government agencies when the survivor didn't consent to that. This could be the tech company's decision, or their response to a legal process like a valid court order.

If a database company uses encryption, but also has the decryption key for your data, that is called *service-side* or *server-side encryption*. That means that the company could still access the data. They could provide it to a court or law enforcement against a survivor's wishes if ordered to do so. Federal law requires grantees to take reasonable measures to prevent inadvertent disclosures. Best practice to meet this requirement is to use a product where only your organization can access stored survivor data. Server-side encryption is the default for most services. Unless a vendor affirms that a product or service offers client-side/zero-knowledge encryption, the vendor can probably read your data. Vendors may not be familiar with victim service providers' confidentiality needs as they are often stricter than those of other sectors. When storing survivor PII with tech, you should aim for client-side encryption and specifically ask the vendor about this.

End-to-End Encryption

Another term you may hear is *end-to-end encryption* (E2EE). In E2EE, data is encrypted on every step of its journey. For instance, if you send a message in an encrypted messaging app that has E2EE, the app encrypts the message while it is still on your device. It remains encrypted on its way to the tech company's servers, as it passes through the servers, and on its way to the recipient's device. Then the app on the recipient's device can decrypt it. Think of it like a protected tunnel. E2EE protects the data when it's *in motion* (for instance, between a sending and receiving device). Client-side encryption or any encryption that only applies to data "at rest" limits protection to the data when it's sitting in a cloud provider's servers, not while in transit.

E2EE and client-side encryption are not in competition. They serve different purposes, and you should look for solutions that have both of them.

HTTPS and Your Website

While browsing the Internet, you have probably seen “http” or “https” at the start of website addresses (URLs). “HTTP” is an acronym for Hypertext Transfer Protocol (HTTP). A “protocol” is a set of common, agreed-upon instructions, and the HTTP protocol is used to structure network communication on the World Wide Web. HTTPS is a secure variant of HTTP. Unlike HTTP, it encrypts internet traffic. HTTPS is now used by default on most websites.

Encryption with HTTPS is important for the confidentiality and privacy of survivors or anyone else (including you) who visit your organization’s website. You can read more details about this, and about how HTTPS works, in our Wi-Fi Safety & Privacy resource. If your website does not use HTTPS, someone could redirect a visitor's browser away from your website to their own device. The person whose browser is redirected would not know. HTTPS is very important for web security and victim service organizations should be using it for their websites. Most browsers show a security alert if a user tries to visit a site that doesn't support HTTPS and some search engines reduce the search rankings of such sites. This will make survivors less likely to find your site through searches.

You can test whether your website supports HTTPS by visiting your website and checking the full URL. If the “s” is not there, Google has a guide to enabling the use of HTTPS on your website.

Making sure that your site supports the use of HTTPS is an important first step, but not the only one you should take. It should not be survivors’ responsibility to understand HTTPS vs HTTP. Your website may be listed as a resource on other websites. These sites may list an HTTP link rather than an HTTPS one. And without other security measures, a cyberattacker could downgrade a user’s connection to your site from HTTPS to HTTP without the user knowing. Therefore, HTTPS should be the *default* on your website, not merely supported. If users click on old HTTP links, their connections to your site should still be HTTPS. You can do this by using

HTTP Strict Transport Security (HSTS). Your IT staff/service provider can find instructions at the US Chief Information Officers Council website. This site also explains why this is more secure than alternatives.

There are many aspects of designing a safer website besides encryption. To learn more about safer websites, please see our resource on designing websites to increase survivor safety and privacy.

Note: HTTPS does not prevent other "low-tech" eavesdropping risks. Someone could have physical access to a device, have installed stalkerware on it, or have a survivor's account or browser passwords and be able to still see what they have done or are doing online.

Encryption is One Tool, Not a Complete Security or Confidentiality Solution

Encryption is many things, including an essential tool for survivor confidentiality and privacy. However, encryption is not a full solution for either security or confidentiality. Advocates and other staff still need training on confidentiality practices. They should know what information is confidential. They need to know how to use day-to-day technology such as listservs or internal messaging systems without breaking confidentiality. Important security practices beyond encryption include (but are not limited to):

- Good password safety practices. These are as important for organization staff as they are for survivors.
- Ensuring appropriate data access levels. Individuals should have access to only the information that they need to do their job. This way, if a staff member's account is hacked, the damage the hacker can do through that account is limited.
- Website implementation by IT staff or contractors that accounts for the OWASP Top Ten. This is a yearly list of the most common security flaws in web applications.

- Use of firewalls on a program's devices, networks, and website. These filter incoming and outgoing network traffic.
- Always following survivors' explicit instructions on who knows what information about them. It is never okay for an advocate to decide to share survivors' information with anyone outside of your program without their consent. Read more about confidentiality obligations for victim service providers in our Confidentiality Toolkit.

Supported by US DOJ-OVW Grant #15JOVW-23-GK-05144-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.