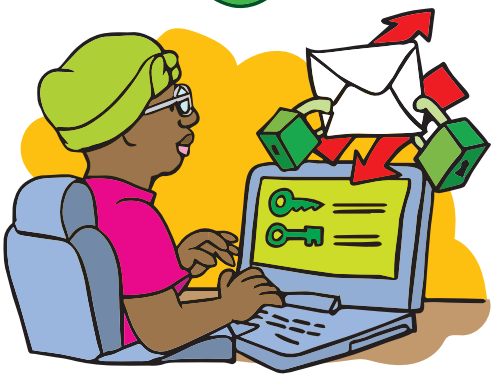
Milpa número 10. 15 de Octubre, 2019

Milpa Digital



Cifrando correos con GPG

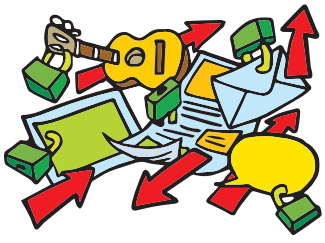
Entendiendo el cifrado

El cifrado se refiere a un proceso de hacer que un mensaje sea ilegible excepto para la persona a la que va dirigido, quien tiene una clave para descifrarlo. No es una técnica nueva, se conoce que Julio César, ya en aquellas épocas (¡unos 50 años antes de la era cristiana!), cifraba sus mensajes de contenido militar.

Hoy en día las computadoras hacen el cifrado en vez de que lo hagamos manualmente y la tecnología del cifrado se ha ampliado más allá de los simples mensajes. Empecemos a entenderlo mejor, existen dos formas de cifrado:

Cifrado de datos en reposo Se refiere a cifrar datos que no están viajando por la red, como nuestro disco duro, un archivo en nuestra computadora, o una partición dentro de nuestro disco duro.

Cifrado de datos en tránsito: Se llaman así porque son datos que están viajando por internet los que se cifran, ya sean mensajes de texto, páginas web, imágenes, música, etc.



Existen dos formas de cifrar la información que está en tránsito:

- **El cifrado en la capa de transporte:** Los datos se cifran mientras circulan por la red, por ejemplo cuando usamos una VPN (Milpa 33) o la extensión Https Everywhere de Firefox (Milpa 15) estamos cifrando datos en la capa de transporte.

- **El cifrado de extremo a extremo:** Los archivos se cifran y descifran en nuestros dispositivos. Se usa por algunas aplicaciones de mensajería como Signal (Milpa 6) y Wire (Milpa 5). El correo electrónico cuando sale cifrado con GPG usa cifrado de extremo a extremo.

Cifrando nuestro correo electrónico con GPG

Para usar cifrado necesitamos ponernos de acuerdo en cual será el protocolo para descifrarlo. En el caso de Julio César, ese protocolo era cambiar cada letra del abecedario por tres letras más adelante, la A se volvía una D y así sucesivamente, entonces CASA venía a ser FDVD.

GPG viene del inglés y quiere decir GNU Privacy Guard, que es la versión libre de cifrado del protocolo llamado PGP , que viene de Pretty Good Privacy. Por eso es posible llamarlo de ambas maneras, aunque su versión libre es GPG.

GnuPG

Cifrar un correo electrónico es parecido a poner un mensaje en una caja, cerrarlo con llave y enviarlo a la persona destinataria. Excepto que necesitaremos dos llaves (que no son más que unos archivos de texto) para que funcione: una **pública** y otra **privada**.

La llave pública la podemos repartir entre nuestras amistades, y la llave privada la guardaremos en un lugar seguro. Tener la llave pública de alguien nos permite **cifrar un mensaje para esa persona** , y nuestra llave privada la usamos para **descifrar los mensajes cifrados que nos envían**.

Aunque dos personas usen correo cifrado, terceras personas como proveedores de servicios de correo electrónico, proveedores de servicios de internet, etc. pueden saber que: estas dos personas se están comunicando y están usando cifrado, y otro tipo de información sobre la comunicación como el lugar, la hora, el idioma, etc.

Nuestras herramientas

Para usar correo cifrado en nuestra computadora es aconsejable usar **Thunderbird**, un gestor de correos electrónico desarrollado por Mozilla, que se puede descargar desde su página web **https://www.thunderbird.net/es-MX/**.

A Thunderbird le añadiremos **Enigmail**, una extensión que nos permitirá generar llaves de cifrado y usar el protocolo OpenPGP para cifrar correos electrónicos. No recomendamos cifrar los correos desde el celular ya que son dispositivos más inseguros para tener acceso a información tan sensible.

Como dijimos al principio, la tecnología del cifrado es muy amplia, y cifrar correos es solo una pequeña parte de aquello para lo que se usa.

Es recomendable leer y aprender más antes de empezar a usar cifrado.Recomendamos revisar las guías sobre GPG, Thunderbird y cifrado en general de la Electronic Frontier Foundation https://ssd.eff.org/es

Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital

¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!

CódigoSur EDICIONES

Créditos: CódigoSur 2019. MilpaDigital. https://milpadigital.org.
Licencia CC https://creativecommons.org/licenses/by-sa/4.0/deed.es.

creative commons