Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen

Imagen: REUTERS/Mario Anzuoni

¿Qué harías si tuvieras que compartir un secreto con alguien por teléfono y no quisieras que nadie se entere?

Probablemente uses un mensaje cifrado y entonces estarías aplicando la criptografía. **La criptografía es el arte de escribir con clave secreta o de un modo enigmático**, define la Real Academia Española (RAE).

Y este arte es tan antiguo como la invención de la escritura misma por parte de los seres humanos.

Uno ejemplo claro de ello es la piedra de Rosetta que se encuentra en el Museo Británico en Londres.

Esta piedra contiene escrito un decreto atribuido al faraón egipcio Ptolomeo V en el año 196 antes de Cristo.

Y en la piedra Rosetta aparece casi el mismo contenido en tres escrituras distintas: jeroglíficos egipcios, la escritura demótica (que era el idioma de los egipcios) y el griego antiguo.

Entonces, el descubrimiento de esta piedra en 1799 resultó un elemento clave para poder descifrar los jeroglíficos egipcios.

Pero ¿qué función tiene la criptografía en la actualidad? Y ¿cómo puede ser que la utilices todos los días sin que te des cuenta?

Seguridad

La criptografía se utiliza en la actualidad para dar garantías de seguridad a la información.

"**Es la responsable de proteger nuestros datos en las comunicaciones** para que solamente la persona receptora de ese mensaje pueda leerlo y ninguna otra pueda acceder a esa información si no es la destinataria legítima", explica la ingeniera y doctora en Informática, Carmen Torrano.

La criptografía ofrece claves capaces de cifrar o descifrar esa información utilizando diferentes técnicas.

"Está la transposición, que es cuando los caracteres se barajan de alguna manera para que no se entienda el mensaje original. También se utiliza la sustitución, que es donde un carácter es reemplazado por otro", enumera.

"Esto con el tiempo se fue volviendo más complejo con sistemas mono alfabéticos, poli alfabéticos, y otras técnicas porque también se fueron complicando los ataques", le dice a BBC Mundo Torrano, que trabaja como investigadora senior en la empresa de ciberseguridad Eleven Paths, en Telefónica, España.

Dejando huellas

Sin embargo, la criptografía en la actualidad no sirve solamente para mantener en secreto la comunicación entre dos personas.

"**La criptografía está en todas partes.** Cuando realizamos una llamada por teléfono, cuando vamos al banco a sacar dinero... en muchos de los casos se están aplicando algoritmos sin que lo sepamos", añade Torrano.

Por un lado con el celular llamamos, mandamos mensajes a través de diferentes aplicaciones, tomamos fotos y videos que también enviamos.

"Esa sería la **información consciente** que transmitimos con nuestros teléfonos", describe María Isabel González Vasco, profesora de Matemáticas Aplicadas del departamento MACIMTE de la Universidad Rey Juan Carlos, de España.

Y mucha de esa información sabemos que está cifrada, como por ejemplo si usamos las aplicaciones de mensajería instantánea Whatsapp o Telegram que ofrecen un servicio de encriptación de extremo a extremo.

Esto quiere decir que el mensaje está en clave y si alguien quisiera interceptarlo, atacando el teléfono, no podría leer el contenido porque está cifrado. Y para ello se utiliza la criptografía

Pero luego hay otros tipos de datos que es inevitable que no podamos compartir. Por ejemplo, la información de localización que es inseparable al uso del celular porque la señal del teléfono es captada por distintos repetidores.

"Y esa **información** se la estamos cediendo a la compañía de teléfono y muchas veces a otras entidades de manera más **inconsciente**", alerta González Vasco que también es codirectora del proyecto *Science for Peace and Security* (Ciencia para la paz y la seguridad, SPS en inglés) de la OTAN sobre seguridad de las comunicaciones en la era cuántica.

"También están las aplicaciones que utilizamos para comprar o para almacenar nuestra música que **van construyendo un rastro de información** y que delegamos muchas veces de manera inconsciente porque no leemos las políticas de privacidad de las app", asegura.

¿Por qué es importante proteger nuestros datos?

Aunque tal vez te parezca que a nadie le puede importar qué compras, dónde te mueves o a qué hora tienes tus rutinas, **tus datos pueden ser de extrema utilidad para muchos.**

"Esa información se puede vender y se puede utilizar para fines comerciales. Si ciertas empresas tienen gran cantidad de información de los clientes de una zona y pueden controlar qué tipo de cosas se compran en otros comercios, pueden hacerse con el monopolio del comercio de esa localidad sin tener que haber competido de manera justa con precio y calidad", ejemplifica González Vasco.

"Los criptógrafos siempre decimos que es mucho más potente decir una mentira a cada cliente potencial construida para él, que decir una mentira universal para todos. Va a ser más efectivo decirle a cada uno lo que quiere oír", señala la profesora de la Universidad Rey Juan Carlos, de España.

"Por eso Facebook es un negocio redondo porque la información que recauda de los usuarios permite hacerse una idea muy precisa del tipo de consumo que hace esa persona y ni hablemos de tendencias políticas y religiosas y otros temas más sensibles", agrega.

La ingeniera Torrano coincide y opina que **cualquier usuario puede ser blanco de monitoreo o robo de información.**

"Cuando navegamos por internet, aunque tengamos medidas de seguridad, muchas veces a través de las cookies (datos que almacenan los sitios web en tu navegador)

hay empresas que se dedican a recolectar información (…) para estudiar hábitos", asegura.

"Toda esa información la utilizan las empresas para conocer mejor al cliente y, si se utiliza bien, puede que tengas una experiencia de usuario más cómoda y personalizada, pero si se utiliza mal, esos datos se pueden llegar a vender a empresas para otros fines, como influencia en temas políticos, etc.", describe Torrano.

"Todos somos susceptibles a ser atacados y por eso es muy importante tomar las medidas adecuadas", añade.

¿Qué hacer para proteger nuestros datos?

Ambas expertas consultadas por BBC Mundo revelan algunos consejos y medidas que se puedan tomar adicionalmente para estar seguros utilizando la criptografía.

1. Mensaje cifrado

Observar si una aplicación de mensajería dice que **cifra los mensajes de extremo a extremo.**

"Son pistas de que nuestra información se está tratando con cierta seguridad", dice González Vasco.

"También existen aplicaciones que permiten cifrar las llamadas y los *sms* (mensajes de texto) para personas que tienen información muy importante o confidencial", agrega Torrano.

2. Políticas de privacidad

Hay que leer siempre la política de privacidad de las aplicaciones.

"Es importante ser consciente de que **no es necesario dar todos nuestros datos a una plataforma** de servicios de música online para que ellos nos den recomendaciones. Hay herramientas técnicas que permiten hacer recomendaciones sin que uno ceda demasiados datos", opina González Vasco.

"Si quiero una aplicación que mida mis pasos, por ejemplo, ¿hay alguna cuya política de privacidad me garantice que va a borrar los datos de mis trayectos? ¿Tengo control sobre esos datos? Leer ese tipo de cosas nos hace muchísimamente menos vulnerables", añade.

3. Detectores

Existen **herramientas con apoyo criptográfico** que podemos descargar y que pueden **detectar rápidamente si entra malware** (software malicioso) a través de una aplicación.

"Se trata de algún tipo de software que puede ser instalado con una aplicación que parece inocente y que termina leyendo otra información que pueda estar almacenada en nuestro teléfono", describe González Vasco.

4. Agregadores

"Los **agregadores (lectores o recopiladores de contenidos)** son muy cómodos, porque en una sola aplicación puedes mirar todo, como las cuentas bancarias. Pero creo que este tipo de recursos hay que utilizarlos con mucha precaución", advierte la profesora González Vasco.

Por ejemplo, un supermercado en el que haces compras online te permite a través de su web no solo hacer la lista de la compra para ellos sino la de otras tiendas diferentes.

"Entonces al supermercado, que suele ser el dueño del agregador, le estás dando no solo los datos de lo que le compras a él, sino los de todo lo que compras", explica la especialista.

5. Conexiones públicas

"Cuando te conectas a **las redes de internet (wifi) públicas no debes ingresar a sitios que sean confidenciales**, como por ejemplo el banco para hacer una transacción. Estas son redes abiertas que no están cifradas y que otras personas pueden estar accediendo a tu información", advierte Torrano.

Tampoco "cargar el portátil en cualquier sitio, o fuente USB que haya en una cafetería en un aeropuerto. Estas son acciones muy convenientes, pero pueden tener algún tipo de consecuencias si uno lleva información sensible en la computadora", agrega González Vasco.

6. Red Privada Virtual

Instalar una **aplicación de VPN (Red Privada Virtual) en el celular.**

"Es como un túnel por el que van los datos que van cifrados y esto permite que la comunicación vaya 'encriptada' y que alguien no la pueda interceptar. Hay aplicaciones hasta gratuitas para descargar en el teléfono móvil", aconseja Torrano.

7. Anonimato

"Otra medida para fomentar la privacidad del usuario es **utilizar redes anónimas** como Tor o I2P, o Freenet", dice Torrano.

Estas redes "pretenden conservar la privacidad del usuario para que esos rastros que vamos dejando cuando navegamos por internet no sean descubiertos poniendo muchos elementos intermedios como servidores y utilizando también la criptografía".

"Y esto es como todo: hay personas que utilizan el anonimato para proteger su privacidad, pero otras desgraciadamente, lo usan para hacer cosas ilegales, como tráfico de armas, drogas, personas, etc.", destaca.

8. Dominios seguros

"Cuando accedemos a determinados dominios (direcciones de internet) debemos asegurarnos que el navegador sea seguro", aclara la doctora en Informática, Carmen Torrano.

"Muchos aparecen con un **candado en verde o en rojo y si muestra https** (con la 's' al final) significa que estamos utilizando una capa de cifrado y esto es lo recomendado porque estamos navegando por sitios que son de confianza", agrega.

9. Certificado digital

"Se puede instalar un certificado digital y utilizarlo para **firmar documentos. Esto también es parte de la criptografía**", asegura Torrano.

El certificado digital permite la firma electrónica de documentos. Quien recibe un documento firmado puede tener la seguridad de que es el original, no fue manipulado y el autor de la firma electrónica no puede negar su autoría.

10. Respaldo o "Back up"

"Es recomendable como medida de protección hacer un *back up* (respaldo de información) de los datos del teléfono **en el caso de ser víctima de la criptografía mal utilizada**", dice Torrano.

Un ejemplo de esto es ser atacado por un *ransomware*, que infecta el teléfono cifrando los datos de forma que el usuario no pueda acceder a ellos. **Esta es la criptografía que se utiliza para atacar**", señala la especialista en ciberseguridad.

El *back up* se puede hacer conectando el teléfono a la computadora o a la nube.

Educación del usuario

Es una realidad que para proteger mejor nuestros datos no basta con herramientas sofisticadas que utilizan criptografía.

"Es muy importante hacer que la gente sea consciente que revelar continuamente su localización, gustos de consumo, o ideas políticas es proporcionar poder a grupos que escapan al control. Y eso hace que seamos mucho más vulnerables como consumidores y en general como ciudadanos", reflexiona la profesora González Vasco.

"**La criptografía lamentablemente no es como una buena medicina. Es más bien como unos buenos hábitos higiénicos sumados a una buena**

alimentación. Hay mucho que podemos hacer nosotros y que no es sustituible por herramientas tecnológicas mágicas que tengamos en el celular", concluye

Fuente:

Lorente, A. (2019). Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. World Economic Forum https://es.weforum.org/agenda/2019/12/criptografia-que-es-y-por-que-deberias-usarla-en-tu-telefono-para-que-no-te-espien/