Consejos Técnicos: alguien podría estarme espiando[1]

Por Antonio Hernández

Que "Alguien me puede estar espiando" no es el título de la próxima novela de espionaje o una "mitología urbana" que anda circulando por ahí. Se trata de una verdadera amenaza resultado del uso de aparatos "inteligentes" que tienen cámaras fotográficas, como las computadoras, las tabletas y los teléfonos. Cuando uno trabaja con la computadora, algún "pirata informático" –comúnmente conocidos como "hackers– o algún otro criminal que usa la tecnología informática, potencialmente puede verlo o escucharlo, aunque uno no esté usando la cámara o el micrófono. Esto se refiere más que nada a los sistemas operativos más comunes, como Android y Windows.

¿Cómo logran hacerlo? Primero, tratan de encontrar la manera de instalar "software malicioso" –conocido como "malware" –en su computadora. "Malware" es una especie de programación "troyana"[2] que pertenece a la familia de software conocida como "Software de Control Remoto" (la sigla en inglés es "RAT") –o sea, es una clase de virus de computadoras. Una vez que está instalado, el pirata informático puede tomar control de su computadora y activar la cámara y el micrófono, sin que uno se dé cuenta. Este fenómeno ocurre más que nada en aparatos y en programas que han sido diseñados dándole más importancia a su funcionalidad que a su seguridad. Es el precio que todos pagamos por tener acceso a tecnologías fáciles de usar a un precio razonable.

¿Cómo puede uno reducir el peligro de una intrusión? Existen varias recomendaciones para evitar las intrusiones:

- Cubra la cámara de su aparato. Use una cinta adhesiva o, mejor aún, una "ventana", que es un dispositivo o cobertura especial diseñado para tapar la cámara. No cuesta más que un par de dólares. Yo he incorporado eso a todos mis aparatos, y una buena costumbre es tener cerrada dicha "ventana" cuando no se esté usando la cámara. Durante video conferencias o comunicaciones

[1] Este artículo se escribió basado en un artículo publicado en el periódico colombiano El Tiempo, el 18 de junio de 2020.
[2] Se denominan troyanos o troyanas, por el mito del Caballo de Troya

cara a cara, yo solamente abro la "ventana" cuando estoy seguro de que la persona o el grupo de personas con las que voy a interactuar son de mi confianza. Esto también protege su privacidad y le puede evitar situaciones incómodas.

- Tenga cuidado con los programas o las aplicaciones que "descarga" de la Internet, especialmente los GRATIS. Trate de verificar la fuente o la compañía productora o vendedora del programa; verifique si hay comentarios o análisis del producto, escritos por los consumidores. Siempre trate de descargar programas del sitio oficial de la compañía productora o vendedora.

- En los programas o las aplicaciones que descargue, especialmente en los GRATIS, siempre lea la "letra menuda" del vendedor antes de instalarlos. Uno siempre se sorprende de todo lo que uno está autorizando en términos de cómo los vendedores van a usar nuestra información personal. Un detalle demasiado común que se usa con las plataformas móviles como celulares y tabletas es la autorización de ver dónde está usted. ¡¡Esencialmente, lo van a poder seguir por todos lados y saber dónde está usted –todo el tiempo!!

- Evite todos los mensajes, encuestas y ofertas que prometen cosas más allá de lo razonable. Generalmente esas ofertas no tienen sentido, pero sirven como mecanismo para "cosechar" información personal suya, y pueden "infectar" su aparato. Siempre esté alerta y piense si "esto es demasiado bueno para ser verdad".

- NUNCA inserte una unidad de memoria USB en sus aparatos, si usted no está seguro de quién o dónde esa unidad USB ha sido usada antes.

Recuerde, siempre que utilice aparatos electrónicos use el sentido común y emplee prácticas seguras.