- ¿Lo sabías?: Cinco mandamientos para asegurar tu vida digital

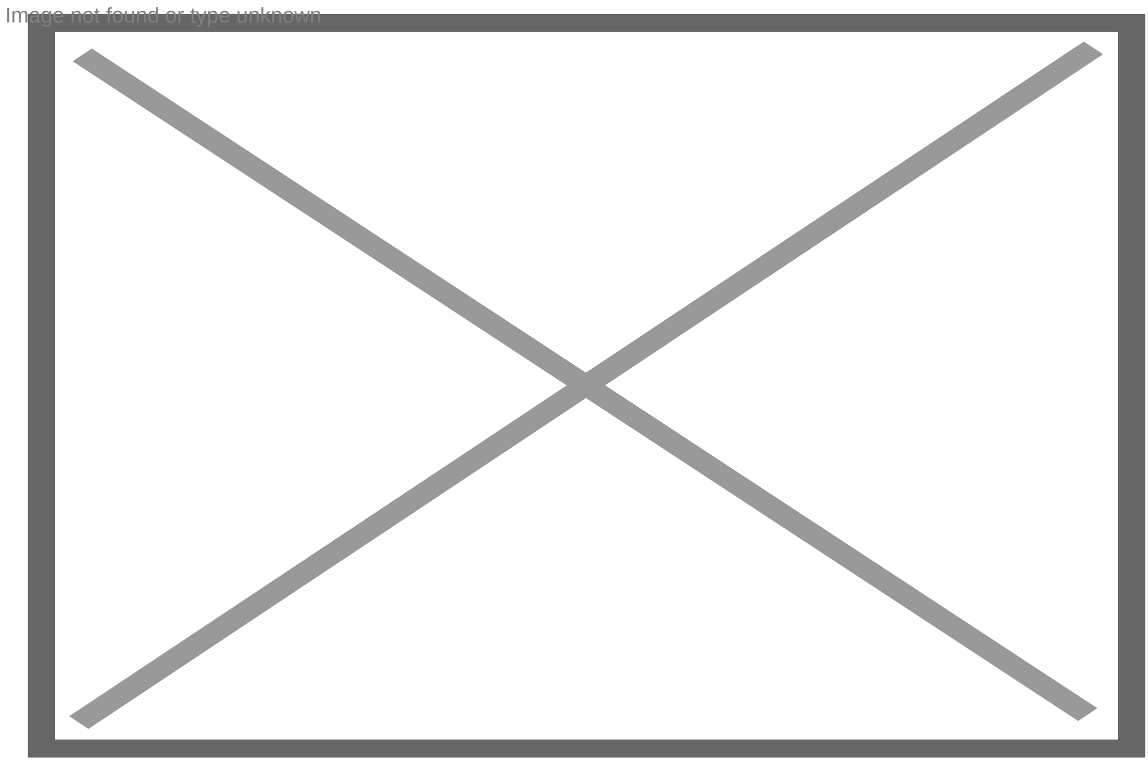

Foto: Internet.

La tecnología siempre está cambiando, al igual que la forma en que la usamos. Eso significa que siempre encontraremos nuevas formas de bajar la guardia para que personajes malignos espíen nuestros datos.

¿Recuerdas cuando compartiste tu lista de contactos con aquella nueva aplicación popular? ¿O cuando publicaste fotografías en las redes sociales? Todas esas acciones podrían tener consecuencias que debiliten tu seguridad y la de las personas que te importan.

Vijay Balasubramaniyan, director ejecutivo de Pindrop, una firma de seguridad que desarrolla tecnología para detectar llamadas telefónicas fraudulentas, afirmó que siempre debemos recordar que cualquier parte de nuestra identidad que publiquemos en internet podría con el tiempo ser utilizada por estafadores para intentar apoderarse de nuestras cuentas en línea.

“Tu identidad digital, que incluye todas tus imágenes, videos y audio, les permitirá en esencia a los hackers crear una identidad completa de ti, que se ve exactamente como tú, en la que no estarás involucrado”, dijo.

Por lo tanto, te presento algunas de las directrices más importantes —como fortalecer contraseñas y minimizar los datos compartidos por la cámara de tu teléfono— para que tanto tú como tus seres queridos permanezcan a salvo en el futuro previsible. Me referiré a estos como los cinco mandamientos tecnológicos, con la esperanza de que los recuerdes como si fueran el evangelio.

No utilizarás contraseñas débiles

Hablemos de los malos hábitos de las contraseñas. Cerca del 45 por ciento de los estadounidenses utilizan contraseñas débiles de 8 caracteres o menos, según una encuesta realizada por security.org, una compañía de investigación (el 14 por ciento usó “Covid” en sus contraseñas el año pasado). La mayoría de los estadounidenses también reconoció reutilizar la misma contraseña para sitios web diferentes.

Esto abre las puertas a muchos problemas de seguridad. Los ciberdelincuentes que intenten obtener acceso a tu cuenta pueden adivinar con facilidad las contraseñas débiles. Además, si utilizas la misma contraseña para varios sitios, como, por ejemplo, la de tu cuenta bancaria, la cuenta de compras en Target y Facebook, entonces lo único que se necesita es que uno de esos sitios sea hackeado para que todas esas cuentas queden vulnerables.

Para la mayoría de las personas, la solución más simple es un administrador de contraseñas, un software que ayuda a generar de manera automática contraseñas largas y complejas para las cuentas. Todas las contraseñas se almacenan en una bóveda a la que solo se puede acceder con una contraseña maestra. Mi herramienta favorita es 1Password, que cuesta 36 dólares al año. Sin embargo, existen administradores de contraseñas gratuitos como Bitwarden.

La otra opción es anotar las contraseñas en una hoja de papel que esté almacenada en un lugar seguro. Solo asegúrate de que las contraseñas sean largas y complejas, con algunas letras, números y caracteres especiales.

Utilizarás autenticación multifactor

No importa cuán fuerte sea tu contraseña, los piratas cibernéticos de todos modos podrán obtenerla si logran vulnerar los servidores de una compañía que contiene tu información. Es por eso que los expertos en seguridad recomiendan la autenticación multifactor, también conocida como la verificación en dos pasos.

La autenticación multifactor ha funcionado por lo general de la siguiente manera: digamos, por ejemplo, que ingresas tu nombre de usuario y contraseña en tu cuenta bancaria en línea. Ese es el paso uno. El banco procede a enviar un mensaje de texto a tu teléfono con un código temporal que debe ser ingresado en el sitio para permitirte el acceso. Ese es el paso dos. De esta manera, demuestras tu identidad con el acceso a tu teléfono y a ese código.

La mayoría de los sitios web y aplicaciones principales, incluidos Facebook y los principales bancos, ofrecen métodos de verificación en dos pasos que implican mensajes de texto o las llamadas aplicaciones de autentificación que generan códigos temporales. Basta con buscar en internet las instrucciones de configuración.

Si una empresa no ofrece autenticación multifactor, probablemente debas buscar otro producto, dice Balasubramaniyan.

"Si un proveedor dice: 'Solo uso contraseñas', no es lo suficientemente bueno", dijo.

No compartirás en exceso

Muchos de nosotros utilizamos nuestros teléfonos como nuestras cámaras diarias. Pero nuestros celulares recopilan muchos datos sobre nosotros y el software de la cámara puede registrar de manera automática nuestra ubicación cuando tomamos una fotografía. Esto con mayor frecuencia es un riesgo potencial de seguridad antes que un beneficio.

Comencemos por la parte positiva. Cuando permites que tu cámara etiquete tu ubicación, las aplicaciones de gestión de fotografías como Apple Fotos y Google Fotos pueden organizar de forma automática las imágenes en álbumes según la ubicación. Eso es útil cuando sales de vacaciones y quieres recordar dónde estuviste cuando tomaste esa foto.

Pero cuando no estás de viaje, tener tu ubicación etiquetada en las fotografías no es precisamente ideal. Supongamos que acabas de conectar con alguien en una aplicación de citas y le enviaste un mensaje de texto con una fotografía de tu perro. Si tenías activa la función de localización cuando tomaste la foto, esa persona podría analizar los datos para identificar dónde vives.

Para estar protegido, asegúrate de que la función de localización de fotografías esté desactivada de forma predeterminada:

En los iPhones, abre la aplicación Configuración, selecciona la opción Privacidad, luego Servicios de ubicación y, finalmente, Cámara. En "Permitir acceso a la ubicación", selecciona "Nunca".

En celulares con sistema Android, dentro de la aplicación Cámara, toca el ícono de Configuración / Ajustes que parece un engranaje. Busca la opción de Ubicación (Etiquetas de ubicación o Guardar ubicación dependiendo de la marca del teléfono) y desactívala.

Puedes optar por activar la función de localización temporalmente para documentar tus vacaciones, pero recuerda desactivarla cuando termines tu viaje.

Jeremiah Grossman, director ejecutivo de Bit Discovery, dijo que debemos ser juiciosos con las fotos que tomamos y enviamos a otros. Las fotografías explícitas podrían llegar a exponerse al público.

"La gente se separa, y la gente es imbécil", dijo. "Incluso si no es el caso, si le das unas fotos a alguien y te las piratean, de repente todo el mundo puede verlas".

No compartirás datos de amigos

Esta es una lección que tenemos que aprender una y otra vez: por lo general no es buena idea dar información sobre tus amigos cuando utilizas sitios web y aplicaciones, en especial con marcas desconocidas.

Cuando, por ejemplo, compartes tu lista de contactos con una aplicación, estás potencialmente proporcionando los nombres, números de teléfono, domicilios e información de correo electrónico de todos tus conocidos a esa compañía.

Cuando compartes tu lista de contactos con una aplicación para invitar a otros a unirse, estás cediendo la información de los demás, incluso si deciden no aceptar la invitación.

Por lo general, cuando compartes tu lista de contactos con una aplicación, es con el propósito de encontrar a otros amigos que también estén utilizando ese servicio. Pero Clubhouse, una aplicación de redes sociales que se ha popularizado durante la pandemia, fue criticada recientemente por su agresiva recolección de listas de contactos.

Al registrarse en Clubhouse, los usuarios pueden negarse a compartir sus listas de contactos. Pero incluso si lo hicieran, otros usuarios de la aplicación que sí las subieron podrían ver que esos nuevos usuarios se han unido al servicio. Esto no es un escenario ideal para las personas que intentan evitar contacto con exparejas abusivas o acosadores.

Más de 10.000 usuarios firmaron una petición en la que se quejaban del fallo de privacidad, según el regulador de datos francés, que dijo la semana pasada que había abierto una investigación sobre Clubhouse.

Clubhouse actualizó la aplicación este mes, para abordar algunos de los problemas de privacidad. No respondió inmediatamente a una solicitud de comentarios.

Hay formas más amables que compartir tu libreta de direcciones para saber si tus amigos utilizan un nuevo servicio, como preguntarles directamente.

Recordarás permanecer escéptico

Todos los expertos en seguridad están de acuerdo en una regla básica: no confíes en nadie.

Cuando recibas un correo electrónico de alguien pidiéndote tu información personal, no hagas clic en ningún enlace y comunícate con el remitente para preguntarle si el mensaje es auténtico. Los estafadores pueden incrustar con facilidad correos electrónicos con programa malicioso y hacerse pasar por tu banco, aseguró Adam Kujawa, director de la firma de seguridad Malwarebytes.

En caso de duda, opta por no compartir datos. Las empresas y los bancos han experimentado con tecnologías de detección de fraude que escuchan tu voz para verificar tu identidad. En algún momento, incluso podrías interactuar con representantes del departamento de servicio al cliente a través de videollamadas.

Los estafadores más sofisticados podrían con el tiempo utilizar los componentes audiovisuales que publicas en línea para crear un ultrafalso, un clip de audio o video generado por computadora haciéndose pasar por ti, afirmó Balasubramaniyan.

Si bien esto puede sonar alarmista —los ultrafalsos no son todavía una preocupación inmediata— una buena dosis de escepticismo nos ayudará a sobrevivir el futuro.

“Piensa en todas las diferentes formas en las que estás dejando identidad biométrica en tu mundo en línea”, dijo Balasubramaniyan.

(Tomado The New York Times en Español)

Radio Habana Cuba