EL MERCURIO

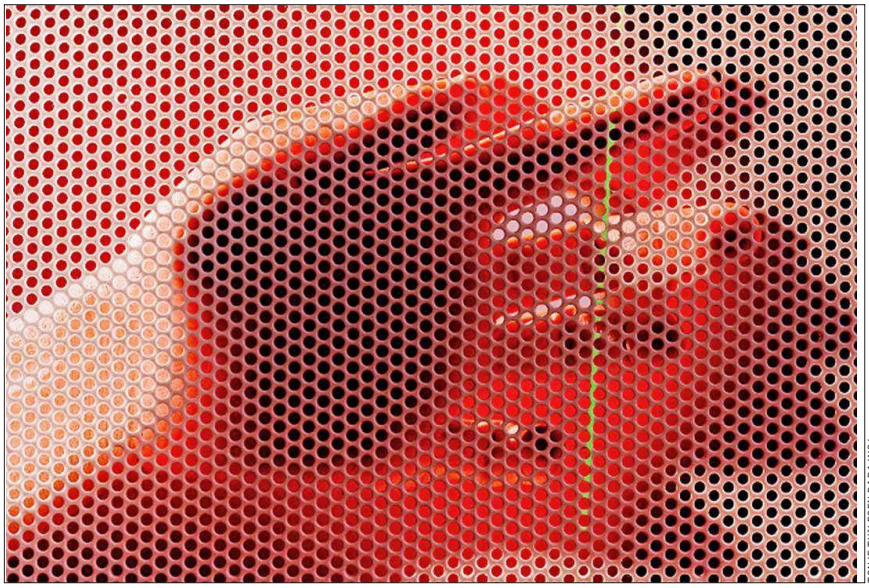
Fecha: 18/09/2024 Audiencia: 66.983 Sección: ECONOMIA
Vpe: $8.340.761 Tirada: 20.174 Frecuencia: 0
Vpe pág: $20.570.976 Difusión: 19.138
Vpe portada: $20.570.976 Ocupación: 40,55%

Los riesgos en el tratamiento digital de la información biométrica:

Amazon quiere su palma y la TSA, su rostro. Qué significará decir que sí

Utilizar sus datos corporales para pagar o pasar con facilidad por seguridad es como desbloquear su teléfono, en cierto modo.

CORDILIA JAMES
THE WALL STREET JOURNAL



TONJE THILESEN PARA WSJ

Cada vez más empresas y entidades de gobierno quieren leer las partes de nuestro cuerpo.

Ya no necesito andar con mi billetera o teléfono cuando compro en Whole Foods. En cambio, puedo pagar con mi palma.

Todo lo que tuve que hacer fue ingresar en la aplicación Amazon One, dar permiso a Amazon para que utilice los datos únicos de mi cuerpo —biometría— y tomar una foto de cada una de mis palmas. Amazon utilizó esas fotos para generar una representación basada en números llamada una "firma palmar" en su nube, luego borró las imágenes, indica la compañía.

Después de que elegí una tarjeta de crédito para vincularla con mi palma, fui al Whole Foods más cercano. Extendí mi mano sobre un sensor de palma en la caja y salí con una caja de barras de proteínas con chips de chocolate.

Cada vez más empresas y entidades de gobierno quieren leer las partes de nuestro cuerpo. La Administración de Seguridad en el Transporte (TSA), por ejemplo, empezó a escanear los rostros de los pasajeros en lugar de revisar los documentos de identidad. Estos grupos explican que el propósito de estos procesos biométricos es eliminar la fricción, ahorrar tiempo y reducir las filas.

Aunque podrían parecerse a los sistemas de huellas dactilares y reconocimiento facial que hemos utilizado durante años, estos servicios son diferentes. Nuestros teléfonos y *laptops* guardan para sí nuestra información biométrica. Para funcionar, los servicios públicos recolectan y extraen datos vinculados con usted y los almacenan en la nube. Eso implica mayores riesgos de seguridad y una nueva serie de preocupaciones para usted, el consumidor.

Para decidir si debería decir que sí y darles su cara o palma, tiene que saber cómo funcionan, cómo se protegen sus datos y en quién puede confiar para que conozca su cara y sus manos.

Cómo funciona

Cuando instala Face ID en un iPhone, Apple captura un mapa y una imagen infrarroja de su rostro, luego los convierte en un código matemático que se almacena solo en el dispositivo. Cuando desbloquea su iPhone con su cara, los sensores del teléfono leen su cara de nuevo, comparando el nuevo código con el que está almacenado. Si hay coincidencia, ¡perfecto! Ya entró.

En algunos puestos de control de seguridad del aeropuerto, la TSA hace algo como esto: una cámara le toma una fotografía y la compara con la que está en su documento de identidad, para asegurarse de que es la misma persona. Todo eso sucede frente a usted y las imágenes se borran de inmediato.

Touchless Identity Solution de la TSA es más futurista. Usted mira a la cámara, y esta le dice al agente que está bien que siga. No se requiere de ningún documento de identidad. Para que esto funcione, la TSA tiene que tener información de antecedentes que usted ya ha compartido.

Para empezar, tiene que tener un pasaporte estadounidense y TSA PreCheck, y ser miembro de un programa de cliente frecuente de una aerolínea participante. Cuando los viajeros aptos hacen el *check in* utilizando la aplicación de su aerolínea, pueden optar por el escaneo de sus datos biométricos.

El hecho de optar por ese sistema permite que la TSA solicite a la Oficina de Aduanas y Protección de Fronteras de EE.UU. que localice su información y agregue su fotografía a su Servicio de Verificación de Viajeros basado en la nube. Hace esto para todos los otros pasajeros registrados que vuelen desde ese aeropuerto dentro de las próximas 24 a 48 horas.

SEGURIDAD
Las compañías no son totalmente inmunes a las violaciones de datos, las lecturas inexactas o algún tipo de hackeo avanzado.

Cuando se aproxima a la cámara, el sistema trata de comparar su imagen en vivo con la que está almacenada. Si hay coincidencia, avanza sin mostrar su documento de identidad. La imagen en vivo y la que está almacenada se borran dentro de 24 horas después de la partida de su vuelo.

En Whole Foods, el escaneo de su palma se compara con la firma palmar registrada en la nube de Amazon hasta que encuentra una coincidencia. Cuando eso sucede, se realiza la transacción.

Puesto que todo lo que Amazon guarda es la firma matemática de la palma, no las fotos reales de la palma, no sería útil para un *hacker* que quisiera, por ejemplo, desbloquear un sistema biométrico diferente basado en la palma. Igualmente, se almacena en forma separada de la información de su tarjeta de crédito, indica una vocera de Amazon. Las posibilidades de que el sistema confunda la firma de su palma con la de otra persona también son extremadamente bajas: Amazon asegura que no ha tenido ningún falso positivo después de millones de interacciones con los consumidores.

Manejarlo en forma responsable

Probablemente es obvio que el sistema de coincidencia facial de la TSA no puede ser engañado por un delincuente que ponga la foto de usted en su rostro. El agente sabría que algo pasa.

Esa es la ventaja que brinda la lectura biométrica en un lugar público, observan analistas.

"No es algo que probablemente alguien pueda falsificar, porque está en una tienda pagando por cosas", dice Maxine Most, jefa ejecutiva de Acuity Market Intelligence, una firma consultora de tecnología enfocada en biometría e identidad digital.

Sin embargo, aun cuando no haya ningún vigilante humano cerca, estos sistemas generalmente utilizan la detección de "vitalidad", observando el movimiento, la profundidad, la textura y otros factores. Incluso funciona para las huellas de la palma: cuando sostuve una foto de mi mano sobre el sensor en Whole Foods, el sistema no la reconoció.

La detección de vitalidad funciona bastante bien en estos entornos, siempre que alguien no haya creado una máscara facial suya al estilo de Ethan Hunt. Pero el reconocimiento facial podría no ser tan útil en el futuro, dicen analistas de seguridad, especialmente en situaciones en línea donde no lo tienen que ver en persona.

Las *deepfakes* generadas con IA se están volviendo más sofisticadas; al imitar expresiones faciales, patrones de parpadeo y micromovimientos. Alrededor de un 30% de empresas no dependerá de la verificación de identidad por su cuenta para 2026 debido a ataques de *deepfakes* generados con IA, pronosticó la firma de investigación Gartner en febrero.

Y aunque, en general, puede confiar en instituciones y compañías tecnológicas intachables para que manejen sus datos biométricos, estas no son totalmente inmunes a las violaciones de datos, las lecturas inexactas o algún tipo de hackeo avanzado que aún no hemos visto.

"Eso es lo que me preocupa más, que una máscara o una *deepfake*, o que alguien saque mi foto de Facebook", expresa Frances Zelazny, jefe ejecutivo de Anonybit, un emprendimiento que se centra en proteger los datos biométricos.

Sin embargo, la conveniencia y eficiencia de los sistemas biométricos significa que probablemente verá este tipo de cosas en más lugares. Y en la mayoría de las situaciones, debería sentirse cómodo probándolo.

Artículo traducido del inglés por "El Mercurio".