OUCH! Enero 2023

El Boletín Mensual de Concientización en Seguridad para ti

Biométricos - Haciendo la seguridad más simple

Resumen

¿Odias las contraseñas? ¿Estás cansado de iniciar sesión constantemente en sitios web nuevos o no puedes recordar todas tus contraseñas complejas? ¿Frustrado por tener que generar nuevas contraseñas para nuevas cuentas o tener que cambiar contraseñas antiguas para cuentas existentes? Tenemos buenas noticias para ti. Existe una solución llamada biometría que ayuda a facilitar la ciberseguridad. A continuación, explicamos qué son los datos biométricos, cómo simplifican tu vida y por qué comenzarás a ver más de ellos.

Primero, ¿por qué contraseñas?

Las contraseñas son una parte de algo llamado autenticación, el proceso de demostrar quién eres. Por lo general, han habido dos cosas que puedes proporcionar para demostrar tu identidad: algo que sabes (como sus contraseñas) y algo que tienes (como una tarjeta bancaria o tu celular). Tradicionalmente, la autenticación se ha realizado con contraseñas. Las contraseñas se adoptaron en un principio porque era una de las soluciones de autenticación más fáciles de implementar. Sin embargo, a lo largo de los años, nuestras vidas se han vuelto mucho más complicadas con muchas más cuentas de las que nadie esperaba. Es bastante común que una persona tenga más de 100 contraseñas en su vida laboral y personal.

Además, los ciberatacantes se han vuelto bastante buenos adivinando, robando o descifrando contraseñas. Es por eso que existen demasiadas reglas sobre las contraseñas, como hacerlas largas (para que sean difíciles de adivinar) y usar una contraseña única para cada cuenta (de modo que si una de tus cuentas es vulnerada, las otras aún están seguras). El problema con todos los requisitos para las contraseñas es que dificultan la ciberseguridad. Los gestores de contraseñas ayudan bastante, ya que recuerdan de forma segura todas tus contraseñas e inician sesión en sitios web por ti, pero ¿hay una mejor manera? Aquí es donde la biometría puede ayudar al proporcionar una tercera opción para demostrar tu identidad: algo que tú eres.

Datos biométricos

Al igual que las contraseñas, los datos biométricos son otra forma de demostrar quién eres. La diferencia es que en lugar de tener que recordar algo (como tus contraseñas), se usa un elemento de quién eres físicamente para probar tu identidad, como usar la huella digital para acceder a tu teléfono.

La biometría es mucho más simple ya que no tienes que recordar ni escribir nada, simplemente te autenticas utilizando quién eres. Existen diferentes tipos de datos biométricos, como tu voz, tu forma de caminar o los patrones únicos de tu iris. Sin embargo, las huellas digitales y el reconocimiento facial son los dos más comunes, especialmente para dispositivos móviles. Si bien la biometría tiene un gran número de ventajas, también tiene algunas desventajas, una de las más importantes es que si los ciberatacantes copian tu huella digital o tu rostro, no puedes cambiarlos.

Passkeys

En los próximos meses y años, deberías comenzar a ver que la biometría reemplaza a las contraseñas tradicionales con una nueva tecnología llamada Passkeys. Esta tecnología está siendo adoptada por Microsoft, Apple y Google y pronto verás que se adopta en más y más sitios web a lo largo del tiempo. Passkeys reemplaza a las contraseñas al permitirte demostrar quién eres simplemente usando datos biométricos combinados con tu dispositivo móvil. Cuando creas una cuenta en un sitio web (como Google o Apple), en lugar de crear una contraseña, registras tu dispositivo móvil. En el futuro, iniciarás sesión en ese sitio web autenticándote con tu dispositivo móvil utilizando datos biométricos, como la huella digital o reconocimiento facial. El sitio web confía en tu dispositivo móvil, y este confirma que eres tú quien usando datos biométricos. Además, tus datos biométricos (huella digital o rostro) no se envían a ningún sitio web. En vez de eso, tus datos biométricos se almacenan localmente de forma segura en tu dispositivo. Solo se usa para desbloquear la "Passkey", una clave única, creada para cada sitio, que tu dispositivo envía al sitio mientras protege tus datos biométricos. Si bien ninguna solución es perfecta, la biometría y las soluciones como Passkeys pueden ayudarte a mantenerte seguro y al mismo tiempo simplificar la seguridad.

Editor invitado

El Dr. Johannes Ullrich es Decano de Investigación en el Instituto Tecnológico SANS. Con más de 20 años de experiencia en la industria, monitorea las amenazas actuales al operar el SANS Internet Storm Center. Enseña SEC522 (Seguridad de aplicaciones web) y SEC503 (Detección de intrusos).
Twitter: @johullrich y LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Recursos

Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/
Más sobre Passkeys: https://www.sans.org/blog/what-is-phishing-resistant-mfa/

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT