LITORALPRESS

Fecha: 17-09-2024
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Noticia general
Título: ¿Llegó el fin de las contraseñas? autenticación biométrica sería el control más seguro para proteger datos personales

Pág. : 9
Cm2: 487,7

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

¿Llegó el fin de las contraseñas? autenticación biométrica sería el control más seguro para proteger datos personales

De acuerdo a un estudio de la compañía rusa de ciberseguridad Kaspersky, entre agosto de 2022 a agosto de 2023, Chile habría sufrido 27 ataques digitales por minuto. Ante esto, Javiera Lobos, gerente comercial y experta en prevención de fraude de Ionix Chile, explica que una de las soluciones que se vienen para el futuro, y que algunas empresas ya están implementando, son los factores de seguridad de inherencia.

"El Factor de Seguridad de Inherencia, también conocido como biometría, se basa en características físicas o de comportamiento únicas de una persona. Incluye desde las huellas dactilares y el reconocimiento facial y de voz, hasta el escaneo de iris o incluso patrones de escritura. A diferencia del factor de conocimiento, la biometría ofrece una forma muy segura y conveniente para verificar la identidad de una persona y minimizar los riesgos de sufrir la suplantación o filtración de sus datos", explicó la experta.

Por otro lado, la asociación gremial de empresas tecnológicas Chiletec realizó un informe que muestra que la cantidad de ciberataques ha aumentado en un 138% con respecto al año pasado. Por lo mismo, Zady Parra, subgerente operacional y seguridad de Zenta Group, explicó que la autenticación biométrica da una solución segura y robusta, ya que "no cuenta con vulneración de contraseña o clonación, como sí ocurre con las contraseñas. Los datos biométricos como reconocimiento facial o reconocimiento de voz se usan principalmente en aplicaciones financieras o bancarias, sin embargo, se está implementando en correos electrónicos y en otras aplicaciones".

Finalmente, Javiera Lobos, explicó diferentes tipos de factores de seguridad de inherencia:

- Huella dactilar

Es el uso de los patrones únicos de las huellas dactilares para autenticar a una persona, y se emplea por lo general en smartphones, sistemas de acceso físico y laptops. Su principal ventaja, como con otros aspectos biométricos, es su alta precisión y conveniencia.

- Reconocimiento facial

Como su nombre lo indica, es la identificación de una persona basada en la estructura y características de su rostro. Es usual en dispositivos móviles, sistema de seguridad y control de fronteras, por solo poner algunos ejemplos, y es elegido como factor de autenticación porque es conveniente, efectivo y no intrusivo.

● Según un informe de Chiletec, los ciberataques han aumentado en un 138% en Chile

- Reconocimiento de iris

Es el análisis de los patrones únicos en el iris del ojo y su uso común se da en instalaciones de alta seguridad y controles de acceso, sobre todo por su alta precisión y lo difícil que resulta su falsificación. No obstante, cabe destacar que requiere de hardware especializado, por lo que implica una gran inversión.

- Reconocimiento de voz

El reconocimiento de voz se da mediante la verificación de la identidad de una persona a través de sus patrones vocales únicos. Es muy usado, por ejemplo, en los servicios telefónicos de la banca. Si bien puede verse afectado por el ruido ambiental o los cambios en la voz del usuario, no requiere ingeniería demasiado especializada y es fácil de implementar. Patrón de escritura o tecleo Al momento de escribir en un teclado, todos tenemos un ritmo diferente. De eso se trata el patrón de escritura o tecleo, que analiza el ritmo de escritura al teclear. Si bien no es de mucho uso, sí es implementado en procesos de autenticación en sistemas de alta seguridad.