LA AUTENTICACIÓN DE DOS FACTORES (2FA)

La autenticación de dos factores (2FA) es un método de seguridad que agrega una capa adicional de protección a tus cuentas en línea, más allá de simplemente ingresar un nombre de usuario y contraseña. Esta medida de seguridad se utiliza para asegurarse de que solo la persona adecuada pueda acceder a una cuenta, incluso si alguien más conoce la contraseña.

El proceso de autenticación de dos factores generalmente implica dos o más de los siguientes elementos:

Algo que sabes: Esto generalmente incluye una contraseña o un código PIN que solo tú conoces.

Algo que tienes: Esto puede ser un dispositivo físico, como un teléfono móvil o una tarjeta de seguridad que solo tú posees.

Algo que eres: Esta categoría se refiere a características biométricas, como la huella digital o el escaneo facial.

Para utilizar la autenticación de dos factores, primero debes habilitarla en tu cuenta. Esto a menudo se hace a través de la configuración de seguridad de la cuenta. Una vez habilitada, el proceso de autenticación de dos factores puede llevarse a cabo de diferentes maneras:

Autenticación por SMS: Recibes un código de seguridad único en tu teléfono móvil a través de un mensaje de texto cuando intentas iniciar sesión. Debes ingresar este código junto con tu contraseña.

Aplicaciones de autenticación: Utilizas una aplicación de autenticación como Google Authenticator o Authy para generar códigos temporales que debes ingresar al iniciar sesión.

Correo electrónico de verificación: Recibes un correo electrónico con un código que debes ingresar para completar la autenticación.

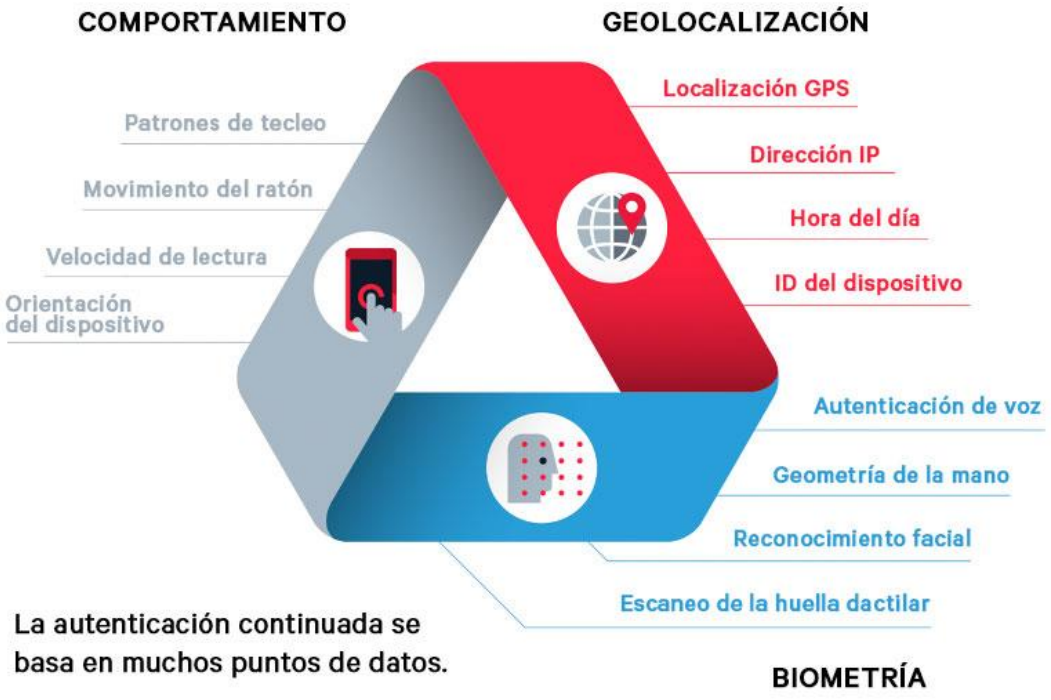
Llave de seguridad: Utilizas un dispositivo USB o NFC (Near Field Communication) para verificar tu identidad.

La autenticación de dos factores (o 2FA) requiere una contraseña (el primer factor), y un segundo factor, que puede ser un código numérico, una notificación de inserción, una pregunta de seguridad, un token de seguridad o una lectura biométrica (una huella digital o reconocimiento facial) que se lleva a cabo desde una aplicación de autenticación para acceder a datos en línea. También conocido como verificación en dos pasos o autenticación de doble factor, el proceso de autenticación 2FA valida ambos conjuntos de credenciales de usuario antes de dar acceso a una cuenta digital.

La mayoría de los procesos 2FA combinan dos de los cinco factores habituales de autenticación: conocimiento, posesión, herencia, ubicación y tiempo. Los factores de conocimiento son elementos que el usuario conoce, como una contraseña o un PIN, mientras que un factor de posesión es algo que el usuario posee, como su teléfono móvil o una determinada identificación. Otros factores utilizados son los de herencia, también conocidos como factores biométricos, que incluyen huellas dactilares, tono de voz u otros identificadores heredados como el reconocimiento facial. Si estás usando tu huella digital o el reconocimiento facial en tu dispositivo móvil, ya estás usando una autenticación biométrica.

Como sugiere el nombre, los factores de ubicación provienen de fuentes de datos como direcciones IP o software con GPS con información específica verificable sobre tu ubicación. Por último, aunque igualmente valiosos entre las herramientas 2FA, encontramos los factores de tiempo, donde la autenticación del usuario solo puede darse durante periodos fijos y queda prohibida fuera de ellos.

Es probable que los consumidores reconozcan los factores de conocimiento, posesión y herencia como los métodos 2FA más comunes a partir de la experiencia personal. Sin embargo, a pesar de los métodos 2FA resulten familiares, los usuarios de Internet siguen pareciendo menos preocupados por el robo de contraseñas que por la facilidad de acceso. Da la impresión de que poder abrir el correo electrónico o verificar el saldo bancario rápidamente es más importante que proteger sus cuentas digitales.



La autenticación continuada se basa en muchos puntos de datos.

Fuente: Javelin Strategy & Research, 2021

¿Es suficiente la autenticación 2FA?

Según el informe sobre investigaciones de filtración de datos (Data Breach Investigations) de Verizon de 2019, empresas de todos los sectores corren el riesgo de sufrir una filtración incluso con un proceso de autenticación adicional. «Independientemente del tipo o la cantidad de datos con los que trabaje su organización, siempre hay alguien que intentará robarlos». Los robos masivos de datos de Adobe, Anthem, eBay, Equifax, Home Depot, Hilton, Hyatt, JP Morgan Chase, LinkedIn, Marriott International, Sony Pictures, Target, Uber, la Oficina de Administración de Personal de EE. UU. o Yahoo demuestran que, si estás en Internet, tus datos personales son susceptibles de estar en peligro. Teniendo en cuenta que 2019 fue el peor año registrado en cuanto a filtraciones de datos, parece que no basta con la autenticación 2FA para proteger tu identidad virtual, cuenta bancaria o calificación crediticia.

Al tratarse de un proceso asequible y, generalmente, fácil de usar, la autenticación 2FA reduce posibles amenazas como el fraude de identidad sintética, el fraude de robo de cuentas, la piratería o el phishing. Aún así, como sucede en cualquier otro sistema, la autenticación 2FA solo es tan fuerte como su eslabón más débil.

La clave reside en hallar los dos factores adecuados

Los sistemas de autenticación de dos factores pueden ser vulnerables, a menos que utilices la combinación correcta de factores. Los métodos que se basan en tokens de seguridad dependen de la calidad del fabricante, mientras que los procesos que utilizan factores biométricos también requieren de un software fiable y seguro. Un proceso de autenticación de dos factores basado en factores de conocimiento, como el código de verificación único enviado al dispositivo móvil del usuario, es susceptible de sufrir ataques de ingeniería social. «Cualquier niño de 13 años puede descargar la herramienta disponible y llevar a cabo estos ataques», afirma Kevin Mitnick, uno de los hackers más buscados por el FBI en su momento. Y la investigación sugiere que aumentar la ciberseguridad a nivel de gerencia es una idea inteligente. En 2018, «los ejecutivos de nivel C tenían doce veces más probabilidades de sufrir incidentes sociales y nueve veces más probabilidades de sufrir filtraciones sociales que en años anteriores. Los incidentes de seguridad y las filtraciones de datos que afectaron a ejecutivos aumentaron de porcentajes de una sola cifra a decenas», según informa Verizon. Ningún sistema de seguridad es perfecto, los hackers pueden interceptar SMS con códigos 2FA con la misma eficacia con que descifran contraseñas débiles. Sin embargo, el uso de los dos factores correctos, como la verificación del documento de identidad en combinación con una verificación biométrica, garantiza un enfoque más estratificado y seguro.

La autenticación de dos factores es una práctica importante para aumentar la seguridad de tus cuentas en línea, ya que incluso si alguien más obtiene tu contraseña, no podrán acceder a tu cuenta sin el segundo factor de autenticación. Esto agrega una capa adicional de protección en caso de que tus credenciales sean comprometidas. Se recomienda encarecidamente habilitar la autenticación de dos factores en todas las cuentas que ofrecen esta opción, especialmente en servicios sensibles como el correo electrónico y la banca en línea.

a autenticación de dos factores (2FA) en Gmail es una medida importante para mejorar la seguridad de tu cuenta de correo electrónico. Aquí te indico los pasos para habilitarla:

Iniciar sesión en Gmail: Abre tu navegador web y ve a la página de inicio de Gmail (https://mail.google.com).

Inicia sesión en tu cuenta: Ingresa tu dirección de correo electrónico y contraseña para iniciar sesión en tu cuenta de Gmail si aún no lo has hecho.

Acceder a la configuración de seguridad:

Haz clic en tu foto de perfil en la esquina superior derecha y selecciona "Cuenta de Google".

En la página de "Cuenta de Google", selecciona "Seguridad" en el panel de la izquierda.

Habilitar la autenticación de dos factores:

Desplázate hacia abajo en la página de seguridad hasta que veas la sección "Iniciar sesión en Google" y busca "Verificación en dos pasos". Haz clic en "2 Pasos".

Verificación de identidad: Google te pedirá que vuelvas a ingresar tu contraseña para verificar tu identidad.

Configura la verificación en dos pasos:

A continuación, se te presentarán varias opciones para configurar la autenticación de dos factores. Puedes elegir entre recibir un mensaje de texto (SMS) con un código de verificación, usar una aplicación de autenticación o utilizar una llave de seguridad. Selecciona la opción que prefieras.

Configura tu método de autenticación: A continuación, sigue las instrucciones para configurar el método de autenticación que seleccionaste. Por ejemplo, si eliges la opción de SMS, deberás ingresar tu número de teléfono y recibirás un código de verificación en un mensaje de texto.

Verificación exitosa: Una vez que hayas configurado la autenticación de dos factores, Google te pedirá que ingreses un código de verificación cuando intentes iniciar sesión en tu cuenta. Dependiendo del método que hayas seleccionado, recibirás un código por SMS o desde tu aplicación de autenticación.

Finaliza la configuración: Sigue las instrucciones para finalizar la configuración de la autenticación de dos factores.

A partir de este momento, cada vez que inicies sesión en tu cuenta de Gmail, se te pedirá el código de verificación generado por tu método de autenticación de dos factores. Asegúrate

de guardar tus códigos de respaldo en un lugar seguro en caso de que pierdas el acceso a tu método principal de 2FA.

La autenticación de dos factores en Gmail es una medida de seguridad importante para proteger tu cuenta de correo electrónico contra accesos no autorizados, y te recomiendo habilitarla si aún no lo has hecho.