ENJOY SAFER TECHNOLOGY™

GUÍA DE

Doble autenticación

Introducción

La gran mayoría de los servicios y sistemas que utilizamos en el día a día requieren como único control de acceso un nombre de usuario y contraseña. En estos casos, la clave actúa como una llave digital que le permite a un usuario identificarse en el sistema para poder acceder a información sensible. De este modo, dicha contraseña protege los datos privados del acceso no autorizado por parte de terceros.

Sin embargo, el aumento de ataques informáticos sumado a las conductas inseguras de las personas, como las contraseñas débiles e iguales en varios servicios, hacen necesario utilizar otros métodos de autenticación más robustos. Por lo mismo, muchas empresas están implementando la doble autenticación.

Esta guía tiene como objetivo, explicar qué es la doble autenticación y el modo de activarla en algunos servicios públicos.

Índice

¿Qué es la doble autenticación?

Se trata de una metodología de autenticación que, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor, el cual podría ser un código de seguridad o un dato biométrico para que la autenticación sea exitosa.

Si tomamos como ejemplo un código de seguridad, este segundo factor de autenticación puede estar asociado con un dispositivo del usuario como un teléfono celular o token. Este último es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Luego, la persona debe ingresarlo para poder validarse en el sistema.

El siguiente esquema muestra el funcionamiento de la doble autenticación:

Factores de autenticación

Dicho en otras palabras, un sistema de doble autenticación es aquel que utiliza dos de los tres factores de comprobación para validar al usuario. Estos factores pueden ser:

- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.

Por motivos económicos y de factibilidad, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token para recibir código de seguridad) en detrimento del factor inherencia o sistemas de biometría.

Ataques informáticos que roban contraseñas

A continuación, se explican los cuatro tipos de amenazas informáticas que utilizan los cibercriminales para vulnerar contraseñas:

Fuerza bruta: software que utiliza un diccionario para descifrar contraseñas combinando distintos caracteres y palabras de forma aleatoria.

Phishing: falsificación de una entidad de confianza como bancos o redes sociales por parte de un ciber-criminal. De este modo, el atacante busca manipular a la víctima para que ingrese sus credenciales de acceso en un sitio fraudulento.

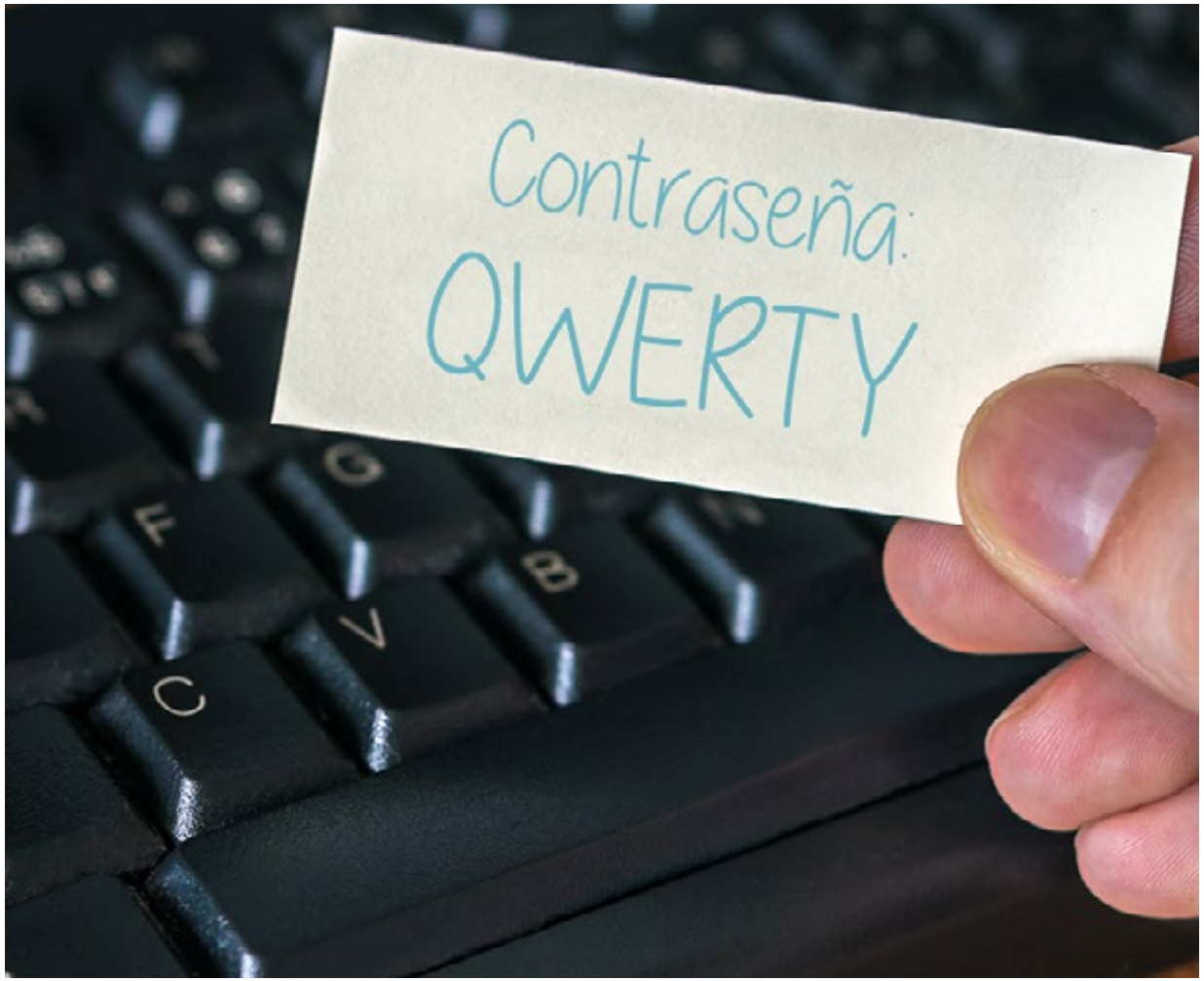
Malware: programa diseñado para realizar diversas acciones maliciosas, como el robo de contraseñas y credenciales de acceso.

Ataques a servidores: vulneración de un sistema informático utilizado para almacenar la base de datos de credenciales de acceso de un determinado servicio.

Conductas inseguras del usuario con las contraseñas

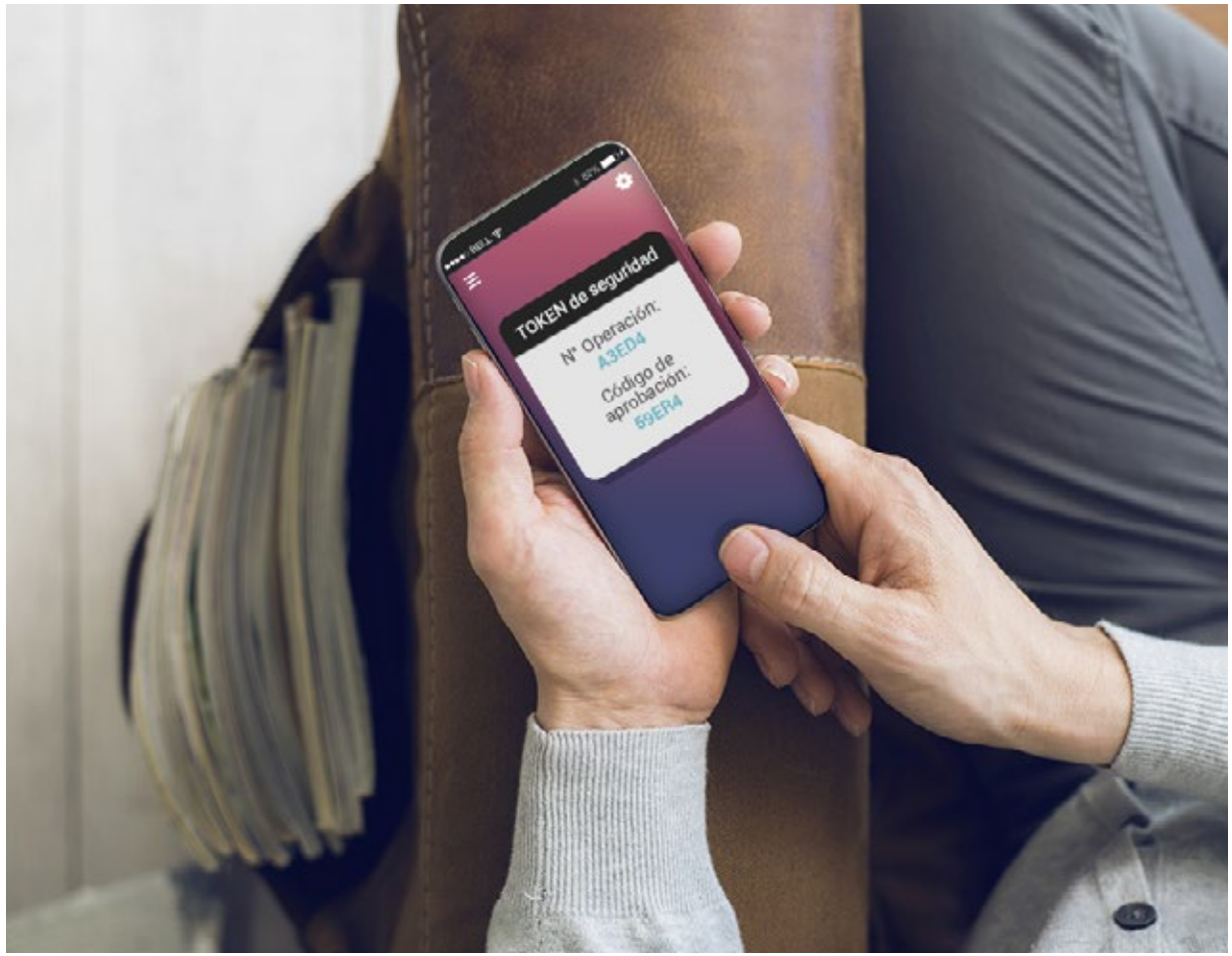
En conjunto con las amenazas explicadas anteriormente, una conducta insegura por parte del usuario también contribuye a que una contraseña pueda ser vulnerada. Para no favorecer incidentes es importante evitar:

- El uso de una clave única para varios servicios
- La elección de contraseñas fáciles de adivinar
- Guardarlas de manera escrita en documentos
- Que sea compartida



Doble autenticación y mitigación de ataques

Son diversas las amenazas y conductas que pueden contribuir a que un usuario se vea afectado por el robo de contraseñas, no obstante, la doble autenticación permite mitigar considerablemente tales casos. Por ejemplo, un cibercriminal podría robar una clave utilizando un código malicioso, y si bien dicha contraseña sería obtenida, el atacante no podría lograr el acceso al sistema debido a que desconocería el segundo factor de comprobación (autenticación), es decir, el código que se envía al teléfono o token del usuario.



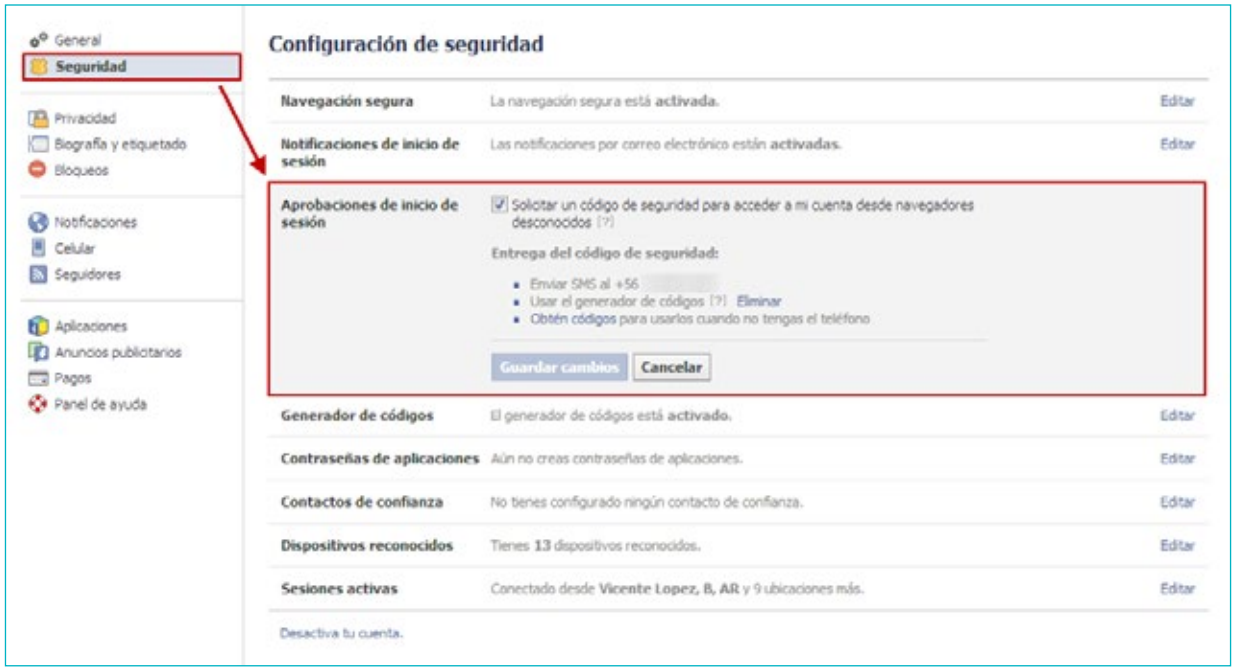
Doble autenticación en aplicaciones cotidianas

Muchos servicios que utilizamos a diario ofrecen la posibilidad de activar la doble autenticación de forma gratuita, ya que en los últimos años importantes empresas han sufrido diversos ataques que involucran el robo de contraseñas. Es importante destacar que este tipo de protección no está activada por defecto, por lo tanto, el usuario deberá modificar algunos parámetros para activarla. En las siguientes páginas se detallan las instrucciones necesarias para configurar este sistema de protección en Facebook, Twitter, LinkedIn, Google y Apple.

En Facebook

Para activar la doble autenticación en Facebook se debe seguir el siguiente procedimiento:

1) Hacer clic sobre el ícono en forma de rueda dentada ubicado en la parte superior derecha del sitio. Posteriormente hacer clic en "Configuración de la cuenta".
2) Luego hacer clic sobre la opción "Seguridad" que aparece en el costado izquierdo de la página.
3) Allí se debe activar la opción "Solicitar un código de seguridad para acceder a mi cuenta desde navegadores desconocidos" tal como aparece en la siguiente captura:

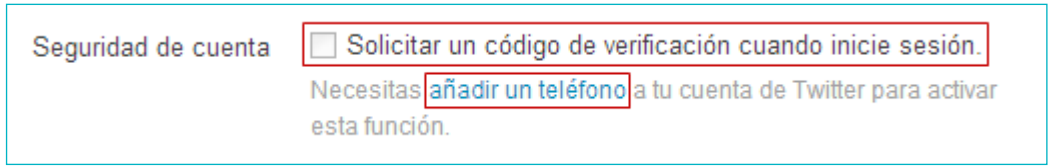


En el caso de Facebook, el segundo código de seguridad será solicitado cada vez que el usuario ingrese al servicio utilizando un dispositivo desconocido, es decir, un equipo que no ha sido utilizado anteriormente para acceder a la red social.

En Twitter

Para activar la doble autenticación en Twitter se debe seguir el siguiente procedimiento:

1) Hacer clic sobre el ícono en forma de rueda dentada ubicado en la parte superior derecha del sitio. Posteriormente hacer clic en "Configuración".
2) En la sección "Cuenta" activar la opción "Solicitar un código de verificación cuando inicie sesión". Esta opción aparece casi al final del sitio:



3) Para poder activar dicha opción el usuario deberá asociar un número de teléfono con la cuenta de Twitter. Esto puede realizarse haciendo clic en el enlace "añadir un teléfono".

En LinkedIn

Para activar la doble autenticación en LinkedIn se debe seguir el siguiente procedimiento:

1) Acceder al menú de configuración haciendo clic en el nombre del usuario que aparece en el costado superior derecho de la página. En el menú, hacer clic sobre "Configuración".
2) En la sección de configuración se debe acceder a la pestaña "Cuenta" y luego hacer clic en "Gestionar configuración de seguridad".
3) Luego activar la opción "Verificación en dos etapas para inicio de sesión":

En Google

Para activar la doble autenticación en los servicios de Google se debe seguir el siguiente procedimiento:

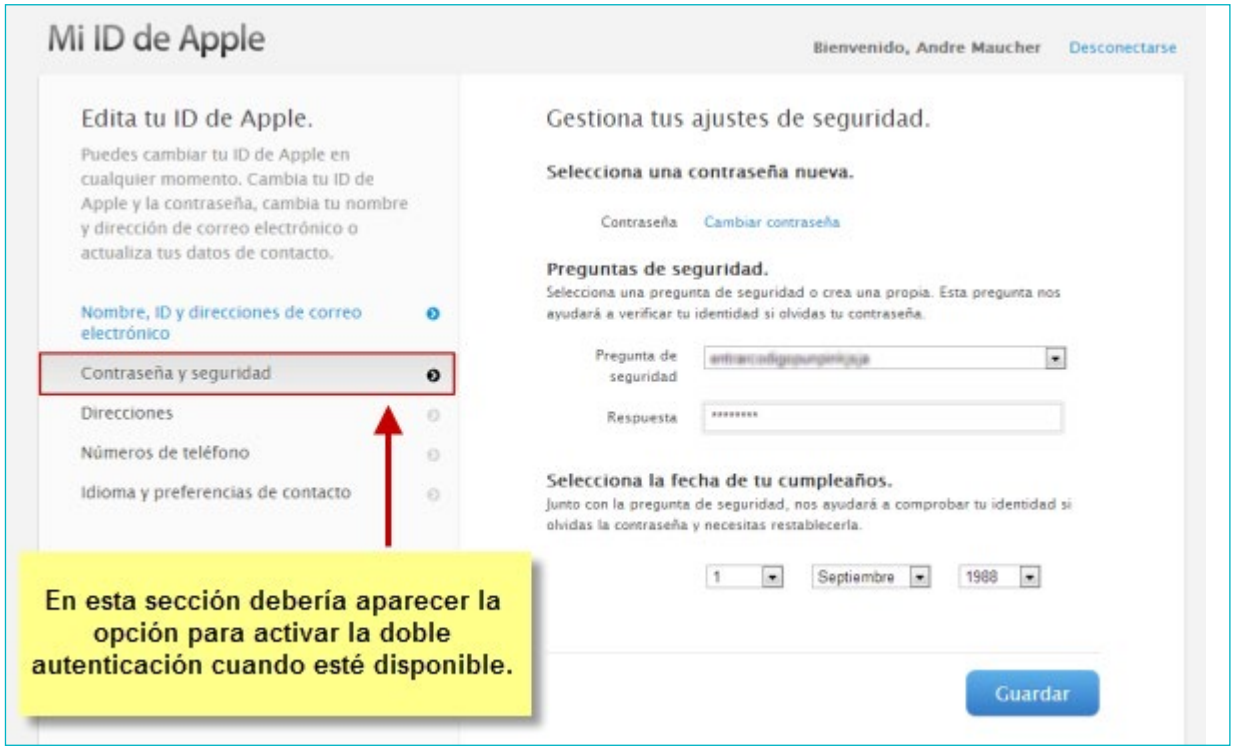
1) Ir al botón en forma de rueda dentada (ubicado en el costado superior derecho) y presionar sobre "Configuración".
2) Se debe hacer clic en la pestaña "Cuentas" y luego sobre el enlace "Otra configuración de la cuenta de Google":

3) Allí presionar sobre "Seguridad" y luego hacer clic en el botón "Configuración" o "Editar" que aparece en la sección Verificación en dos pasos que figura casi al final de la página:

En Apple

Para activar la doble autenticación en Apple se debe seguir este procedimiento:

1) Ingresar al portal Mi ID de Apple. Luego, presionar el botón "Gestionar tu ID de Apple" que aparece en la parte derecha del sitio.
2) Allí se deberá iniciar sesión utilizando las credenciales de acceso y presionando sobre el botón "Conectarse".
3) Una vez que el usuario se ha identificado en el sistema, se deberá hacer clic en "Contraseña y seguridad" tal como aparece en la siguiente imagen:



Nota: Apple está implementando la doble autenticación de forma gradual, por lo tanto, la disponibilidad de esta opción varía de acuerdo al país del usuario.

Doble autenticación en la empresa

La necesidad de utilizar un segundo factor de autenticación debe pensarse más allá de los servicios que se encuentran públicos. Para que una empresa garantice que la persona que está queriendo acceder a información clasificada es realmente quien dice ser, una alternativa es utilizar este tipo de soluciones de seguridad.

Los sistemas de doble factor de autenticación son más seguros que las contraseñas. Incluso si un atacante logra infectar un equipo y roba una credencial, el escalamiento de acceso no podrá ser logrado ya que no cuentan con el segundo código de acceso. Es importante recordar que los sistemas de doble factor son mejores que la contraseña por sí sola, pero no son infalibles.

Conclusión

A lo largo de esta guía quedó de manifiesto la importancia de contar con un método de autenticación robusto. En esta línea y conscientes de esta problemática, muchas empresas han implementado sistemas de doble autenticación. Si se considera que los usuarios utilizan cada vez más información sensible, resulta lógico que los cibercriminales destinen mayores recursos al robo de contraseñas. Desde el punto de vista técnico y de factibilidad, es posible mitigar este tipo de ataques, sin embargo, la participación del usuario en todo el proceso de protección es primordial para poder frenar un posible robo de contraseñas.

Varias empresas y bancos ofrecen sistemas de doble autenticación, no obstante, en la mayoría de los casos dicha opción se encuentra desactivada por defecto. Para solucionar este inconveniente es necesario que el usuario se concientice sobre la importancia de este método de protección y cómo configurarlo en los distintos servicios disponibles en Internet.

Vale la pena utilizar esta alternativa en aplicaciones de uso diario para mantener segura la información personal, y se hace imperativo aplicarlas cuando se trata de información laboral.

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica