SEON


# Una guía sobre cómo evitar el robo de identidad en internet

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

# Tabla de Contenidos

¿Tienes problemas para proteger tus cuentas de usuario? En esta guía, veremos por qué las cuentas son objeto de ataque, cómo las adquieren los defraudadores y, por supuesto, qué pasos debes tomar para protegerlas.

**Esta es tu guía completa para entender y prevenir los ataques de robo de identidad en internet.**

# ¿Qué es el robo de identidad en internet?

El robo de identidad en internet sucede cuando alguien ingresa a una cuenta que no le pertenece. En términos sencillos, se conoce usualmente como hackeo de cuenta.

Mark Zuckerberg, Elon Musk, Kim Kardashian, Jeff Bezos, Barack Obama, Jack Dorsey, Kanye West: todos ellos han sido víctimas de ataques de robo de identidad en internet.


# ¿Cómo funciona el robo de identidad en internet?

Existen muchos caminos para un robo de identidad en internet exitoso. Pueden suceder distintas cosas, dependiendo del vector de ataque:

**Oportunista:** un defraudador se topa con las credenciales de acceso de alguien. Esto puede ser accidental, o de forma más sofisticada, por ejemplo llevando a cabo una campaña masiva de suplantación de correos electrónicos. Puede deberse a una contraseña fácil de adivinar, la fuerza bruta o a través de malware como un keylogger.

**Credenciales compradas:** cualquier gran filtración de datos significa que seguramente habrá una proliferación de intentos de robo de identidad en internet debido a que las credenciales de acceso se venden en volumen a bajo costo en la darknet.

**Relleno de credenciales:** esto es cuando los defraudadores automatizan los ataques (usualmente con bots) utilizando credenciales de acceso que compraron de una base de datos filtrada.

**Explotación de vulnerabilidades de seguridad:** aquí es cuando se utilizan brechas de seguridad desactualizadas para obtener acceso no autorizado al sistema. Por ejemplo, el Cross-Site Scripting (XSS) y el Server Side Request Forgery (SSRF).

**Ataque dirigido:** los defraudadores usualmente abordan cuentas específicas que saben que son vulnerables. En las redes sociales y el gaming, por ejemplo, hay un enorme mercado para lo que se conoce como cuentas OG o cuentas con un identificador corto y extraño. Para abordar estas cuentas, los defraudadores se apoyan usualmente en técnicas de phishing (phishing dirigido) o ataques de duplicación de SIM.

# ¿Qué puedo hacer si fui víctima de robo de identidad en internet?

Si una cuenta fue comprometida, lo primero que hay que hacer es inhabilitarla. Esto evitará que el defraudador realice cualquier acción como cambiar la contraseña o realizar una compra.

Si la contraseña ya fue cambiada, deberías forzar un restablecimiento de contraseña e informar al usuario original. No olvides que los usuarios probablemente culparán a tu compañía por lo que ellos ven como una falta de seguridad. Debes tener un proceso sólido de comunicación diseñado para tranquilizarlos acerca de que se trata únicamente de una inhabilitación temporal y que su cuenta será restaurada tan pronto como sea posible.

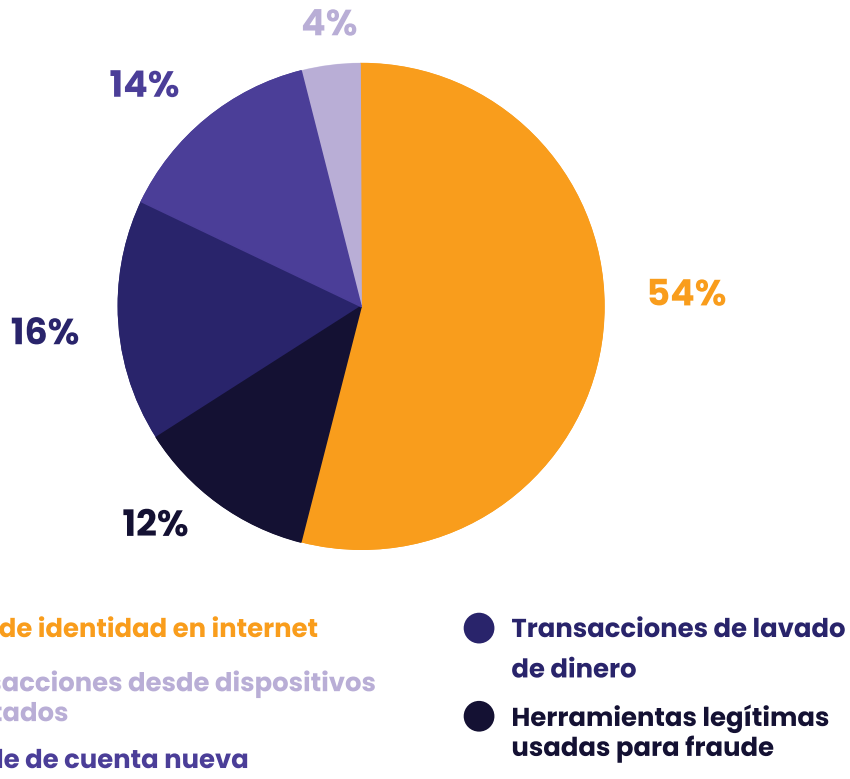
# ¿Cuánto le cuesta a los negocios el robo de identidad en internet?

De acuerdo a una investigación de Kaspersky, más de la mitad de los ataques fraudulentos son de robo de identidad.

Aunque es más difícil para los negocios poner valor monetario a las pérdidas por robo de identidad en internet que al fraude de tarjeta de crédito, por poner un ejemplo, esto no significa que sea un crimen sin víctimas. Existen consecuencias muy reales para los negocios afectados:

- **Los hackeos y los problemas de seguridad son una carga para tu equipo de TI**
- **Soporte técnico está abrumado por las solicitudes de los usuarios mientras intentan recobrar su cuenta**
- **El departamento financiero necesita lidiar con los contracargos**
- **Los usuarios se van con la competencia debido a una falta de reputación y confianza en la marca**

En el peor escenario, las acciones incluso pueden caer en picada después de que una filtración se haga pública. Según investigaciones de Bitglass, este desplome puede ser hasta de un 7.5%.



# 8 razones por las cuales sucede el robo de identidad en internet

Los defraudadores tienen numerosas razones para abordar a las cuentas preexistentes:

**Para adquirir más datos:** una vez que los hackers han ingresado en una cuenta, pueden recolectar más información. ¿Hay un número de teléfono asociado? Incluso mejor, ¿un número de tarjeta de crédito válido? Algunas veces, se trata de recolectar información personal de identificación (PII) para otras formas de fraude y robo de identidad. Este tipo de ataques suceden por lo general en el sector salud, el sector público o incluso en las instituciones académicas.

**Fraude financiero:** todos los robos de identidad en internet están diseñados para extraer valor monetario en algún punto. Entre más cerca esté una cuenta de una tarjeta de crédito, retirando fotos y enviando dinero, mejor para los defraudadores. Esto es cierto tanto para las divisas estándar como para las criptomonedas e incluso los puntos de lealtad o certificados de regalo.

**Fraude de moneda virtual:** algunas divisas son exclusivamente virtuales, como los objetos digitales en juegos que pueden revenderse para obtener ganancias en el mundo real.

**Abuso de promociones:** los defraudadores se basan en técnicas de cuentas múltiples para ganar la mayor cantidad de bonos de referido posible. Esto es incluso más fácil con las cuentas legítimas que han comprometido.

**Prueba de tarjetas:** ciertas cuentas son utilizadas únicamente para realizar pequeñas compras o probar tarjetas de crédito. Esto le ayuda a los defraudadores a verificar la validez de tarjetas de crédito robadas, que pueden utilizar después para sus compras compulsivas criminales.

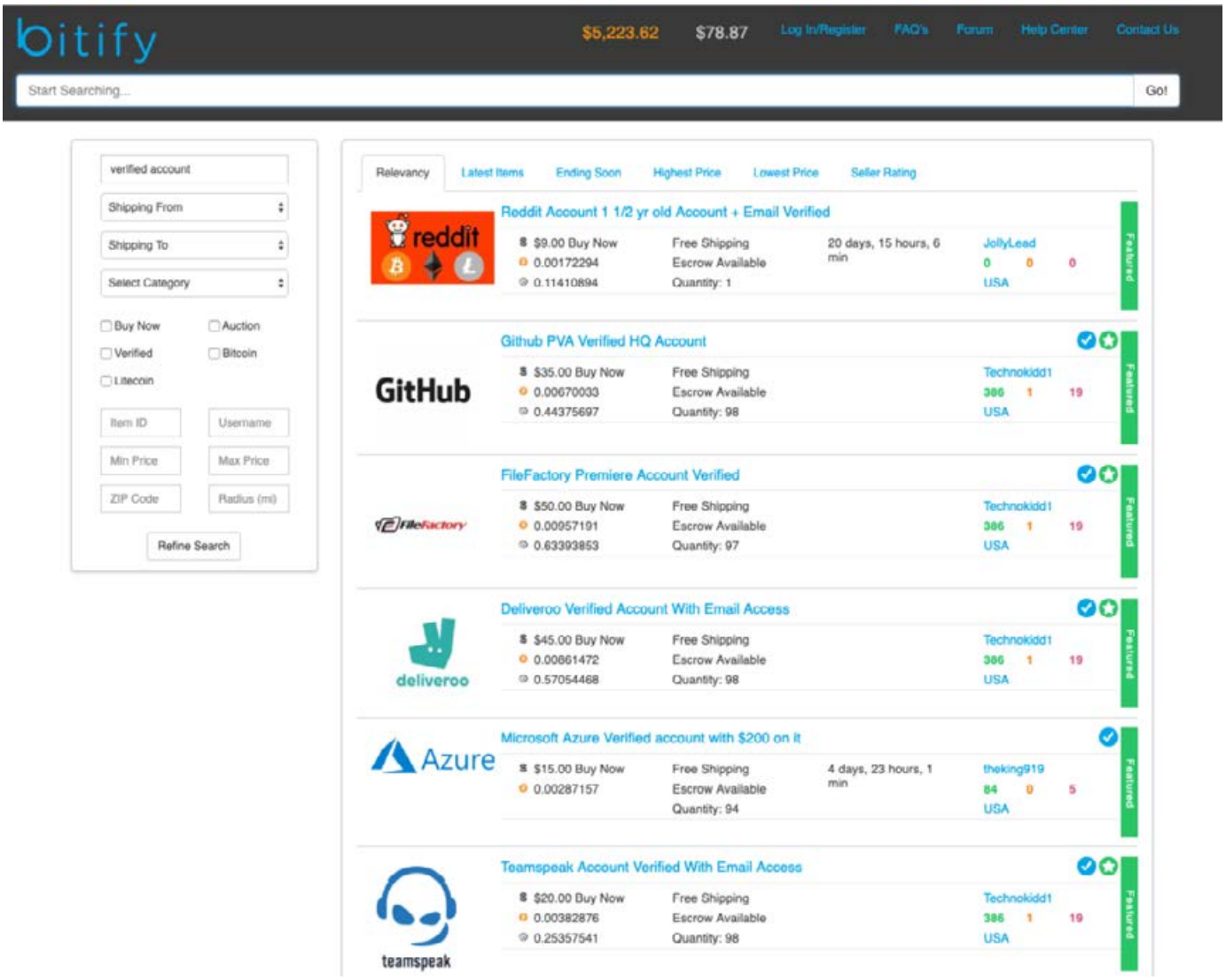
**Spam:** una cuenta legítima es una gran herramienta para crear listados falsos, vender bienes que no existen, escribir reseñas y calificar servicios propios.

**Suplantación de identidad:** los atacantes acceden a los contactos de la cuenta y los hacen su objetivo directo. La cuenta inicial les otorga legitimidad y hace a los contactos más susceptibles a revelar información valiosa.

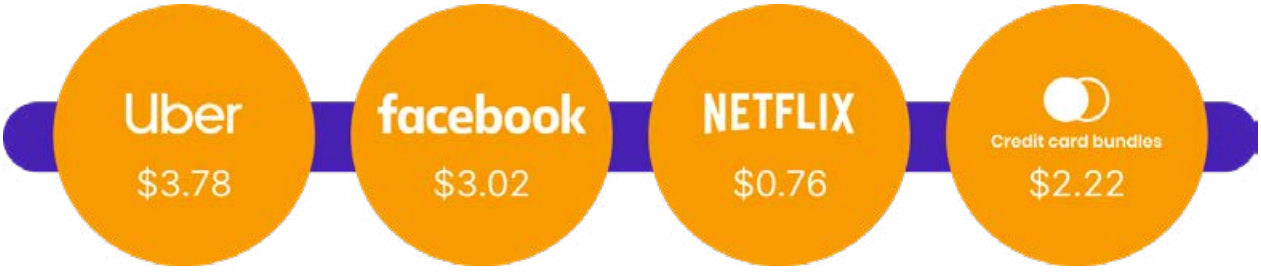
**Chantajes:** si una cuenta es extremadamente valiosa, los criminales pueden tratar de devolverla por un precio.

Finalmente, existe un enorme problema de **reventa de cuentas:** los actores maliciosos agrupan numerosas credenciales de acceso y las revenden en mercados criminales.

***Es por ello que, a largo plazo, el robo de identidad en internet es uno de los tipos de fraude más dañinos. El robo de identidad en internet alimenta los mercados de fraude, lo que conduce a más robos de identidad en internet.***




Ejemplos de cuentas completas disponibles en un sitio de la clearnet




Valor de una cuenta de diferentes proveedores en el Darkmarket - Fuente: TrendMicro

# 6 escenarios para los fraudes de robo de identidad en internet

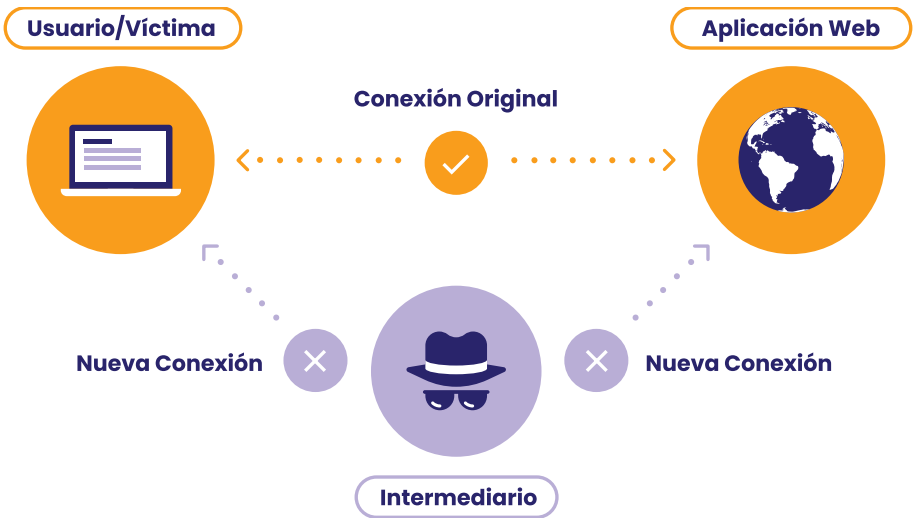
Existen muchas opciones para aquellos criminales que quieran adquirir cuentas de usuario. Algunos de los métodos más comunes incluyen:

**ataque de llenado de credenciales:** esto es cuando un defraudador intenta todas las combinaciones de direcciones de correo y contraseñas que ha encontrado en un gran vertedero de información;

**robo de identidad por suplantación:** los criminales envían un mensaje de texto o correo electrónico solicitando que ingreses al clon de un sitio conocido;

**ataques de ingeniería social:** los defraudadores contactan gente en persona e intentan extraer información de acceso. Esto no solo funciona en usuarios finales sino también en empleados y ejecutivos de negocio;

**ataque de intermediario (MITM):** esto es donde los defraudadores interceptan los datos entre tu sitio y los usuarios finales. Es el equivalente digital de escuchar a escondidas una conversación utilizando técnicas como el SSL stripping o los ataques de gemelo malvado, que imitan puntos de acceso WiFi para capturar datos;




**duplicación de SIM:** la mayoría de las cuentas de nombres de alto perfil al principio de esta guía fueron robadas utilizando ataques de duplicación de SIM. Esto sucede cuando los defraudadores contactan a operadores de telecomunicaciones y logran tomar el control de un número de teléfono móvil. Ya que muchas cuentas se verifican a través de autenticación en dos pasos (2FA), obtener acceso al número significa que puedes ingresar al Instragram, Twitter y una gran variedad de otros servicios potenciales de una persona.

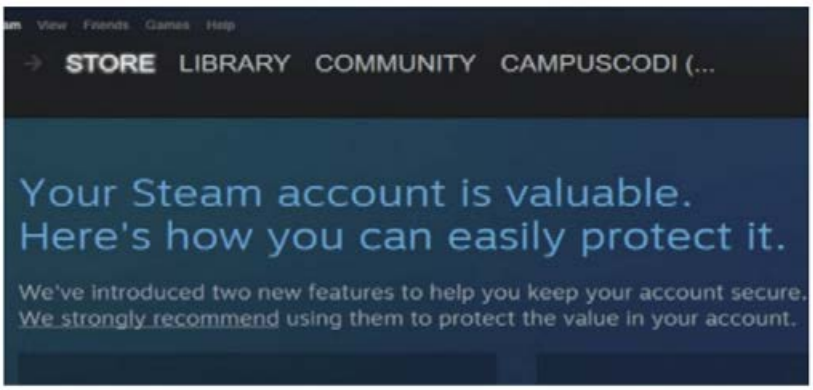
**XSS para robo de identidad:** XSS quiere decir Cross-Site Scripting. Permite a los criminales abordar un sitio web ejecutando scripts maliciosos en el navegador de la víctima. Usualmente, esto es con el objetivo de establecer nuevas contraseñas en cuentas preexistentes.

# Cómo protegerte del fraude por robo de identidad

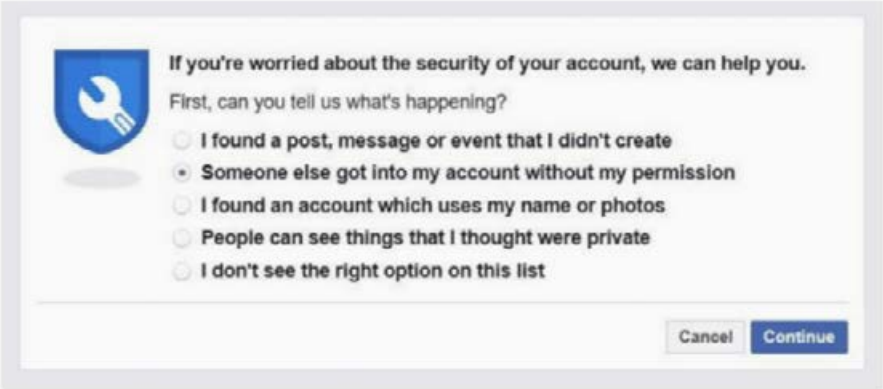
Informar a tus usuarios y empleados acerca de lo valiosas que son sus cuentas es un buen primer paso para hacerle la vida difícil a los defraudadores ya que esto hará que cambien su comportamiento con respecto a la protección de sus cuentas.

El sentido común ayuda, pero también deberías hacer un esfuerzo coordinado para recordarle a la gente que:

- **deje de reutilizar contraseñas:** perder una cuenta puede tener varias consecuencias negativas. Perder todas tus contraseñas online puede ser desastroso;
- **actualice sus contraseñas regularmente:** esto puede proteger las cuentas de filtraciones de datos históricos. Puedes comprobar si tus datos han sido filtrados, por ejemplo utilizando el sitio web Have I Been Pwned para direcciones de correo electrónico y asegurarte de que tus contraseñas se actualicen rápidamente después de una filtración mayor;
- **utilice administradores de contraseñas:** estos generan contraseñas seguras, las almacenan a salvo y las autocompletan en sitios web y aplicaciones cuando es necesario;
- **tenga cuidado con los enlaces:** especialmente desde remitentes de correo electrónico desconocidos, texto pobremente escrito o páginas de internet sospechosas. Siempre es mejor acceder a sitios importantes a través de tu navegador en lugar de seguir cualquier enlace;
- **verifique URLs:** permanece alerta de las señales de intento de phishing si un URL o sitio web parece inusual, especialmente al ingresar credenciales o información personal, por ejemplo: www.paypall.com
- **habilite MFA (autenticación multifactor):** la verificación en dos pasos (2SV) o la autenticación de dos factores (2FA) son más fáciles de usar que nunca gracias a aplicaciones de terceros como Google Authenticator;
- **utilice un VPN:** especialmente al estar conectado a redes WiFi públicas.



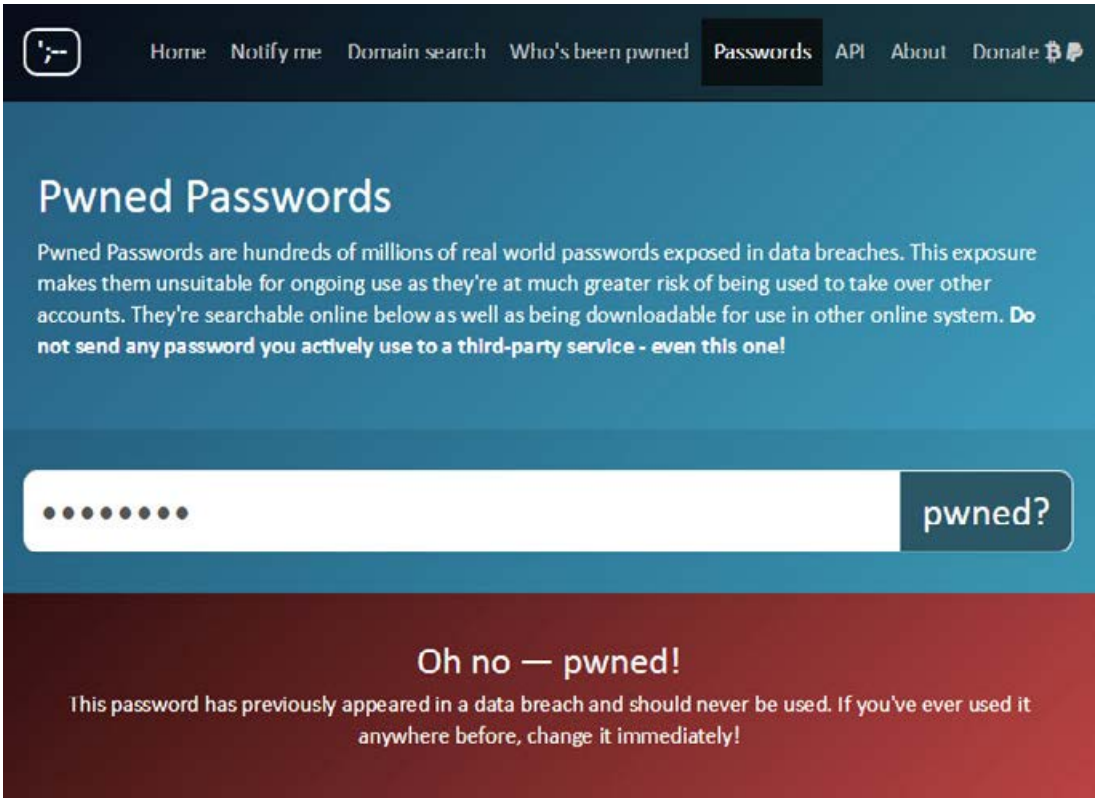

*Cómo el mercado de videojuegos STEAM incentiva el uso de 2FA*




*La característica de reporte de robo de identidad de Facebook*

También deberías ser transparente con tus usuarios acerca de los riesgos del robo de identidad en internet, y comunicarte con ellos regularmente acerca de cambios que puedan afectar sus cuentas.

Por ejemplo, esto podría ser a través de un correo electrónico informándoles que un nuevo número de teléfono ha sido registrado o confirmar su conversación reciente con un representante de servicio al cliente.




Puedes comprobar si tu contraseña(s) ha sido expuesta en el sitio web Have I Been Pwned

# Cómo mejorar tu seguridad contra el fraude por robo de identidad en internet

Como negocio, lo mejor es asegurarte de que se siguen las mejores prácticas de protección de datos. Esto debería ser cierto para todos los datos que son recolectados, transferidos, procesados y accedidos. Una lista no exhaustiva de ejemplos incluye:

**usar SSL:** especialmente en páginas que recaban información personal o sensible como tarjetas de crédito, números de seguridad social o direcciones;

**usar encriptación cuando sea posible:** no únicamente para los inicios de sesión, sino también para las comunicaciones;

**asegurar dispositivos físicos:** esto es particularmente importante para las compañías de teléfonos, laptops y computadoras de escritorio, especialmente en una configuración de trabajo desde casa;

**contratar hackers éticos o de sombrero blanco:** por ejemplo, Facebook tiene recompensas por bugs en las que premian a investigadores independientes hasta por $40,000 por encontrar vulnerabilidades que pudieran resultar en robo de identidad;

**verificar las contraseñas de usuario:** puedes utilizar servicios de terceros para verificar si las credenciales de un usuario han sido filtradas anteriormente, por ejemplo Troy Hunt's Pwned Passwords2 o K-Anonymity si eres un cliente de Cloudflare. Esto es útil para alertar a tus usuarios al registrarse si están a punto de utilizar una contraseña filtrada o para disparar una verificación de correo electrónico al iniciar sesión para asegurarse de que no son víctimas de robo de identidad;

**restringir la entrada del usuario:** esto incluye limitar la entrada de HTML, sanitizar los valores ingresados y el uso de listas de elementos permitidos para asegurarse de que el código de tu sitio está limpio y no es vulnerable a ataques de inyección SQL o HTML.

## Considera la fricción de usuario:

En un mundo ideal, serías capaz de establecer tantos pasos de verificación y autenticación como necesites para asegurarte de que tus usuarios son quienes dicen ser.

Sin embargo, en la práctica estos pasos son serios obstáculos en la trayectoria de tu cliente y pueden proporcionar una mala experiencia de usuario. Añadir más fricción, ya sea al registrarse o al iniciar sesión, es la forma más segura de enviar a los usuarios hacia competidores más permisivos, especialmente en la economía actual de “siempre conectado”.

Entonces, ¿cómo balanceas el nivel adecuado de seguridad con la baja fricción de usuario? **Desplegando herramientas invisibles de autenticación.**

# Software de detección de fraude para el robo de identidad

Un desafío clave de detectar los inicios de sesión sospechosos es que a menudo los datos son limitados. En la prevención de fraude, entre más puntos de datos tengas, más precisas pueden ser tus decisiones. Al momento de iniciar sesión, usualmente tenemos una dirección IP, información del dispositivo y el comportamiento básico del cliente.

Sin embargo, un solo punto de información puede ser suficiente para colocar en la lista negra intentos de inicio de sesión, siempre y cuando los datos sean enriquecidos en tiempo real para confirmar su validez.

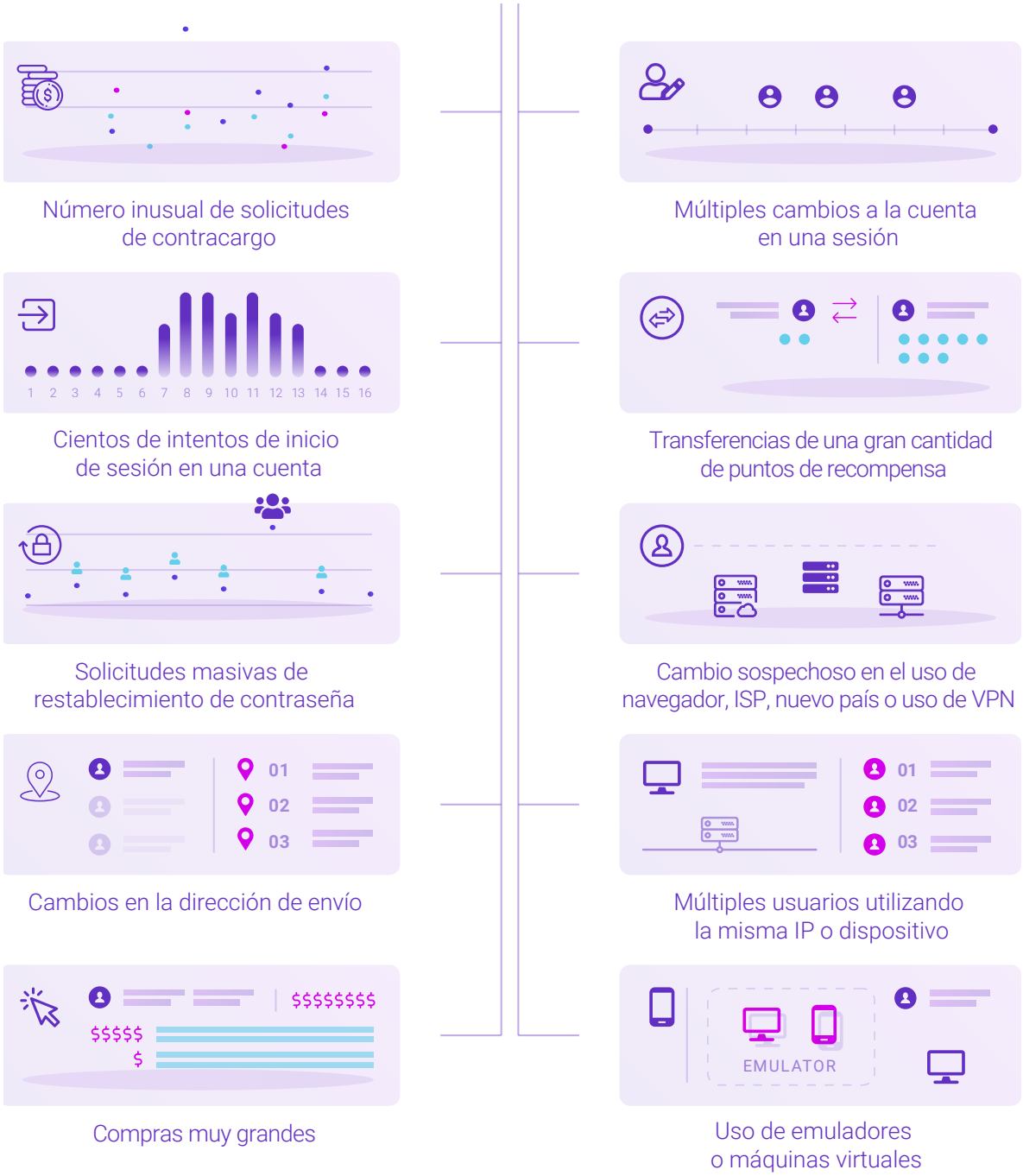
**Huella digital del dispositivo:** se puede crear un hash o identificación de dispositivo utilizando los datos de un navegador, sistema operativo, dispositivo y red para alertar sobre conexiones sospechosas. Esto es algo que no requiere cálculos excesivos, y aún así puede ser muy efectivo para prevenir que los usuarios inicien sesión desde dispositivos o navegadores desconocidos. También puede detectar el uso de máquinas virtuales o emuladores sospechosos que los defraudadores usan a menudo para realizar múltiples solicitudes desde una misma computadora.

**Análisis de IP:** este es un método clásico de prevención de fraude que puede ser enriquecido para revelar proxies VPN sospechosos o el uso de TOR.

Registrar los datos obtenidos puede ser útil para la creación de listas blancas para tus usuarios y reducir los falsos positivos. Por ejemplo, si un usuario pudo avisar con anticipación que estará de viaje, puede reflejarse en la inclusión de su dirección IP en una lista blanca.

Puedes aprender más acerca de la huella digital en internet aquí.

## Prevén el fraude por robo de identidad con análisis de comportamiento con reglas de velocidad




Si un robo de identidad está en progreso, tu única oportunidad es identificar un comportamiento de usuario sospechoso. Ya sea inspeccionado a través de un sistema dedicado de prevención de fraude o a través de investigación manual, aquí hay algunas señales de que un ataque de robo de identidad en internet pudo haber ocurrido.

Es esencial establecer reglas que te permitan entender lo que se considera como un comportamiento seguro y lo que debería emitir señales de alerta.

## Fricción Dinámica

A pesar de tus mejores esfuerzos por desplegar capas de seguridad invisibles, habrá momentos en los que las áreas grises puedan confundir a cualquier sistema que tengas instalado.

En estas circunstancias no deberías dudar en desplegar tu arsenal y utilizar métodos de autenticación más rigurosos. Estos incluyen:

- **Identificación por selfie**
- **Mensaje de voz**
- **2FA**

Sin embargo, como ya mencionamos, estas herramientas de alta fricción únicamente deberían utilizarse como último recurso. Es mucho más fácil ofrecer una experiencia de autenticación fluida si tus herramientas de prevención de fraude te permiten controlar los límites entre lo que es aceptable y lo que requiere mayor investigación.


En SEON, por ejemplo, permitimos que los gerentes de fraude ajusten los límites de sus puntajes de riesgo, para que ellos permitan o rechacen inicios de sesión con base en el apetito de riesgo de la compañía.

# Cómo funciona la protección de robo de identidad con SEON

En SEON hemos desarrollado numerosas características de prevención del robo de identidad en el núcleo de nuestra plataforma de detección de fraude de extremo a extremo. También procuramos poner la experiencia de usuario en primer plano, reduciendo el tiempo de procesamiento al mínimo mientras te permitimos aprovechar:

**poderosa huella del dispositivo:** saber instantáneamente cuando un usuario se conecta con una combinación de software y hardware sospechosa;

**machine learning whitebox:** el algoritmo de SEON aprende de tus patrones de robo de identidad y se readapta varias veces al día. Obtienes resultados en forma de reglas legibles que puedes utilizar para probar tus datos de inicio de sesión para identificar las tasas de falsos positivos;

**reglas de velocidad:** recoge y evalúa toda la actividad de usuario en tu sitio a través de llamadas API personalizadas que se relacionan con cualquier punto de datos que desees enviar. Es lo más parecido al análisis del comportamiento para ayudarte a entender precisamente cuando alguien está actuando sospechosamente.

**La buena noticia es que puedes proteger cuentas de usuario individuales y tus intereses generales de negocios utilizando las mismas herramientas. Usar la flexibilidad y las opciones de personalización provistas tanto por las reglas de riesgo de SEON como por nuestras llamadas API le da a tu negocio el nivel de protección de fraude que necesitas.**

# Preguntas frecuentes

## ¿Qué puedo hacer si he sido perjudicado por el fraude de robo de identidad?

La acción inmediata es bloquear cualquier movimiento que sea posible desde esa cuenta. Si es realizar pagos, deberías inhabilitar tus tarjetas. Si es enviar mensajes a parientes, deberías avisarles que podrían recibir mensajes de phishing.

Para recuperar tu cuenta, deberías contactar a la compañía tan pronto como sea posible e informarle lo que sucedió.

## ¿Dónde encuentran los defraudadores los detalles para el robo de cuentas?

Los criminales tienen acceso a un número cada vez mayor de mercados para comprar, vender o intercambiar detalles de cuentas.

Mientras que la dark web es famosa por proporcionar anonimidad, ahora es cada vez más fácil comprar cuentas en sitios de subastas con criptomonedas en la clearnet o incluso en grupos de Telegram, donde puede ocurrir el fraude de criptomonedas.

## ¿Cómo evitas que los defraudadores encuentren credenciales para el robo de identidad?

Tristemente, a pesar de los mejores esfuerzos en ciberseguridad, organizaciones de todos tamaños siguen perdiendo millones de expedientes de usuario; una señal de que no puedes confiar en la seguridad estándar de tecnologías de la información para proteger tus cuentas.

Aún así, hay algunos pasos clave que deberías seguir:

- educar a los usuarios acerca del valor de sus cuentas;
- reforzar la seguridad de la fase de autenticación con software de prevención de fraude;
- habilitar 2FA, OTP u otras formas de autenticación multifactor.

SEON

**Para ver cómo SEON puede ayudar a su empresa a prepararse para el futuro, visite seon.io**

**O programe ahora una llamada de presentación de productos personalizada.**

Visite nuestro sitio web

Programe una llamada

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900