¿ES EL ROBO DE IDENTIDAD EL CIBERDELITO AL QUE MÁS LE TEMEMOS?

Un detallado análisis de las opiniones de los usuarios sobre el robo de identidad y diversos delitos cibernéticos

F-Secure

CONTENIDOS

INTRODUCCIÓN

¿Ha tenido usted alguna vez la sensación como si hubiera una filtración de datos a diario?

Esto podría deberse a que estadísticamente la hay.

Entre enero del 2005 y octubre del 2019 la cámara de compensación de derechos de privacidad registró 9.705 filtraciones de datos .[1] Eso es un promedio de 1,8 al día.

Por supuesto que la prensa no cubre cada uno de los casos de robo o divulgación de datos privados. Pero los ejemplos que aparecen en los titulares y que afectan a millones de usuarios, son cada vez más numerosos y abarcan ya todos los ámbitos de la economía.

El caso que hizo "despertar" a muchos consumidores frente a los peligros derivados de nuestras vidas digitales involucró a Equifax, una de las empresas de informes de crédito más grandes del mundo. En el 2017 cerca de la mitad de la población de los Estados Unidos - aproximadamente 150 millones - se enteró de que sus datos habían sido interceptados. El hecho dio lugar a un acuerdo con las entidades reguladoras, lo que podría costarle a la empresa 700 millones de dólares.[2]

Al año siguiente, la cadena de hoteles Marriot reveló haber sido víctima de una filtración de datos que afectó a casi 400 millones de clientes. En la ocasión se habrían divulgado informaciones de pago, nombres, direcciones postales, números de teléfono, direcciones de email y números de pasaporte.[3]

Antes de que terminara el primer mes de 2019, se supo que se había producido una de los mayores robos de datos en todo el mundo. El experto en seguridad cibernética Troy Hunt subió 773 millones de combinaciones de correos electrónicos y claves a su sitio web Have I Been Pwned.[4]

Es más, sólo en los últimos doce meses, un hacker obtuvo acceso a cerca de 100 millones de aplicaciones y cuentas de tarjetas de crédito de Capital One,[5] Facebook sufrió también diversas transgresiones,[6] y 2 millones y medio de víctimas de desastres naturales vieron su información privada expuesta, debido a una filtración en la agencia federal de manejo de emergencias de Estados Unidos.[7]

A comienzos de este año, Microsoft se ocupaba de una "enorme laguna de seguridad" que dejaba los historiales de servicio y asistencia de unos 250 millones de clientes a la vista de cualquier persona con acceso al internet.[8]

¿Qué hacen los hackers cuando tienen el control sobre nuestros datos?

Todo lo que pueden, desde robar nuestras claves hasta acceder a nuestras cuentas más delicadas o apoderarse de nuestras identidades.

---

1 Privacy Rights Clearinghouse: Data Breaches https://privacyrights.org/data-breaches
2 Equifax Breach Affected 147 Million, but Most Sit Out Settlement https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html
3 Marriott CEO Reveals New Details About Mega Breach https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/
4 ';--have i been pwned? https://haveibeenpwned.com
5 A hacker gained access to 100 million Capital One credit card applications and accounts https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
6 Unsecured Facebook Databases Leak Data Of 419 Million Users https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers
7 Hack Brief: FEMA Leaked the Data of 2.3 Million Disaster Survivors https://www.wired.com/story/fema-leaked-the-data-2-million-disaster-survivors/
8 Microsoft accidently exposed 250 million customer service records https://finance.yahoo.com/news/2020-01-22-microsoft-database-exposure.html

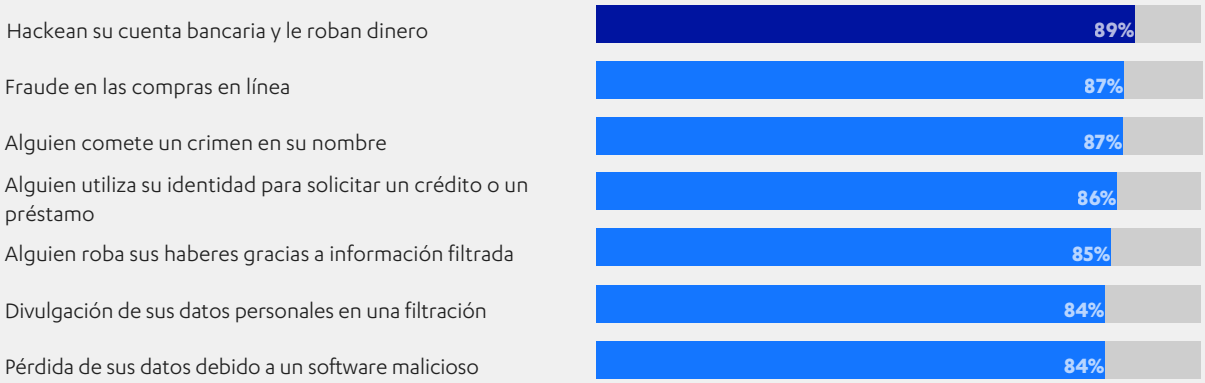
LOS RIESGOS

El usuario promedio de la web tiene docenas de claves de acceso a cuentas online y aún más con información personal que puede ser vinculada a tarjetas de crédito y a otros servicios. Resulta sorprendente que ocho de cada diez consumidores reutilicen las claves en diversos sitios, comportamiento que eleva significativamente el riesgo ser hackeados.[9]

La idea de que nuestros datos podrían ser utilizados para atentar en contra de nuestra identidad existe, posiblemente porque los usuarios entienden que no es posible asegurar nuestra información en todos los lugares donde se almacena.

Una encuesta de F-Secure realizada en nueve países reveló que nueve de cada diez usuarios están al menos algo preocupados por los diversos riesgos en el internet, al estar nuestros dispositivos conectados y nuestras cuentas y datos no debidamente protegidos.

¿QUÉ TAN PREOCUPADO ESTÁ RESPECTO A LOS SIGUIENTES PELIGROS ONLINE?

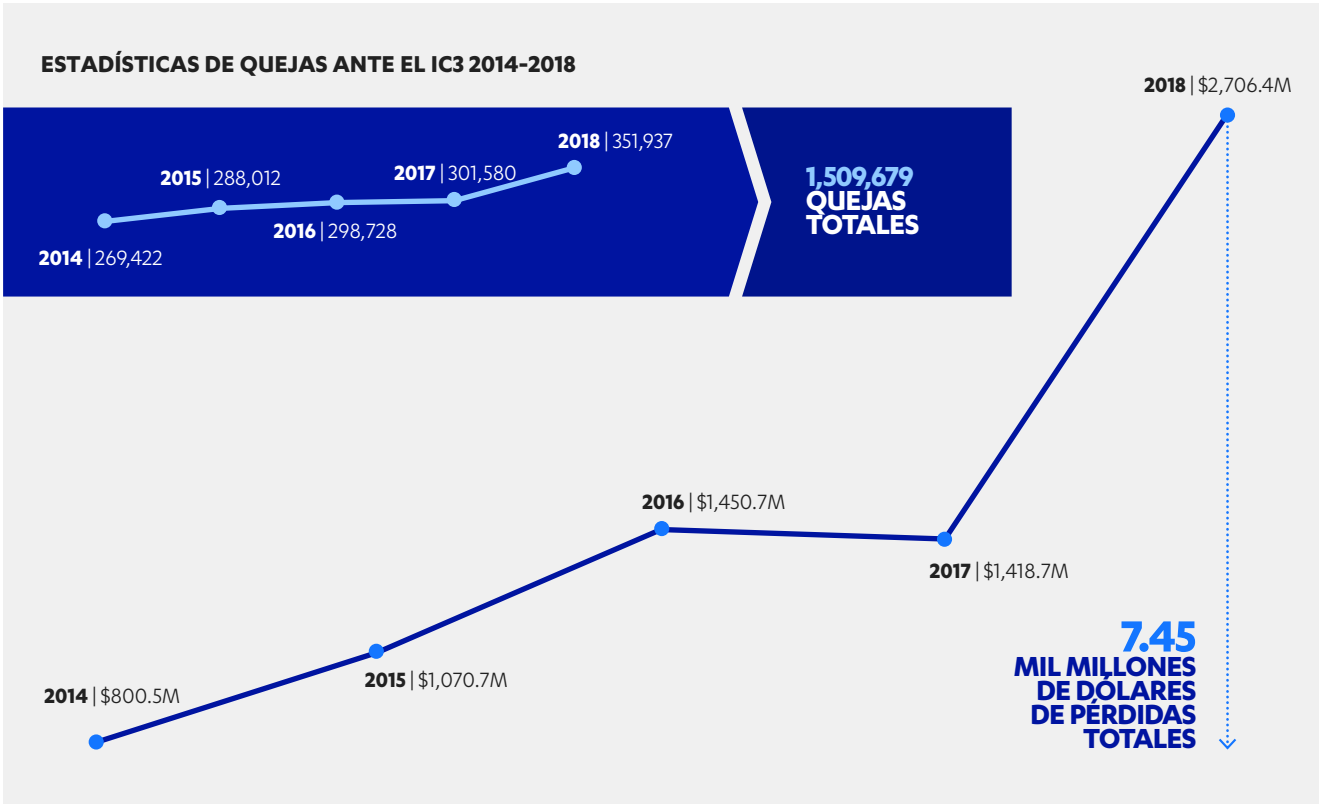


Incluso si las víctimas de los ciberataques aseguraran todos sus datos empleando todos los recursos a su disposición, éstos seguirían siendo vulnerables frente a las diversas técnicas que los hackers utilizan para sacar provecho a la información. Por ejemplo, el uso de información privada para recibir atención médica, para evitar la aplicación de la ley en ciertos casos y para crear cuentas falsas y hacer compras o solicitar préstamos.

Los resultados de nuestra encuesta indican que los usuarios comprenden el riesgo que corren al abrir las docenas o cientos de cuentas, no sólo por el hecho de usar la web, sino también para obtener servicios básicos del gobierno y tarjetas de crédito.

Anualmente, el número de crímenes cibernéticos reportados al centro de denuncias de delitos de internet (IC3) aumenta tanto en número como en impacto económico.[10]

9 Poll: Americans leave their personal info open to thieves https://www.creditcards.com/credit-card-news/data-security-poll.php
10 Internet Crime Complaint Center (IC3) 2018 Internet Crime Report https://pdf.ic3.gov/2018_IC3Report.pdf



Los crímenes más costosos reportados involucran casi todos fraude, estafas o abuso de datos personales.

Mientras que el robo de identidad en sí es clasificado como el quinto delito más caro con pérdidas de más de 100 millones de dólares, muchos de los crímenes que ocasionan las mayores pérdidas - el fraude de correo electrónico comercial (BEC) o el de cuentas de correo electrónico (EAC) hasta la filtración de datos personales y corporativos y el fraude de tarjetas de crédito - implican facetas de lo que muchos de nosotros conocemos como robo de identidad.

PÉRDIDAS POR ROBO DE IDENTIDAD

Tipo de crimen	Pérdida (USD)
BEC/EAC	$1,297,803,489
Fraude de Confianza/Romance	$362,500,761
Inversión	$252,955,320
Falta de pago/no entrega	$183,826,809
Bienes raíces/arriendo	$149,458,114
Filtración de datos personales	$148,892,403
Filtración de datos corporativos	$117,711,989
Robo de identidad	$100,429,691
Cuota por adelantado	$92,271,682
Fraude con tarjetas de crédito	$88,991,436
Extorsión	$83,357,901
Falsificación	$70,000,248
Suplantación (del gobierno)	$64,211,765

IDENTITY THEFT MAKES CYBER CRIME REAL

El robo de identidad se define generalmente como la recopilación de información confidencial de una persona para hacerse pasar por ella o acceder a sus datos o archivos personales, con el fin de obtener un beneficio económico. El robo de identidad puede derivar tanto en delitos en línea como en el mundo análogo. La base de datos de Consumer Sentinel Network, a cargo de la comisión federal de comercio de Estados Unidos, reportó 444.602 denuncias de robo de identidad en el 2018, más de 167.000 de ellas provenían de "personas que afirmaban que sus datos fueron utilizados indebidamente en una cuenta existente o para abrir una nueva tarjeta de crédito".[11]

TIPOS DE ROBO DE IDENTIDAD

1 Fraude de tarjetas de crédito: 157.688 denuncias

2 Otros robos de identidad: 122.499

3 Fraude relacionado con el trabajo o con impuestos: 67.374

4 Estafa telefónica o de servicios públicos: 63.563

5 Fraude bancario: 52.529

6 Estafa de préstamos o arrendamientos: 51.856

7 Fraude de documentos o referente a beneficios del gobierno: 24.854

Si observamos los peligros que más preocupan a los usuarios –hackeo de su cuenta bancaria, fraude en las compras en línea, alguien que cometa un delito a su nombre o que solicite un préstamo en su nombre y alguien que robe sus haberes utilizando información robada-, todas ellos implican algún tipo de delito que podría denominarse como robo de identidad.

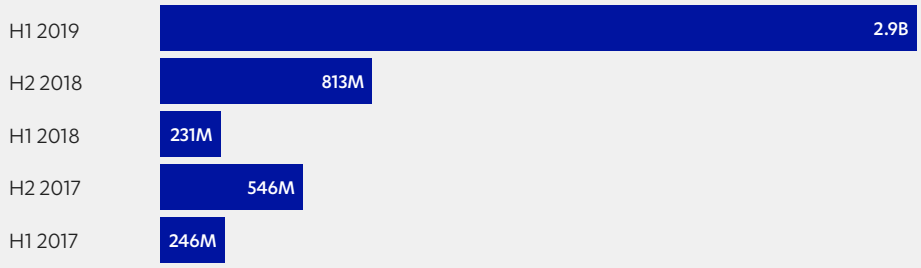
Hoy en día, la información necesita ser protegida más que nunca. Si los piratas se apoderan de ella pueden disponer de nuestra identidad o nuestras cuentas para cometer delitos que perjudiquen nuestra capacidad futura para obtener préstamos, firmar contratos o incluso conseguir un empleo.

11 Consumer Sentinel Network: Data Book 2018 https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

EXPERIENCIAS Y PREOCUPACIONES DE LOS USUARIOS

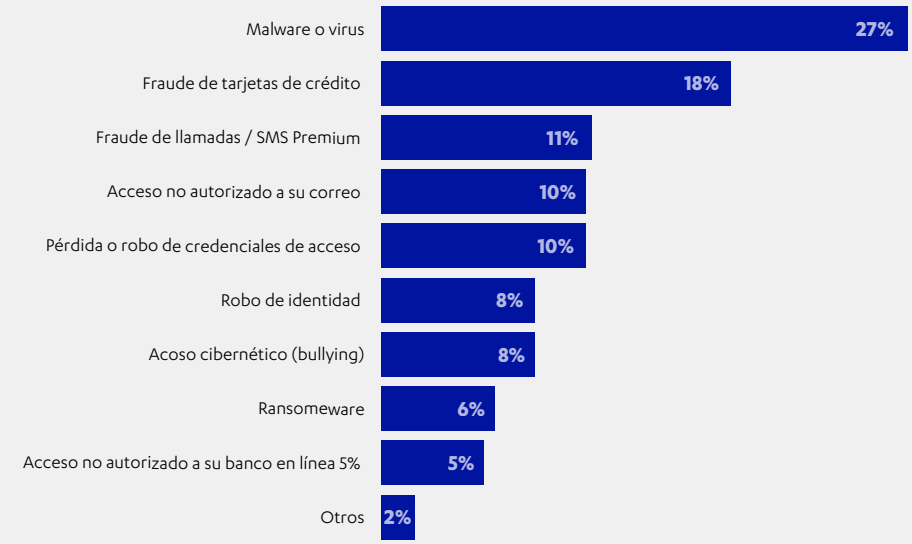
La red mundial de honeypots de F-Secure midió miles de millones de ataques en el primer semestre de 2019.[12]

TOTAL DE ATAQUES AL HONEYPOT MUNDIAL POR PERÍODO



Los ataques reportados por los usuarios a sus dispositivos electrónicos y redes domésticas que provienen de malware y virus (27%). Fraude con tarjetas de crédito (18%), fraude por SMS/llamadas (11%) y hackeo de correo electrónico o de cuentas (10%).[13]

LOS INCIDENTES MÁS COMUNES REFERENTES A SEGURIDAD



Si bien los software de seguridad evitan la infección a través de muchos de los programas dañinos y virus actuales, hoy en día, ante muchos ataques -fraude con tarjetas de crédito, estafa con llamadas, apropiación no autorizada de cuentas y robo de identidad- debemos proteger los datos tanto en los dispositivos electrónicos de los usuarios, como en las múltiples cuentas que la mayoría tiene con una amplia variedad de servicios y proveedores.

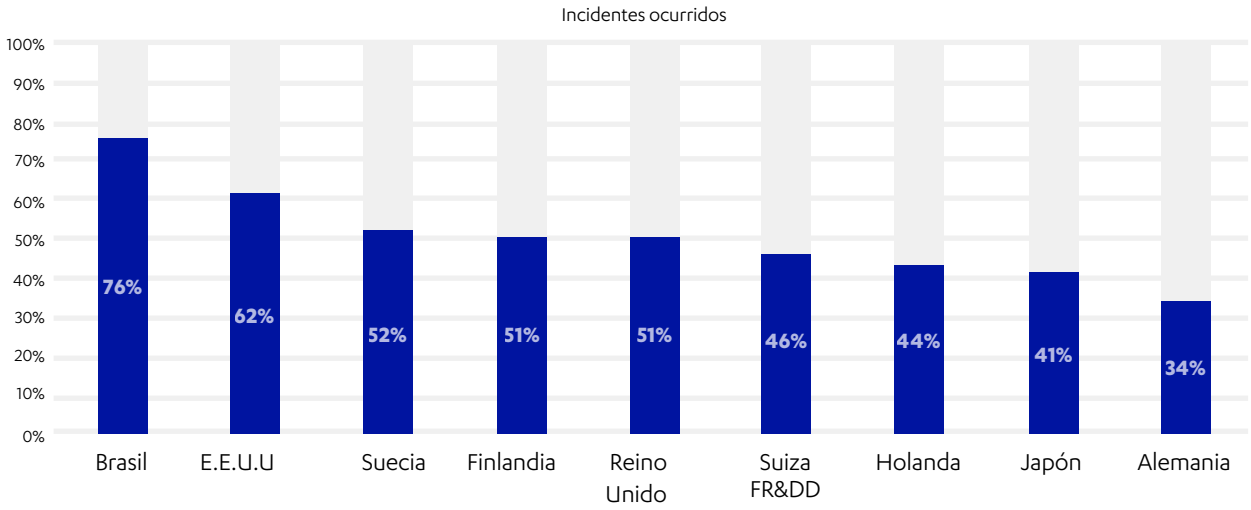
En la tercera década del siglo veinte, para estar seguro en la web, no es suficiente proteger sólo los aparatos que

12 Attack Landscape H1 2019: IoT, SMB traffic abound https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/
13 Source: F-Secure Identity Protection Consumer (B2C) Survey, May 2019, conducted in cooperation with survey partner Toluna, 9 countries (USA, UK, Germany, Switzerland, The Netherlands, Brazil, Finland, Sweden, and Japan), 400 respondents per country = 3600 respondents (+25years)

usamos, sino que también controlar la identidad y evitar el robo y el fraude en caso de que información privada termine en las manos equivocadas.

¿Quién ha sido afectado?

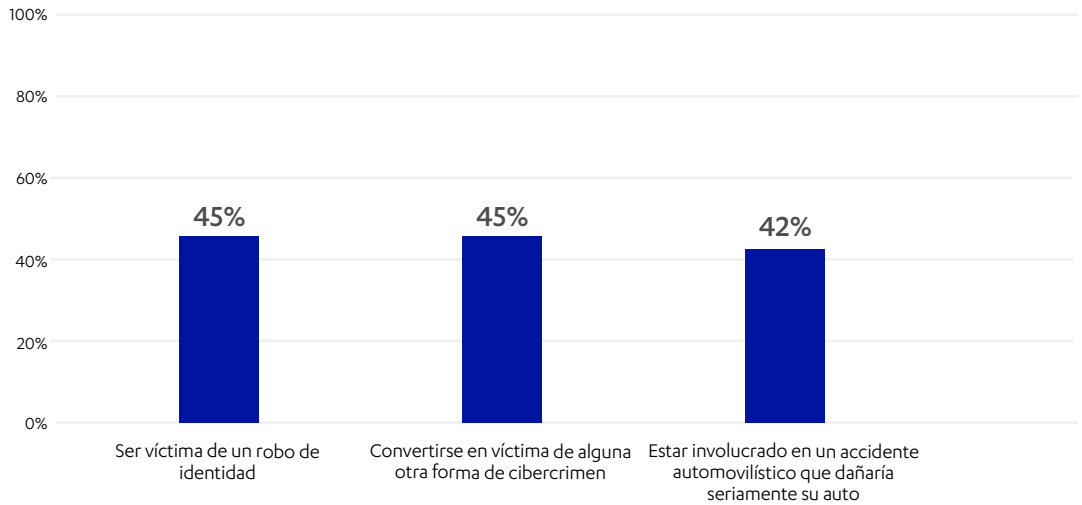
¿HA SIDO USTED O ALGUIEN DE SU FAMILIA VÍCTIMA DE UN DELITO CIBERNÉTICO?



Brasil es el país en el que es más probable verse afectado por la ciberdelincuencia, la impresionante cifra de tres de cada cuatro personas (76%) que han informado de un incidente experimentado en su familia lo demuestra. La mayoría de las familias en EE.UU. (62%), Suecia (52%), Finlandia (51%) y el Reino Unido (51%) han sufrido al menos un caso de cibercrimen.

Mundialmente hablando, la mayoría de las personas (51%) han sido afectadas por ciberdelitos, uno de cada cuatro (26%) reportó incluso lidiar con varios incidentes. Los alemanes, sin embargo, están haciendo algo bien, con sólo uno de cada cuatro (34%) reportes en su entorno familiar.

¿QUÉ TAN PREOCUPADO ESTÁ RESPECTO A LAS SIGUIENTES AFIRMACIONES?

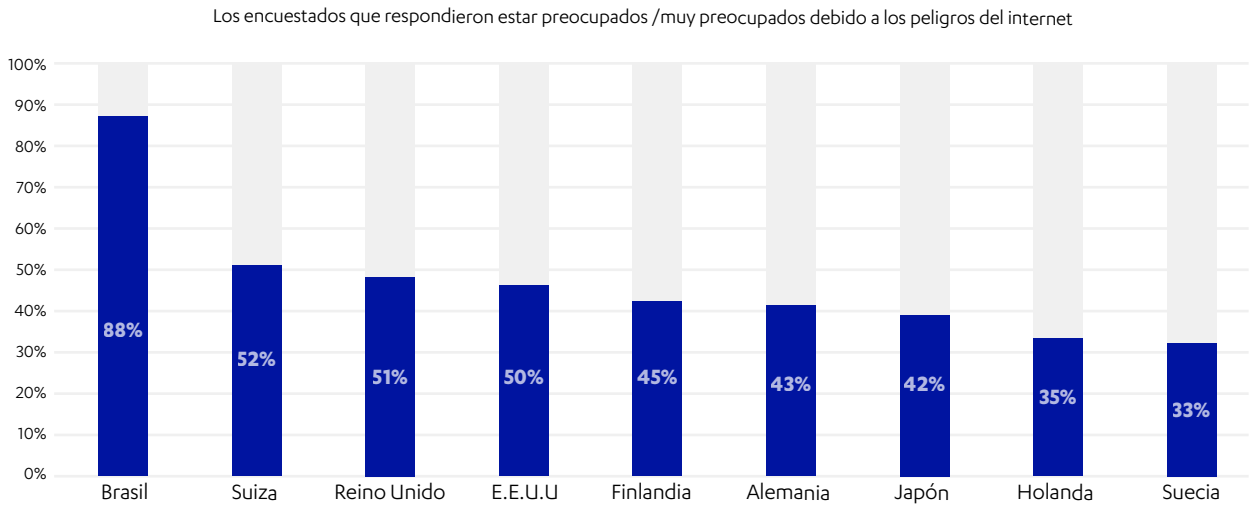


¿Es el robo de identidad el ciberdelito que más le tememos?

A nivel mundial, el temor al robo de identidad (45%) y a la ciberdelincuencia (45%) superan al miedo a tener un accidente de automovilístico que dañe gravemente su vehículo (42%). Los usuarios perciben que una identidad dañada causa más problemas que un auto dañado.

Si bien es fácil encontrar un mecánico para reparar un auto, la recuperación total de una identidad afectada no lo es.

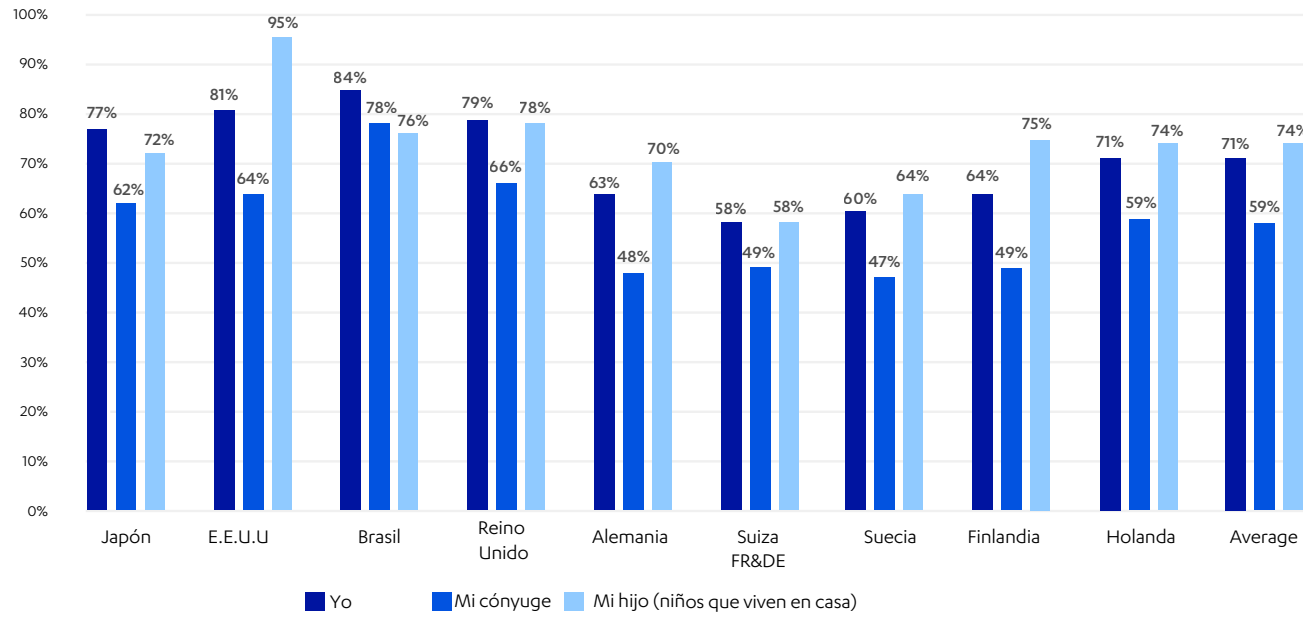
QUÉ PAÍSES ESTÁN MÁS PREOCUPADOS POR LAS AMENAZAS EN LA WEB



En vista de que más de tres de cada cuatro brasileños han tenido una experiencia propia con el cibercrimen, eso concuerda con que casi nueve de diez de ellos estén preocupados por las amenazas en línea.

Aproximadamente la mitad de los entrevistados en Suiza, el Reino Unido y Estados Unidos manifestaron temores del mismo tipo. Los usuarios de Internet holandeses y alemanes deberían compartir sus secretos de seguridad informática con el mundo. Sólo uno de cada tres están preocupados por las amenazas online.

PROBABILIDAD DE CONVERTIRSE EN VÍCTIMA DE UN DELITO CIBERNÉTICO O DE UN ROBO DE IDENTIDAD



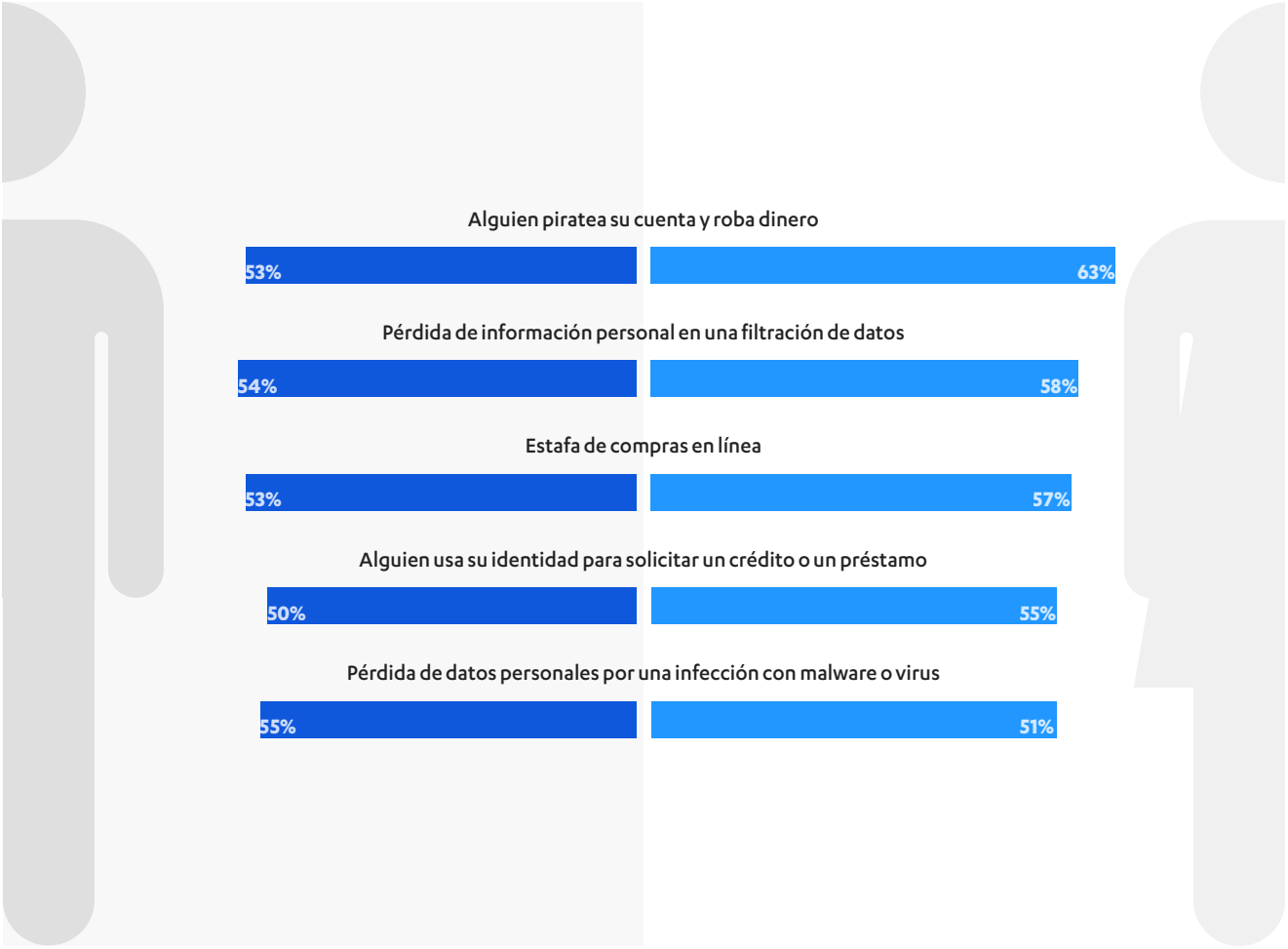
Incluyó respuestas: Moderadamente probable - Muy probable
Excluyó: Poco probable y nada probable

En todos los países examinados, la mayoría de los encuestados revelaron tener al menos un temor moderado a sufrir algún tipo de robo de identidad por concepto de ciberdelincuencia (71%)

Sin embargo, el miedo de los padres a que sus hijos tengan que enfrentarse a este tipo de situación, en ocho de los países encuestados supera la preocupación por su propia seguridad online - con excepción de Japón (77% Yo versus 72% Mi hijo) y Brasil (84% Yo comparado con 76% Mi hijo)

En Estados Unidos 19 de cada 20 padres (95%) manifestaron miedos significativos a que sus hijos sufran debido a las actividades de los piratas del Internet.

CONTRASTING MEN AND WOMEN



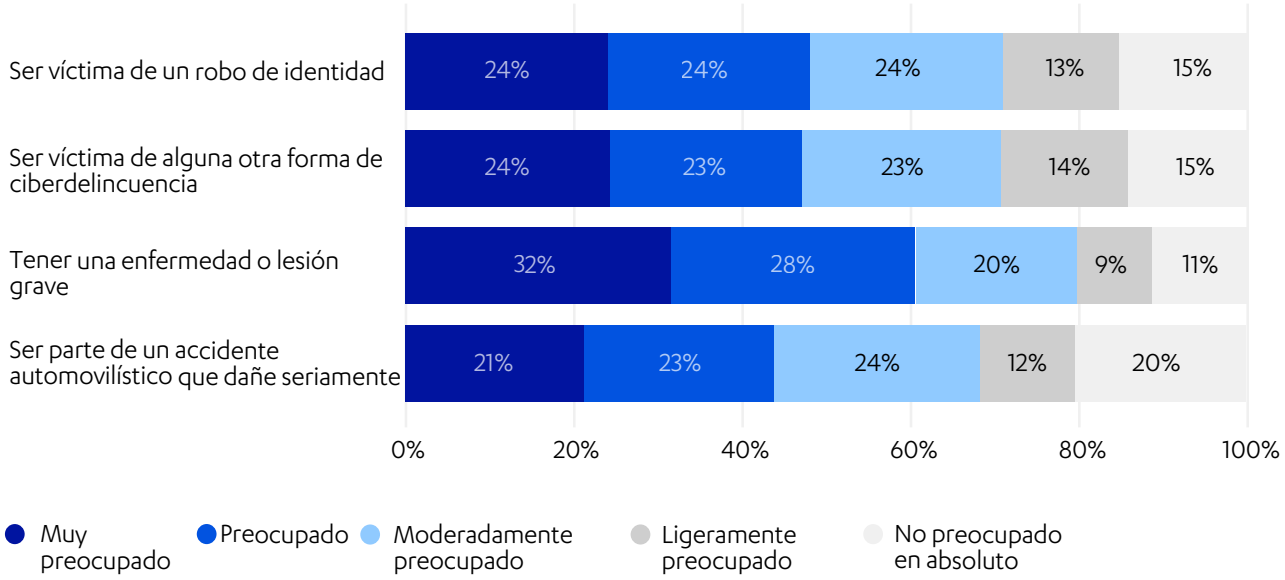
Los datos de este gráfico representan sólo a los encuestados que dijeron estar preocupados o muy preocupados, excluyendo a los que manifestaron estar sólo algo preocupados.

Aunque al menos el 50% de las mujeres y de los hombres están preocupados o muy preocupados por riesgos asociados con el robo de identidad, las mujeres están más alarmadas en relación a diversos peligros. La mayor diferencia, de un 10%, es que el sexo femenino tiene más temor (63%) a que alguien piratee su cuenta bancaria para robarles dinero, a diferencia de los hombres (53%).

El porcentaje de mujeres preocupadas o muy preocupadas por el robo de identidad y los cibercrímenes es de un 47 a 48%, cifra superior al 44% referente al miedo a sufrir un accidente de automóvil que dañe un vehículo.

Mujeres

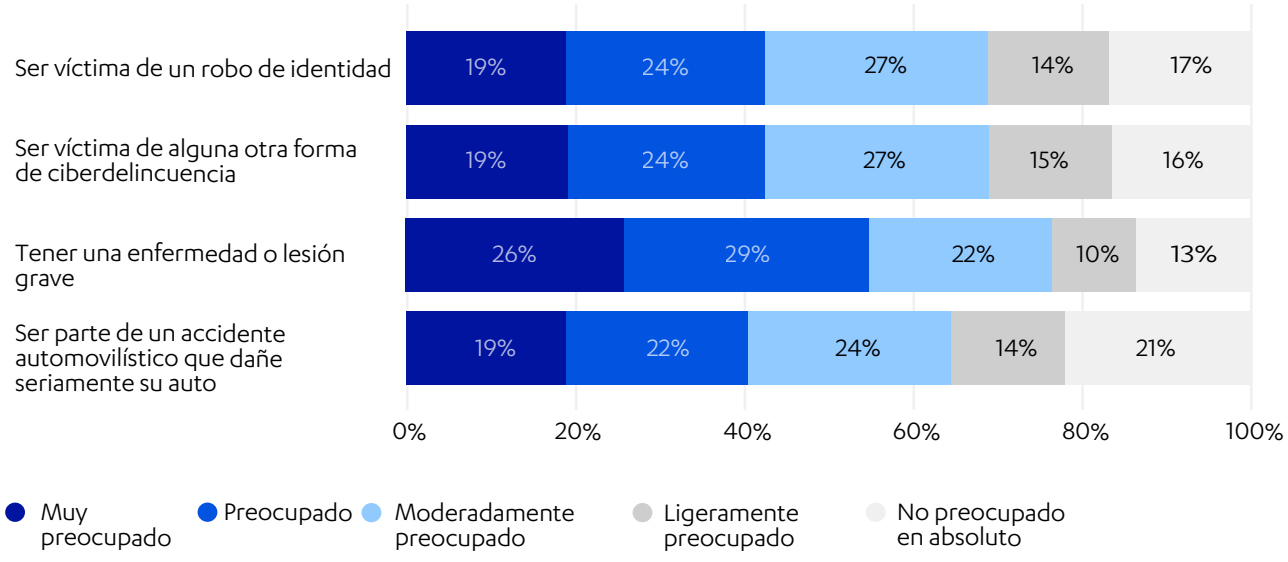
TAN PREOCUPADA ESTÁ USTED RESPECTO A LAS SIGUIENTES AFIRMACIONES? 1.855 Respuestas



También aquí son los hombres que muestran estar menos alarmados en general, un 43% manifesta estár preocupados o muy preocupados respecto al robo de identidad y el cibercrimen.

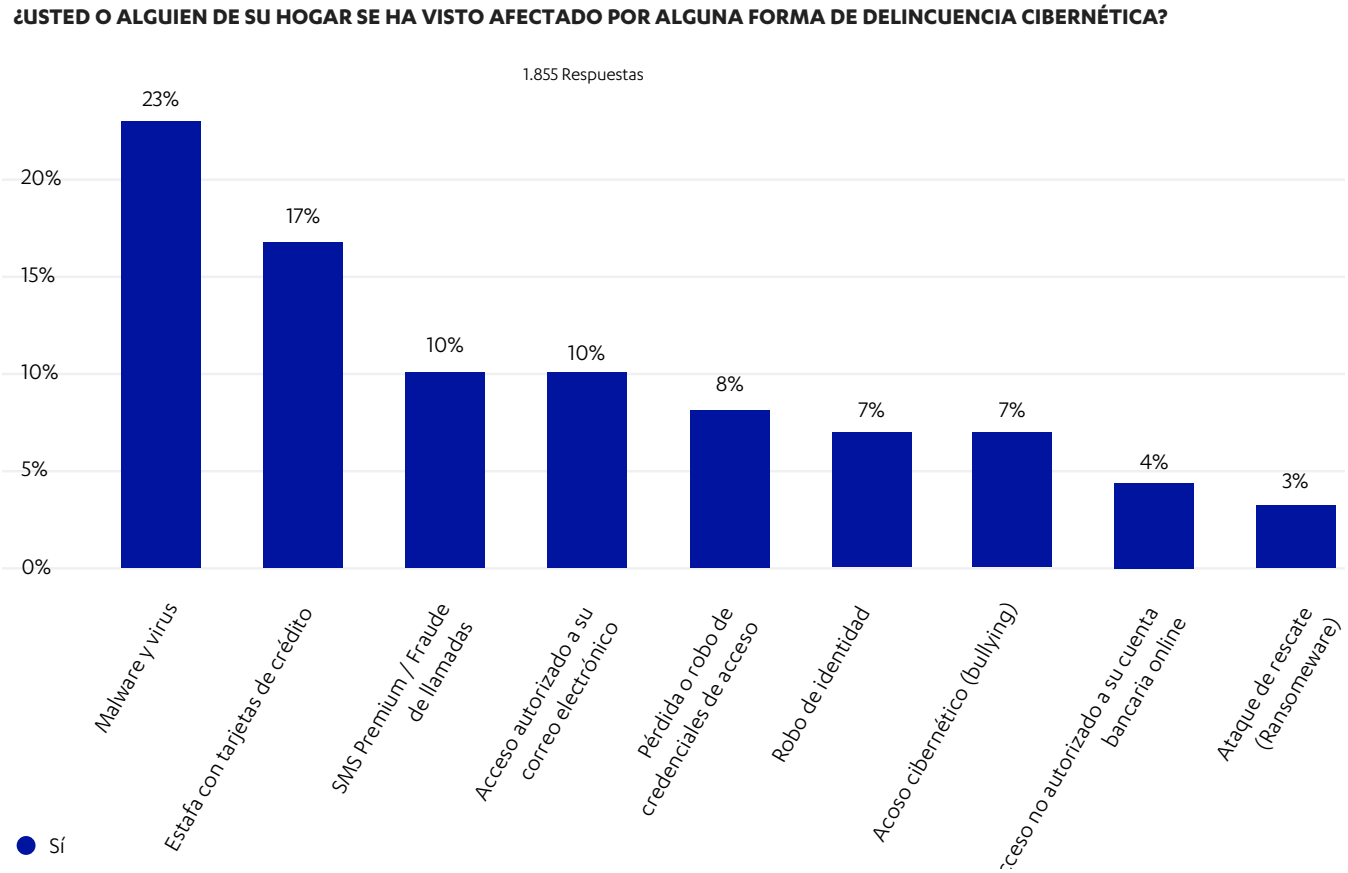
Hombres

TAN PREOCUPADO ESTÁ USTED RESPECTO A LAS SIGUIENTES AFIRMACIONES? 1.745 Respuestas



Mujeres

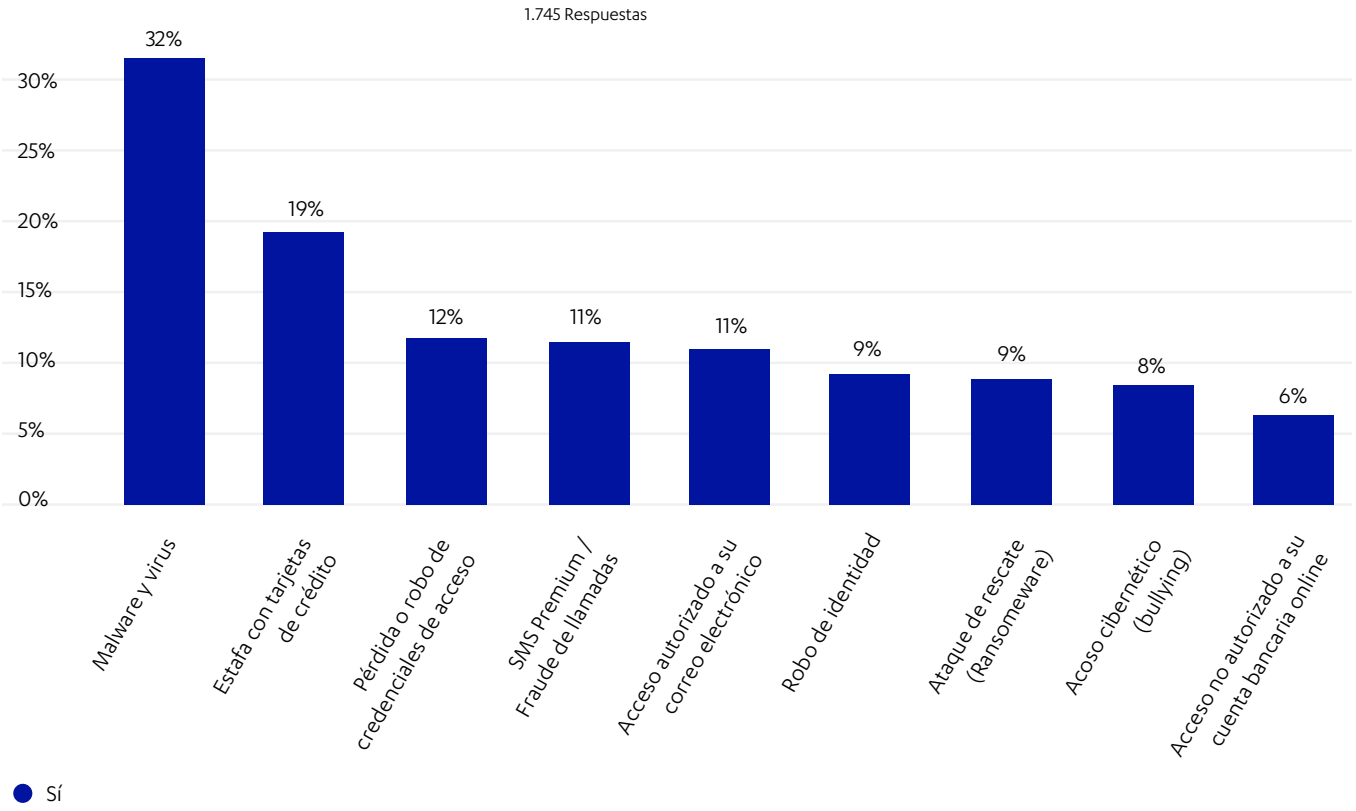
Un dato fascinante es que aunque expresan más preocupación, las mujeres son más reacias a denunciar haber sido víctima de algún tipo de ciberdelito.



Hombres

El 68% de los hombres muestran preocupaciones similares acerca del robo de identidad o los delitos cibernéticos, pero sólo el 42% de ellos con hijos dicen temer por ellos.

¿USTED O ALGUIEN DE SU HOGAR SE HA VISTO AFECTADO POR ALGUNA FORMA DE DELINCUENCIA CIBERNÉTICA?



CONCLUSIÓN

Los seres humanos no nos caracterizamos por ser buenos evaluadores de riesgos.

Si bien solemos sentirnos tensos antes que despegue el avión en que nos encontramos, es mucho más probable que suframos un accidente fatal cuando nos subimos a un auto y eso que éste no está sujeto a un plan riguroso de regulaciones e inspecciones una vez que sale de la línea de montaje.[14]

Un hecho interesante es que los hombres reportan haber estado más expuestos a las amenazas online que las mujeres, sin embargo, se preocupan menos por ellas. Asimismo, aunque los costos originados por la ciberdelincuencia aumenten cada año, el usuario promedio de la web sigue pasando tanto tiempo en línea como lo hace en su trabajo.

Notable es que cuando se trata de los peligros derivados del uso del internet, los usuarios parecen entender que los riesgos van mucho más allá de sólo nuestros dispositivos electrónicos.

Los tiempos en que asegurar el computador era suficiente para prevenir la mayoría de los problemas derivados de estar online se acabó hace rato. Actualmente, proteger docenas de cuentas, incluyendo los datos de las tarjetas de crédito, cuentas bancarias, de redes sociales, programas de filiación etc, es indispensable para proteger nuestra identidad.

El crimen cibernético es una preocupación real y las estafas y los perjucios a largo plazo inquietan a los usuarios. Los daños provenientes del robo de identidad pueden ser elevados y duraderos en el tiempo. Los consejos de los expertos, tanto para prevenir estos delitos como para afrontar rápidamente lasconsecuencias de un ataque, pueden reducir la ansiedad

¿Qué puede hacer usted al respecto?

La mayoría de los consejos de seguridad cibernética que comenzaron a circular en el minuto en que apareció el internet siguen siendo relevantes hoy. Es importante mantener su software actualizado, hacer clic a archivos adjuntos desconocidos sigue siendo una mala idea. Utilizar un software de seguridad de calidad sigue siendo una buena opción.

A pesar de ello, sin importar lo bien que asegure sus dispositivos electrónicos, no es posible proteger sus datos completamente, cuando ellos están almacenados en las redes de una empresa externa.

Las filtraciones de datos no sólo revelan nuestra información privada, sino que también demuestran nuestra dependencia de empresas repartidas por todo el mundo.

La buena noticia es que hay medidas simples que usted puede tomar para ayudar a proteger su identidad en el internet.

Olvide sus claves de acceso

Si puede recordar sus claves, probablemente no sean lo suficientemente seguras para proteger sus cuentas. Entonces, ¿qué hacer con más de una docena de passwords que no puede recordar? La solución a este problema es un administrador de claves fiable.

Emplee en todas sus cuentas la autenticación de dos factores

La mejor clave de acceso del mundo puede ser hackeada si no está bien asegurada por el sitio al que usted la ha entregado. Es por eso que es conveniente utilizar la autenticación de dos factores para asegurar sus cuentas en cualquier lugar en que estén disponibles.

14 Which Is Safer: Airplanes or Cars? https://fortune.com/2017/07/20/are-airplanes-safer-than-cars/

Pero recuerde que es posible sortear la autenticación de múltiples factores accediendo a correos electrónicos y mensajes de teléfono celular. Así que para mayor seguridad le recomendamos una aplicación como Google Authenticator como segundo factor.

Verifique lo expuesto que está actualmente

Las listas de claves de usuarios hackeadas suelen circular entre los criminales que las recolectan para convertir esta información en ataques y obtener lucro de ellos. Esto puede derivar en phishing, spam y en la propagación de malware. Como las actividades fraudolentas son dirigidas, es mucho más probable que tengan éxito en comparación con el típico spam. ¿Cómo puede enterarse de lo vulnerable que es usted actualmente? Le recomendamos consultar un servicio de confianza para verificar si su información está disponible en algún lugar de la dark web.

¿Como comportarse si cree haber sido víctima de un robo de identidad?

Si cree que su identidad ha sido robada, recuerde que no es el único con el problema. Esto sucede a más de un millón de personas cada mes,[15] comparado con los 10.000 automóviles que fueron robados mensualmente en todo el mundo en el 2017 .[16] La clave es actuar rápidamente..

Estos son los consejos de la Comisión Federal de Comercio (FTC) de cómo reaccionar ante tales casos:

1. Llame a los departamentos de fraude de las empresas donde se produjo para congelar sus cuentas. Cambie las claves de inicio de sesión, los pin y password de acceso de todas las cuentas comprometidas.
2. Llame a las principales oficinas de crédito para colocar una "alerta de fraude" y obtener una copia actual de su crédito. Las notificaciones de estafa ante Experian, TransUnion y Equifax son gratuitas. La alerta requiere que todos los nuevos acreedores verifiquen su identidad y ella puede ser renovada posteriormente.
3. En Estados Unidos puede reportar su robo de identidad a la FTC llamando al 1-877-438-4338 o contactando a la agencia por internet.
4. Puede presentar una denuncia ante la policía local. Es probable que necesite identificarse con algún documento emitido por el gobierno, comprobar su dirección y dar prueba del robo. En EE.UU. necesitará además el informe de robo de identidad de la FTC.

15 Facts + Statistics: Identity theft and cybercrime https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
16 Interpol: Vehicle Crime https://web.archive.org/web/20181103162315/https://www.interpol.int/Crime-areas/Vehicle-crime/Vehicle-crime

ACERCA DE F-SECURE

Nadie más cuenta con los vastos conocimientos sobre ataques cibernéticos que posee F-Secure. Somos capaces de cubrir tanto la detección como la respuesta a incidentes, utilizando la incomparable experiencia de cientos de los mejores consultores del sector, millones de dispositivos electrónicos dotados con nuestro galardonado software e incesantes innovaciones en el campo de la inteligencia artificial. Los bancos más importantes, aerolíneas y empresas confían en nosotros para hacer frente a los ataques más potentes del mundo.

Junto a nuestra red de partners y más de 200 proveedores de servicios, tenemos la misión de velar por que todos obtengan la seguridad cibernética a nivel empresarial que requieren.
Fundada en 1988, F-Secure cotiza en el NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure

F-Secure