3'50 € PORTUGAL: 4 € / CANARIAS: 3,65 € • Sale viernes sí, viernes no • PRÁCTICA • ACTUAL • QUINCENAL

Computer Hoy

Nº 675 • AÑO XXV
DEL 16 AL 29 DE AGOSTO DE 2024
computerhoy.com

¡No bajes la guardia!
Nuevas estafas en Internet

práctico

¡Acaba con el espionaje!
... sin perder funciones ni rendimiento

iOS

PROGRAMAS, TRUCOS Y CONSEJOS ACTUALIZADOS

- **Frena el filtrado** de datos a Microsoft
- **Elimina rastros** en Windows y macOS
- **Protege tu privacidad** en Android e iOS
- **Evita el seguimiento** en tu navegador
- Y mucho más...

test

10 Suites de seguridad analizadas a fondo

- ¿**Cuánto cuesta** proteger tus dispositivos?
- ¿Es suficiente con **Microsoft Defender?**
- ¿Qué **protección extra** ofrecen?
- ¿**En qué fijarse** antes de comprar?...

6 Gestores de contraseñas

- **Por qué confiar** en ellos
- ¿Qué son las **passkeys**?
- **Cómo crear** contraseñas seguras...

TODO LO QUE DEBES SABER PARA ESTAR PROTEGIDO

ESPECIAL SEGURIDAD

actualidad

Timos en alojamientos vacacionales
No caigas en la trampa: peligros en páginas web

Desaparecer
de Internet no es tan fácil

test / comparativa

8 Cámaras de videovigilancia
¡Protege lo que más te importa!

prácticos

Cómo localizar tus dispositivos perdidos con ayuda de Google

Lee mensajes de WhatsApp sin dejar huella

Computer Hoy

unclick

La newsletter de **Computer Hoy**

La tecnología desde un punto de vista muy personal

Suscríbete a nuestra newsletter gratuita, donde nuestros expertos te contarán la actualidad tecnológica de una forma diferente.

Suscríbete aquí

EDITORIAL

Computer Hoy Nº 675

CARLOS GOMBAU
Redactor Jefe

LA SEGURIDAD ES UNA ASIGNATURA PENDIENTE EN ORDENADOR Y MÓVIL

"Tranquilo, que yo controlo", pero no... Por cuarto año consecutivo, un verano más te traemos un número especial con los mejores artículos sobre seguridad publicados en las páginas de Computer Hoy durante los últimos 12 meses. En la primera edición, hace tres años, apelaba en esta misma página a la Teoría de Compensación del Riesgo para explicar cómo el exceso de confianza nos lleva a no tomar las medidas de precaución necesarias ante escenarios de peligro. Como comentaba, la teoría se conoce actualmente como efecto Peltzman y afirma que, cuanto menor es el riesgo percibido en una situación determinada, las medidas de precaución que tomamos son menores. O, dicho de otra forma, tenemos comportamientos más o menos arriesgados en función de si nos sentimos más o menos protegidos. Y luego vienen los sustos.

Compensamos las medidas de seguridad impuestas tomando conductas más atrevidas de lo normal. El problema es que este sentir puede ser solo una mera ilusión. Recuerda, los sesgos cognitivos se alimentan de nuestra ignorancia sobre ellos: que no percibamos el riesgo o que nos sintamos seguros, no quiere decir que no exista. En este sentido, el Instituto Nacional de Ciberseguridad (INCIBE) junto al Observatorio Nacional de Tecnología y Sociedad (ONTSI) publicaron en octubre de 2023 el dosier 'Cómo se protege la ciudadanía ante los ciberriesgos', un estudio sobre la percepción y el nivel de confianza en España en seguridad informática.

> "EL 66 % DE LOS QUE SE VEN PREPARADOS TIENE SUS EQUIPOS INFECTADOS".

Entre otras cifras y conclusiones que merece la pena analizar, destaca que muchos usuarios de PC creen tomar medidas de seguridad, cuando en realidad no son conscientes de que no (el 86,9 % declara tener su sistema actualizado, cuando sus dispositivos reflejan que el 41,1 % lo está). A esto se suma que afirman adoptar medidas de privacidad, pero la realidad lo desmiente. En el hogar, se tiende a pensar que los PC son más seguros de lo que son, mientras que los móviles se perciben como más vulnerables de lo que han demostrado ser. Solo un dato más: el 66 % de los usuarios que se consideran bastante preparados en ciberseguridad tiene sus equipos infectados. El riesgo es real.

carlos.gombau@axelspringer.es | @cgombau

Tu opinión cuenta...

Computer Hoy computerhoy.com
ComputerHoy
@computerhoy
ComputerhoyTV
@computerhoy.com
axel springer store.axelspringer.es

No te pierdas...

ENGAÑOS Y FRAUDES

En la era digital, los timos online se encuentran en constante evolución, ¡y cada vez son más sofisticados! Es esencial mantenerse alerta y tomar medidas para proteger la información personal. **Página 6**

STOP AL ESPIONAJE

Es imprescindible proteger la privacidad en el ordenador y el móvil. Ahora puedes lograrlo con consejos y programas que te ayudarán a detener el espionaje en tus dispositivos. **Página 36**

LA GRAN PRUEBA DE SEGURIDAD DE 2024

La protección antivirus es ahora más importante que nunca. Analizamos varios programas que prometen seguridad para tu equipo y que van más allá de la eliminación de virus. **Página 50**

SUMARIO

COMPUTER HOY Nº 675

8 Falsos alojamientos vacacionales

Al llegar a tu destino, la sorpresa puede ser mayúscula: la bonita casa de vacaciones ni siquiera existe o ya hay otros inquilinos viviendo en ella. Si te vas pronto de vacaciones, debes protegerte para evitar contratiempos inesperados.

10 ¿Te pueden robar las claves de acceso al banco?

Para robar las claves de acceso a los bancos de las posibles víctimas, los ciberdelincuentes emplean técnicas de diversa índole, que tienen como finalidad encontrar usuarios desprotegidos o descuidados. Te contamos cómo se llevan a cabo este tipo de ataques, y qué puedes hacer tú para protegerte debidamente ante el robo de la información sensible.

44 Leer WhatsApp sin ser visto

Desde la barra de notificaciones, con widgets o mediante el modo avión, existen formas de que tus contactos no sepan que has leído sus mensajes.

48 Encuentra tu móvil Android

No saber dónde has dejado el móvil es una situación muy común. Afortunadamente, Android cuenta con una función que te permite localizarlo en pocos minutos.

58 Elige un gestor de contraseñas

Tus cuentas online deben estar seguras, y los gestores de contraseñas se encargan de lograrlo eficientemente.

64 Cámaras de videovigilancia

Las cámaras de seguridad custodian tu casa, la puerta principal y el jardín. Pero ¿qué modelos graban realmente bien y cuáles vigilan mejor?

70 Peligros y amenzas online en 2024

Es el momento de analizar los principales riesgos en materia de ciberseguridad. La privacidad de los datos, los sistemas de seguridad en la nube y la IA son elementos clave.

73 ¿Qué es Bug Bounty?

Los programas Bug Bounty permiten a las empresas aprovechar la comunidad de hackers éticos (de sombrero blanco) para de esta forma mejorar eficazmente la seguridad de sus sistemas.

Actualidad

Práctico

Test

Saber más

PASAPORTE EUROPEO

UNO PARA TODOS

La UE quiere introducir una cartera digital. Entre otras cosas, servirá de documento de identidad. Sin embargo, el proyecto en cuestión ha levantado ampollas entre los defensores de la protección de datos.

Identificarse ante las autoridades, alquilar un coche, solicitar un préstamo: hasta ahora, se necesitaba el antiguo DNI para estas y otras muchas cosas. En el futuro, la denominada **Cartera de Identidad Digital Europea o EU Digital ID Wallet (ID-Wallet)** lo sustituirá. En diciembre de 2022, los Estados de la UE acordaron las normas para esta cartera digital para el móvil. En cualquier caso, el ID-Wallet podría facilitar muchas cosas: por ejemplo, gracias al número de identificación personal almacenado en ella, no sería necesario demostrar la identidad acercando el DNI a una videocámara.

Uno de los primeros intentos de establecer un documento de identidad digital se llevó a cabo en Alemania y tuvo lugar en 2021: Andreas Scheuer (CSU), entonces ministro federal de Transportes, quería introducir un permiso de conducir digital. Poco después de su lanzamiento, este proyecto se paralizó debido, entre otras cosas, a deficiencias de seguridad. La vecina Austria avanzó un poco más: el país lanzó hace poco tiempo el permiso de conducir digital y ya está reconocido como documento oficial en toda la UE. La república alpina es pues pionera y probablemente también líder en el desarrollo del ID-Wallet.

En cualquier caso, hasta ahora todo esto solo existía sobre el papel. Ahora hay que construirlo paso a paso y, para ello, los Estados de la UE tienen que ponerse de acuerdo sobre la tecnología. Solo así podrá utilizarse el ID-Wallet en todos los países. Y aquí, a más tardar, es donde Protección de Datos querrá opinar.

Muchas críticas

La UE quiere permitir el uso del ID-Wallet no solo para la identificación ante las autoridades o la policía, sino también para que el sector privado pueda utilizar la prueba digital de identidad en sus servicios. Entre otras, plataformas como **Amazon, Google o Meta (Facebook) y los bancos** estarán obligados a apoyar el ID-Wallet. Sin embargo, según los críticos, el reglamento de la UE que lo introduce, hasta ahora solo contiene salvaguardias insuficientes para proteger a los usuarios de la publicidad personalizada o el rastreo, por ejemplo. Aquí es donde la UE debe mejorar. Además, **los defensores de la protección de datos** exigen que la información recogida a través del ID-Wallet solo pueda almacenarse durante un periodo de tiempo muy limitado.

El problema más grave es que la UE quiere que los proveedores de navegadores permitan determinados certificados de seguridad. Así, los llamados Qualified Website Authentication Certificates (QWACs) deberán convertirse en estándar. Sin embargo, en los círculos de protección de datos, se consideran **anticuados y, sobre todo, inseguros**.

> Hay que tomar muy en serio las críticas de los expertos.
>
> **Thomas Fuchs**
> Comisario de Protección de datos

Se requieren mejoras

Así que aún queda mucho por aclarar antes de que el número de identificación personal y el ID-Wallet se hagan realidad. Así lo cree también Thomas Fuchs, Comisario de protección de datos alemán, responsable por ejemplo de Google y Meta/Facebook: "Los certificados de cifrado (QWAC) previstos para la solución que la UE quiere utilizar, son diferentes de los estándares de cifrado utilizados actualmente por los navegadores (estructuras CA) y deben comprobarse con vistas a la seguridad de los datos antes de su uso", declaró Fuchs a Computer Hoy. Y advierte de que la normativa debe redactarse con sumo cuidado antes de que sea demasiado tarde: "Aún quedan muchas cuestiones por aclarar, sobre todo en lo que respecta al uso seguro. En las próximas negociaciones a nivel europeo, todavía hay bastante margen de mejora desde el punto de vista de la protección de datos y la privacidad. Hay que aprovechar esta oportunidad", afirma Fuchs. Esperemos que todas sus preocupaciones se escuchen también en Bruselas. ■

ENGAÑOS Y FRAUDES

Las malas noticias nunca vienen solas: hay toda una serie de estafas y fraudes que convulsionan Internet.

CÓDIGOS QR QUE QUIEREN HACERTE CAER EN LA TRAMPA

Los proveedores de correo electrónico, los gestores de correo y el software antivirus se encargan de filtrar con cierto nivel de fiabilidad los mensajes fraudulentos, para así proteger a los usuarios. Estos programas comprueban de manera automática los enlaces que se incluyen en los mensajes y detectan a tiempo las amenazas. Sin embargo, los delincuentes han descubierto que el filtrado de códigos QR, por el momento, no funciona siempre. Y aunque siguen enviando correos electrónicos falsos de manera indiscriminada a millones de destinatarios, el enlace a las páginas de phishing o de malware se ha convertido ahora en un código QR que puede saltarse los controles básicos de seguridad. Los usuarios ya se ha familiarizado con el uso de este tipo de códigos, que a primera vista parecen completamente 'profesionales', y que por este mismo motivo los usuarios están dispuestos a capturar con la cámara de su smartphone (para así abrir los enlaces). Pero es entonces cuando se cae en la trampa. En caso de que te encuentres en tu buzón de entrada un mensaje de este tipo que incluya un código QR, ten especial cuidado y si tienes la más mínima duda, elimina el email.

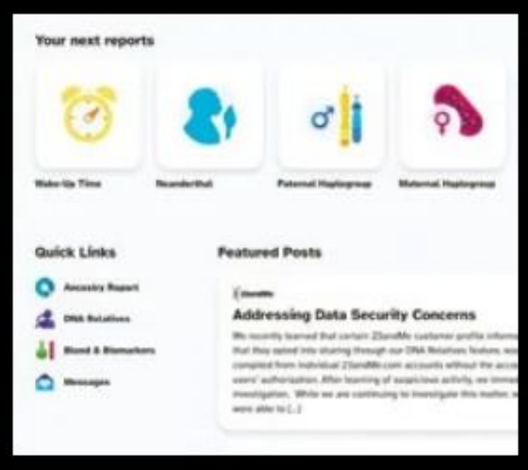
MOTEL ONE: DATOS DE CLIENTES ROBADOS

El grupo hotelero Motel One ha sido víctima de un ataque de ciberseguridad. En la Dark Web, ha aparecido un archivo de 6 TB que contiene información sobre las pernoctaciones de sus hoteles desde 2016. Detrás del ataque se encuentra el grupo BlackCat/AlphV, conocido ya por estar involucrado en algunos casos de extorsión ('petición de rescates'). Por lo que parece, Motel One se negó a pagar un rescate, y el grupo de delincuentes hizo públicos los datos. De todas formas, no se conocen todos los detalles del caso, ya que Motel One apenas ha informado sobre lo ocurrido. La empresa únicamente se ha limitado a comunicar en su página web que se han extraviado direcciones y datos de 150 tarjetas de crédito. Los propietarios de estas han sido informados personalmente, así como las autoridades competentes. Según diversos medios de comunicación, los datos robados incluyen listas con la información de quiénes han realizado reservas en el hotel, con quiénes han estado y en qué habitaciones. De ser esto cierto, el hecho podría dar lugar a situaciones un tanto incómodas.

Foto: Depositphotos.com

EL ADN EN INTERNET

El filtrado de datos de tarjetas de crédito y direcciones es algo que desde hace tiempo forma ya parte de la cotidianidad de Internet. Sin embargo, un problema de seguridad con los datos de la empresa estadounidense 23&Me está llevando ahora las cosas a otro nivel. Desde hace años, esta compañía ofrece a sus clientes la posibilidad de descifrar su información genética. Todo aquel que esté interesado en conocer sus orígenes personales familiares o buscar sus ancestros o parientes lejanos en todo el mundo puede enviar una muestra de saliva a 23&Me. En base a los datos obtenidos, la empresa crea un perfil genético que hasta cierto punto podría revelar información valiosa sobre el linaje de la persona, es decir, sobre su ascendencia o procedencia. Las personas que dan su consentimiento reciben automáticamente información o indicios sobre otros usuarios que muestran coincidencias en su ADN. Un atacante ha puesto a la venta en la Dark Web un millón de registros con datos de dichos perfiles. Como indicó la revista de seguridad **bleepingcomputer.com**, 23&Me niega esta cifra tan elevada, pero ha confirmado la autenticidad de los datos. Es probable que el acceso a la información no se haya producido a través de una vulnerabilidad interna, sino que se haya consumado a través del ataque a cuentas de usuarios individuales. Lo



23&Me podría haber sido víctima de un acceso al legado genético.

que resulta particularmente extraño de todo esto es que, según una publicación del atacante, los datos incluyen perfiles de personas cuyo ADN comparte similitudes de descendencia con los judíos asquenazíes.

ENGAÑO POR WHATSAPP: ESTAFAS SOBRE TRABAJO

¿Quién no se da por aludido cuando un empresario le atrae con la oferta de un empleo fantástico y un sueldo excepcional? Y de esto es precisamente de lo que se sirven los estafadores en las conocidas estafas de trabajo o job-scamming. Envían mensajes por WhatsApp haciéndose pasar por empleados de portales de empleo como Stepstone. A las víctimas se les requiere que proporcionen datos personales, incluso los información sobre su cuenta a través de un sitio web vinculado. Como es de suponer, no existe ninguna oferta de trabajo real y los estafadores hacen uso de los datos robados para otra finalidad, como por ejemplo la suscripción de servicios. Si estás buscando trabajo, debes tener siempre presente que los portales de empleo no se van a poner en contacto contigo a través de WhatsApp, ¡accede siempre directamente al portal web de la empresa en cuestión!

BARATO, PERO TAMBIÉN INFECTADO DE MALWARE

Cerca de 74.000 dispositivos de todo el mundo muestran síntomas de estar infectados con Badbox. El problema involucra a móviles, tablets y TV box baratos con el sistema operativo Android, que se distribuyen ya con el malware desde fábrica. Esto es lo que han descubierto los expertos en seguridad de la empresa Human Security: los dispositivos provenientes de China se preparan con malware tras su fabricación, y después se empaquetan y distribuyen. De esta forma, los compradores no tienen la más mínima sospecha. Las marcas son en gran medida desconocidas y sus dispositivos se venden por lo económicos que son, tanto en Internet como en tiendas de electrónica. Todos los dispositivos infectados examinados habían sido manipulados y no contaban con la capa de seguridad Play Protect de la tienda de aplicaciones. Una vez puesto en marcha, el hardware conecta con el servidor de los ciberdelincuentes y descarga más malware. Este muestra anuncios, roba datos de acceso a cuentas online e intercepta transacciones financieras. Human Security indica que los dispositivos no pueden ser reparados puesto que los fabricantes delictivos podrían volver a tenerlos bajo control con una actualización.

PELIGRO TAMBIÉN EN LINUX

Son muchos los que consideran que el sistema operativo Linux es manifiestamente más seguro que Windows. Investigadores de seguridad de Kaspersky han encontrado precisamente ahora una vulnerabilidad en este entorno, que se cree que ha puesto en peligro a los sistemas durante al menos tres años. Según informó Kaspersky, el sitio web oficial del conocido programa Free Download Manager habría redirigido a los usuarios de Linux a una página maliciosa. Una versión manipulada del software robaba el historial de navegación, la información de acceso a almacenamiento en la nube y las wallets de criptomonedas de las víctimas. Todo el que haya instalado la versión para Linux entre 2020 y 2022 podría estar afectado; mientras que los usuarios de la versión de Windows o Mac del programa probablemente no lo estén.

OTRAS NOTICIAS SOBRE **SEGURIDAD**

Malware para Androiod

El malware XLoader se ha convertido en un gran peligro para los usuarios de Android. Este software se instala sin tu permiso y se disfraza como la aplicación Google Chrome. Todo ello con la intención de acceder a tu información personal y vulnerar la seguridad del dispositivo.

Pagos ransomware

Los pagos de ransomware alcanzaron cifras récord en 2023, marcando un año devastador en la lucha contra este tipo de ciberataques. Según un informe de Chainalysis, las víctimas pagaron a grupos de ciberdelincuentes un total de 449,1 millones de dólares (casi 400 millones de euros).

Regalos falsos de una operadora

Foto: Depositphotos.com

Como suele suceder en estas situaciones, los timadores se presentan como si se tratara de una empresa de renombre, esta vez Vodafone, para informarte de manera fraudulenta de que puedes ganar un regalo, a cambio de realizar una encuesta. Para ello, ofrecen poder conseguir gratis obsequios como teléfonos Samsung o iPhone y vales descuentos.

NO CAIGAS EN LA TRAMPA: ESTAFAS EN PÁGINAS WEB

Falso: este sitio parece una empresa profesional de alquiler de casas de vacaciones, ¡pero no es más que una estafa!

¡Te vas de vacaciones! Vuelo reservado, piso de vacaciones pagado, equipaje hecho... Pero al llegar, te encuentras con la sorpresa de que la bonita **casa vacacional ni siquiera existe**, o de que ya hay otros inquilinos en ella. Últimamente, un número alarmante de veraneantes se encuentra en esta terrible situación. Y el motivo es una nueva moda de estafas. Te explicamos cómo reconocer los timos y qué debes hacer.

Anuncios falsos en Internet

La estafa es siempre la misma: en Booking, Airbnb y otras conocidas plataformas de alojamientos vacacionales, los estafadores publican ofertas de casas que en realidad no existen. Por lo general, se trata de un lugar atractivo a un precio relativamente bajo. Las fotos encajan y resulta que el alojamiento aún está disponible. Incluso las consultas se responden rápida y personalmente. En realidad, todo parece perfecto y acogedor. A la hora de pagar, los propietarios intentan trasladar el contacto a WhatsApp o a otras aplicaciones de mensajería, con el argumento de ahorrarse comisiones. A menudo, ofrecen un descuento del 10 % al 20 %, y así muchas víctimas caen en la trampa. Después, los supuestos arrendadores exigen un anticipo 'como garantía': a veces todo el importe, a veces solo la mitad... que, además, debes transferir a una cuenta en el extranjero.

Millones de euros en daños

Algunas asociaciones europeas de casas vacacionales calculan en decenas de millones los perjuicios causados por este fraude a los turistas. El Centro Europeo del Consumidor calcula que solo en España hay varios miles de víctimas al año. Quienes caen en la estafa casi siempre pierden su dinero, pero aún es peor: las víctimas solo se dan cuenta del fraude cuando llegan al lugar y se encuentran sin alojamiento en otro país. A menudo, tienen que organizar rápidamente una sustitución costosa o, incluso, cancelar sus vacaciones antes de que puedan disfrutarlas. Esto pone a prueba los nervios, sobre todo en un entorno desconocido.

Pero ¿quién responde?

La buena noticia es que, si reservas y pagas directamente a través de **portales de confianza como pueden ser Booking o Airbnb**, estarás protegido frente a este tipo de fraudes. Estos portales siempre retienen el dinero hasta que hayas hecho el check-out. Así, si algo no encaja o si había un timo detrás de la oferta, lo denuncias al proveedor y te devuelve el dinero.

Precisamente por eso, los estafadores siempre intentan que realices pagos fuera de la plataforma. Ahí ya no hay protección, y solo con mucha suerte podrás recuperar el pago a través del banco o del proveedor de la tarjeta de crédito. Sin embargo, los plazos para esto a menudo se superan, los estafadores se encargan de ello. Entonces, tienes las de perder. El portal de reservas solo podrá bloquear al proveedor, lo que no sirve de mucho, ya que los estafadores se limitan a crear nuevas cuentas.

¿En qué debes fijarte?

No es tan fácil distinguir una oferta fraudulenta de una casa de vacaciones auténtica. A veces, los delincuentes incluso copian ofertas reales, en las que todo es correcto y solo las modifican mínimamente. No obstante, hay algunas cosas que son sospechosas y en las que

TIMOS EN ALOJAMIENTOS VACACIONALES

Un viaje estival con sorpresa desagradable: si caes en la trampa de los estafadores, te encontrarás con las puertas cerradas en tu destino de vacaciones. ¡Así es como debes protegerte!

PÁGINAS DE TIMOS SORPRENDENTEMENTE BUENAS

Además de los portales, los estafadores también utilizan sus propias páginas. A menudo, un enlace de la oferta en una plataforma conocida conduce a otra página, en la que se supone que se debe hacer la reserva u obtener un gran descuento. Tanto las entradas de los portales populares como las páginas falsas parecen auténticas y muy profesionales. Y, en algunos casos, los sitios web falsos también aparecen en las primeras posiciones de los resultados de búsqueda de Google. Por ejemplo, buscando ***Mallorca***, se muestran las típicas vacaciones de lujo con las opciones de compra habituales en cualquier reserva. Por lo tanto, asegúrate de seguir nuestros consejos, sobre todo cuando reserves a través de páginas poco conocidas.

debes prestar especial atención cada vez que hagas una reserva. Computer Hoy las ha recopilado para ti en el recuadro 'Lo que debes tener en cuenta', que verás en la parte derecha.

Así te puedes defender

Si caes en una estafa de este tipo, **recopila todo lo que tengas sobre ella**: correos electrónicos, mensajes de WhatsApp, el extracto bancario con la transferencia, las páginas a las que te remitieron. Después, acude a la policía y presenta una denuncia. Si has encontrado la oferta en una plataforma de reservas, denúncialo también directamente allí.

Esto también se aplica si te has dado cuenta a tiempo de que se trata de unos estafadores y aún no has reservado. Denuncia la oferta a la plataforma y ponlo en conocimiento de la policía. ¡Así protegerás a los demás de caer en esa misma trampa!

Lo que debes tener en cuenta

Presta atención a los siguientes puntos importantes, para así poder detectar el fraude a tiempo:

- **¿Solo hay una dirección de correo electrónico o un número de teléfono móvil como contacto?** Atención: el nombre y la dirección del proveedor deben estar siempre disponibles.
- **¿El propietario no tiene todavía ninguna crítica o bien demasiadas y muy positivas?** Si hay otros detalles llamativos, debes ser escéptico.
- **¿La comunicación y, sobre todo, el pago deben realizarse fuera de la plataforma de reservas?** Corta el contacto inmediatamente.
- **¿Solo hay transferencia bancaria o servicios de envío de dinero como opción de pago?** No es seguro: si después hubiera algún tipo de problema, difícilmente recuperarías el dinero.
- **Busca en Google la dirección de la casa, y comprueba con Street View.** Si algo no coincide, no pagues nada por adelantado. Esto también se aplica si encuentras el mismo piso en otro servicio por un precio diferente y de un proveedor distinto, a través de Google. En ese caso, es probable que hayas encontrado el original, que es justo el anuncio que el estafador ha copiado.
- **Busca al propietario en Google.** Puede que encuentres quejas de otras víctimas o, incluso, información que sugiera que su historia no es cierta.
- **¿La oferta es muy barata?** Así es como los estafadores quieren hacer destacar sus anuncios.
- **¿Puedes reservar en cualquier periodo de tiempo?** Algo va mal. Los delincuentes intentan estafar así al mayor número posible de víctimas.
- **¿Un enlace te lleva de la plataforma de reservas a una web propia?** Es peligroso, sobre todo si también se supone que tienes que pagar allí.
- **¿Debes enviar una copia de tu documento de identidad?** ¡No lo hagas! Los estafadores pueden hacer aún más daño de esa manera.
- **¿Hay certificados o sellos digitales en la página?** Si es así, haz clic en ellos. Si esto te conduce a una entrada adecuada en un instituto de renombre, será una buena señal. Si el certificado o sello no está vinculado, probablemente será falso.
- **Comprueba el aviso legal de cada página.** En realidad también pueden copiarlo, pero si ves un contacto completamente diferente al de la oferta real, deberá resultarte sospechoso.

¿CÓMO PUEDEN ROBAR LAS DE ACCESO A TU BANCO?

Las credenciales bancarias representan uno de los activos más valiosos para las personas. Por su parte, obtenerlas significa para los cibercriminales tener en sus manos la llave que abre una importantísima caja fuerte virtual, y poder disponer del dinero de sus víctimas. Para hacerse con ellas, los delincuentes emplean diversas técnicas y, en caso de encontrar a usuarios desprotegidos, desprevenidos o descuidados, suelen dar sus frutos.

ESET, compañía especializada en la detección proactiva de amenazas, repasa ahora cuáles son las **cinco técnicas principales que emplean los ciberdelincuentes**. Explica también de qué manera es posible protegerse del robo de la información sensible y de todos estos ataques.

1 Sitios falsos: los estafadores emplean una URL que incluye el nombre del banco y que hasta tiene una apariencia muy similar a la web oficial. El nombre del sitio suele ser casi idéntico al que utiliza el banco en sus cuentas de Twitter e Instagram, con una mínima diferencia (puede ser a veces una única letra). De hecho, una búsqueda en Google puede llevar a estos sitios fraudulentos, que logran aparecer entre los primeros resultados de búsqueda, muchas veces en forma de anuncios.

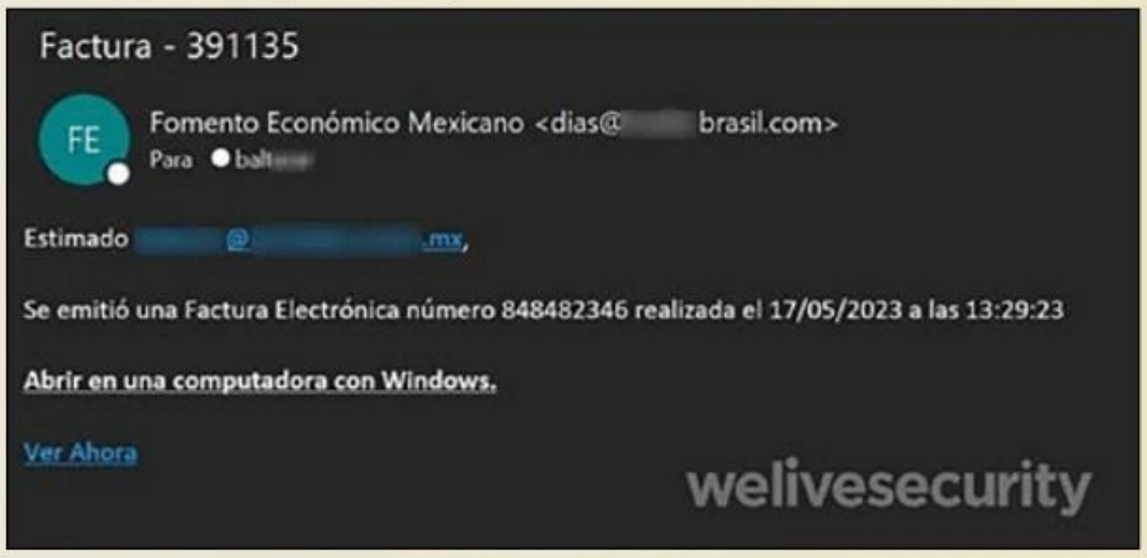
Una vez en el sitio web falso, la estética y el diseño serán idénticos a los de la página oficial. Y para acceder al supuesto homebanking (servicio bancario online), se incluirán los campos en los que las víctimas deberán ingresar las credenciales de inicio de sesión (que en realidad irán a parar a los delincuentes). Una vez que la persona introduce su nombre de usuario y contraseña, el sitio suele simular que verifica los datos entregados, cuando en realidad los cibercriminales inician sesión con las credenciales robadas en el sitio legítimo del banco. Son varios los casos de ataques a entidades bancarias, todos ellos con el objetivo de obtener las credenciales de acceso de sus clientes. En estos casos, es necesario aclarar que el banco también es una víctima, ya que se utiliza su nombre para engañar a sus clientes. De hecho, en la página oficial las entidades, se suelen compartir consejos para evitar que los usuarios caigan en distintos tipos de fraudes en su nombre.

Por otro lado, otra vía usada por los cibercriminales consiste en comprometer previamente determinados sitios web, para desde ellos obtener después las credenciales bancarias. Para ello, los delincuentes pueden explotar cualquier **vulnerabilidad que detecten en scripts o plugins** que no se encuentren actualizados, o bien aprovechar fallos de seguridad que no hayan sido descubiertos. Así, pueden incluir una redirección desde el 'sitio web víctima' hacia el 'sitio atacante', desde el cual podrán obtener las credenciales. Por otra parte, los delincuentes muchas veces crean una página apócrifa dentro del sitio web oficial, que se hace pasar por entidad. Una vez que las víctimas se encuentran dentro de estas páginas falsas, es muy probable que se les solicite introducir sus datos bancarios.

2 Malware: este ha evolucionado a pasos agigantados, de hecho se comercializan diferentes tipos de códigos maliciosos. Los troyanos bancarios, con gran presencia actualmente, han causado daños por millones de euros. Mekotio, Casbaneiro, Amavaldo o Grandoreiro son solo algunas de las familias capaces de realizar distintas acciones maliciosas, pero que destacan sobre todo por suplantar la identidad de los bancos mediante ventanas emergentes falsas, cuyo propósito es robar información sensible de las víctimas.

Hay distintas manera en las que los delincuentes pueden colocar ese tipo de malware en los equipos de sus víctimas. Por un lado, mediante correos de phishing o mensajes de texto. Pero también a través de anuncios maliciosos en un sitio web que reciba muchas visitas (ciertos códigos maliciosos se descargan automáticamente y se instalan en el equipo, apenas el usuario visita el sitio) y hasta puede estar oculto en apps móviles que simulan ser legítimas.

3 Llamadas telefónicas: dado que los estafadores son profesionales en su campo y suelen contar historias de manera muy convincente, se valen de la ingeniería social para engañar y robar información sensible, como las claves de acceso del banco. Los atacantes pueden llegar a la víctima mediante llamadas telefónicas masivas, con el único objetivo de lograr una comunicación más personal que la que se consigue a través de un correo electrónico: así la manipulación es más fácil de llevar a cabo. Como excusa de la llamada, pueden recurrir a la necesidad de tener que informar al usuario sobre **algún problema puntual relativo a la cuenta bancaria** o sobre un movimiento fraudulento asociado a la víctima. Para la supuesta resolución del problema, solicitarán información personal y, claro está, las claves de acceso a la cuenta.



Aquí se un muestra un ejemplo de un correo electrónico que contiene un enlace malicioso. Un clic en él implica la descarga el troyano Mekotio.

CLAVES

ESET, compañía dedicada a la detección de amenazas online, comparte las cinco principales técnicas que se utilizan para el robo de credenciales. Te contamos también cuáles son las prácticas recomendadas para evitar caer en la trampa.

En la imagen, se muestran varios ejemplos de cómo los cibercriminales suplantan la identidad de entidades bancarias en las redes sociales.

Una excusa utilizada para este tipo de engaños es **hacerse pasar por el servicio de atención al cliente** de un banco o entidad reconocida. De hecho, son muchas ya las entidades bancarias que advierten en su página web de este tipo de amenazas, y que brindan información útil de prevención a sus usuarios.

4 **Perfiles falsos en redes:** otra táctica común y muy eficiente es la creación de perfiles falsos en las redes sociales (Facebook, Instagram o Twitter), y desde allí llevar a cabo el engaño que termine con la obtención de las credenciales de acceso bancario de víctimas desprevenidas o desinformadas.

Existen múltiples ejemplos en Twitter e Instagram que evidencian como los estafadores siguen de cerca el empleo de ciertas palabras clave en los comentarios de los usuarios. También están muy alerta cuando estos etiquetan un perfil verificado. Se valen de la urgencia que generalmente conllevan estos mensajes (suelen ser reclamos o algún tipo de inconveniente a resolver) y, a través de estos perfiles falsos (sin marca de verificación), envían mensajes directos haciéndose pasar por la cuenta oficial del banco. Tal es así que utilizan el mismo logo y una variación del nombre oficial, y hasta ofrecen el contacto del servicio de atención al cliente o bien piden un número de contacto. Finalmente, las víctimas son contactadas por falsos representantes de atención al cliente que buscarán obtener información, como claves de acceso, tokens u otros datos, para poder acceder a sus cuentas y vaciarlas.

5 **Scraping:** este sistema se pone en marcha cuando una persona empieza a seguir la cuenta oficial de un banco en redes sociales para realizar una consulta. En ese momento, los atacantes contactan con ella por privado, de manera inmediata, haciéndose pasar por el banco en cuestión. Si la víctima responde el mensaje sin verificar (que se trata de una cuenta falsa), el supuesto asesor pedirá un número de teléfono para continuar con la consulta por esa vía. Allí utilizará toda la información disponible en las redes sociales e Internet para hacerle creer a la víctima que realmente es un colaborador del banco y que está allí para darle soporte. Una vez que la víctima toma confianza, el supuesto asesor pedirá la información bancaria, que le servirá para vaciar la cuenta.

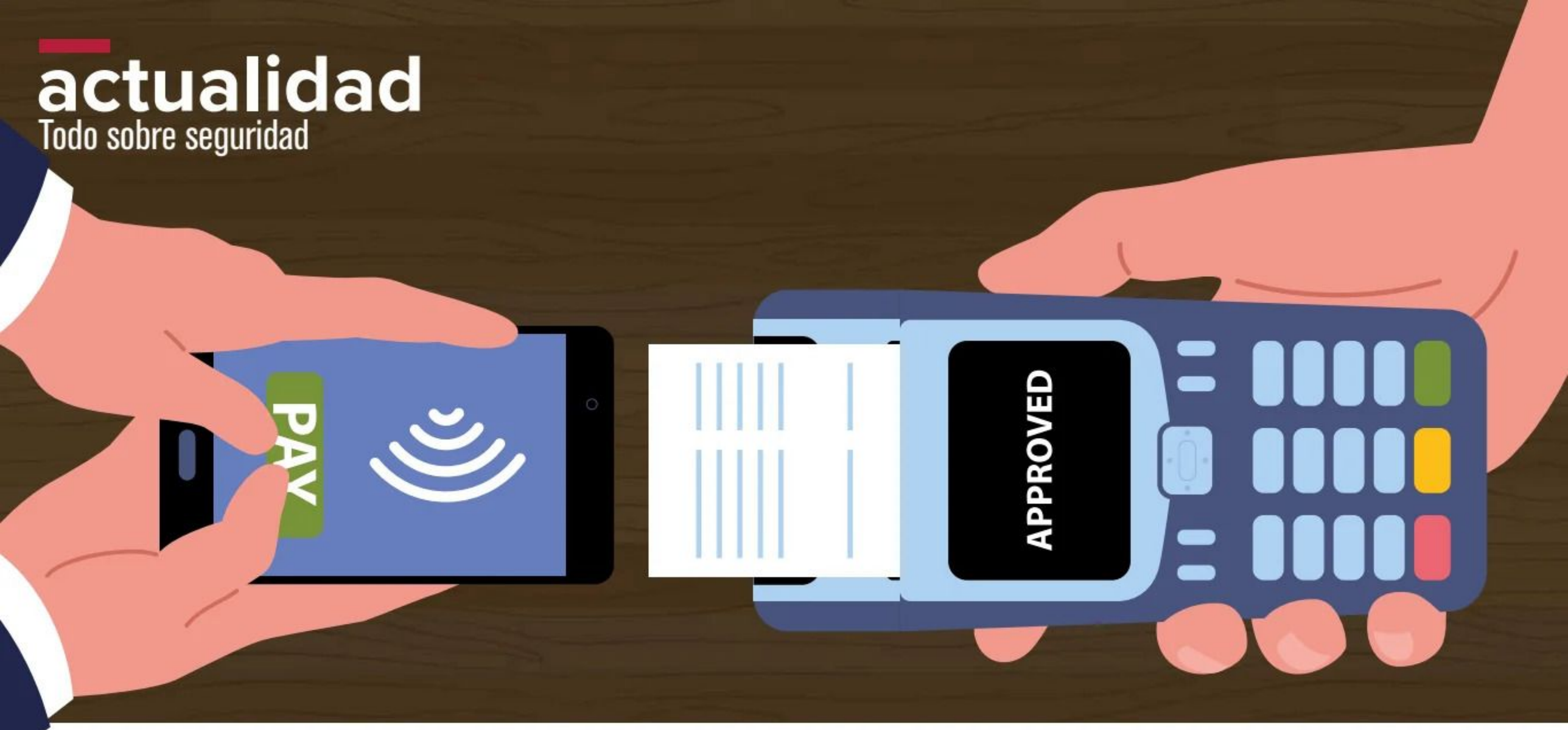
Buenas prácticas, para no ser víctima de estafas

Desde ESET comparten consejos para no caer en la trampa:

- Verificar siempre la dirección web visitada y confirmar que es la correcta.
- Comprobar que el sitio web tenga un certificado de seguridad válido, firmado por la compañía que en realidad dice ser.
- No brindar información personal o financiera, si no se cuenta con la seguridad de que **el sitio web es legítimo**.
- No divulgar ningún detalle por teléfono, incluso si la persona del otro lado suena convincente. Consultar de dónde están llamando y luego volver a contactar con esa organización para verificar. Es clave no utilizar los números de contacto proporcionados por esa persona.
- No hacer clic en enlaces ni descargar archivos de correos electrónicos, mensajes de redes sociales, mensajería instantánea (WhatsApp, Telegram) o con texto sospechoso o de remitentes desconocidos.
- Siempre utilizar software de seguridad para proteger el equipo contra el malware y otras amenazas, y mantenerlo además actualizado.
- Descargar aplicaciones de tiendas oficiales, como la App Store o Google Play.

Foto: Depositphotos.com

Sospecha si al navegar por Internet aparecen ventanas emergentes que afirman que has ganado un premio, suelen ser intentos de estafa o phishing.



Hace aproximadamente dos décadas, las tarjetas de crédito con banda magnética ya se utilizaban de forma habitual. No obstante, su seguridad era débil y el requisito de la firma complicaba a menudo las transacciones, por no mencionar que carecían de cifrado de datos, lo que las hacía **vulnerables a la sustracción y clonación** por parte de los delincuentes.

La evolución hacia las tarjetas con chip representó un avance significativo al introducir el cifrado de datos, autenticación mediante PIN y mayor seguridad en comparación con las tarjetas que solo disponían de banda magnética. Pese a que las tarjetas con chip mejoraron la seguridad al requerir autenticación, aún presentaban riesgos de clonación o robo de información, aunque el reto era ya más complejo para los delincuentes, si lo comparamos con las tarjetas únicamente magnéticas.

Frente a este panorama, la 'comunicación de campo cercano' o NFC (Near Field Communication), derivada de la **identificación por radiofrecuencia (RFID)**, surgió en los últimos años como un nuevo estándar de pago. Así, con esta tecnología, las tarjetas con chip se han vuelto aún más útiles, ya que en lugar de tener que introducirlas en los terminales de pago y en los cajeros automáticos, basta con 'tocar' un dispositivo de pago habilitado para NFC, para que se realice el pago. Y aparte de estas tarjetas sin contacto, llamadas 'contactless', ahora los móviles y otros dispositivos también pueden cumplir esta función a través de servicios especializados para ello como Apple Pay o Google Pay. Es decir, tras cargar los datos de la tarjeta en uno de los servicios anteriores, es posible utilizar el teléfono para realizar pagos.

Sin embargo, debido al corto alcance de la tecnología NFC, este método no es útil para grandes transferencias de datos. "A diferencia del WiFi o del Bluetooth, es más lento y requiere que los dos dispositivos que se comunican estén muy cerca. Esto tiene cierto parecido con las transferencias de archivos por infrarrojos del pasado, que funcionaban de forma similar, pero eran mucho menos cómodas y no funcionaban bien todas las veces. Había que ser muy preciso con la colocación de los teléfonos, y los sensores tenían que casi tocarse", explica Josep Albors, director de Investigación y Concienciación de ESET España.

¿Es segura la tecnología NFC?

Dado que su principal función es facilitar las transacciones sin contacto, cabría suponer que la tecnología NFC debería ser totalmente segura. En comparación con otros **métodos de comunicación inalámbrica,** es mucho más difícil de interceptar debido a la gran proximidad necesaria para que funcione, pero eso no significa que sea imperceptible para algunas formas de ciberataques, recuerda ESET.

Según la compañía líder en ciberseguridad, uno de los métodos de ataque más comunes cuando se trata de comunicaciones inalámbricas son los **ataques man-in-the-middle (MITM).** "Para que funcionen, tiene que haber alguna herramienta (equipo, sitio web falso, correos electrónicos) que intercepte la comunicación entre dos dispositivos/usuarios, y que luego descifre y transmita los datos necesarios al atacante. Esta es una de las razones por las que el uso de WiFi públicas puede resultar peligroso. No cuesta mucho montar un punto de acceso falso con el mismo nombre que la ubicación de una empresa/ciudad, y como la gente tiende a conectarse a ellos, un delincuente puede comprometer fácilmente la comunicación procedente de los dispositivos que utilicen esos puntos de acceso", añade Albors.

No obstante, aunque técnicamente los ataques MITM existen como amenaza en los pagos NFC, no son tan viables, explica ESET, y estas son las razones: en primer lugar, para 'burlar' la comunicación NFC, un lector tiene que acercarse bastante a la tarjeta/teléfono y así poder leer los datos necesarios. En segundo lugar, el delincuente también necesita alguna herramienta especial para hacerlo. Por otro lado, potencialmente, los terminales de pago pueden verse comprometidos. Sin embargo, a diferencia de las tarjetas normales,

Los pagos electrónicos son cada vez más habituales, por lo que el pago con el móvil también se ha popularizado así como el número de posibilidades.

LA SEGURIDAD DE LOS PAGOS NFC

PAGOS SIN CONTACTO

Los pagos sin contacto se están convirtiendo rápidamente en omnipresentes, pero ¿son más seguros que los métodos tradicionales? Abordamos la seguridad de los pagos NFC y te ofrecemos una serie de consejos para evitar los posibles riesgos al utilizar el sistema contactless.

la comunicación NFC está cifrada y tokenizada, lo que significa que una tarjeta difícilmente puede duplicarse, gracias a que su información está oculta.

La seguridad no debe darse nunca por sentada

Si bien es cierto que la tecnología NFC es segura, especialmente cuando se trata de realizar pagos, no significa que sea infalible, ya que los actores maliciosos pueden explotar fácilmente ciertas vulnerabilidades para así conseguir lo que quieren. Los fallos del sistema y los agujeros de seguridad siempre existirán, razón por la cual incluso los proveedores de seguros cibernéticos a menudo subrayan la aplicación de **parches de vulnerabilidad** como requisito para la cobertura.

Además, dado que los pagos NFC se basan intrínsecamente en la comodidad que representan para el usuario, carecen de una autenticación adicional hasta ciertas cantidades de dinero o número de transacciones (como un PIN). Algo que requeriría, por ejemplo, una tarjeta normal basada en un chip. Así, si alguien te roba la tarjeta de crédito, puede realizar pagos fraudulentos fácilmente, sin necesidad de introducir un código (hasta un determinado valor) y, en función de **los límites de pago establecidos,** las sumas pueden ser elevadas.

Por otro lado, ESET analiza la seguridad de las funciones NFC que también están presentes en los teléfonos móviles. Dado que Apple Pay, Google Pay y otros sistemas requieren seguridad añadida en forma de PIN, huella dactilar, escáner facial u otros métodos, la compañía afirma que sí que hay cierta seguridad añadida en los pagos NFC a través de smartphones. Además, ambos servicios de pago solo funcionan cuando están activados,

Hoy en día, con un reloj inteligente o smartwatch, podrás dejar la tarjeta bancaria en casa, ya que es posible pagar con él gracias a la tecnología NFC.

por lo que hay menos posibilidades de que alguien inicie un pago tuyo sin más. Por otro lado, al utilizar Apple o Google Pay, no se transmiten los datos de tu cuenta y, en caso de que pierdas el dispositivo, es bastante fácil desactivar estos servicios de forma remota.

Cómo lograr pagos sin contacto más seguros

Por último, ESET, recuerda también algunas de las principales medidas que hay que tener en cuenta para que los pagos contactless sean más seguros:

- **Prueba los bloqueadores RFID:** se trata de pequeñas fundas o carteras para tarjetas que crean una barrera entre estas y el mundo exterior, mitigando así los posibles ataques de tipo skimming.
- **Establece límites de pago bajos:** esto puede hacerse a través del banco o del software de este, y permite establecer un límite máximo sobre cuánto se puede comprar a través del sistema de pagos sin contacto.
- **Utiliza los pagos por teléfono:** aunque estas aplicaciones pueden tener sus defectos, siguen siendo un poco más seguras que las tarjetas sin contacto, gracias a los requisitos adicionales de autenticación.
- **Omite los smartwatches:** debido a su menor seguridad, habilitar los pagos en los smartwatches podría llegar a plantear problemas, dependiendo del modelo utilizado.
- **Obtén una tarjeta de transporte:** si te preocupa el tema de los pagos exprés, en la medida de lo posible, obtén una tarjeta de viaje recargable, en lugar de utilizar tu propia tarjeta de crédito/teléfono como medio de pago de los billetes. ■

Foto: Depositphotos.com

Google Pay es compatible con todos los terminales con NFC, y ya hay numerosos bancos que soportan este medio y usuarios que lo emplean.

SEGURIDAD BANCARIA

¡CUIDADO! SIM SWAPPING

El aumento de los casos de SIM swapping ha dejado al descubierto una preocupante brecha de seguridad, que afecta sobre todo a los clientes del sector bancario. Por ello, es necesario aplicar soluciones que permitan asegurar la protección de las operaciones digitales.

Los bancos podrían tener que buscar alternativas más seguras a los mensajes de texto o SMS, para así brindar una mayor protección a los clientes de sus plataformas digitales. Esta medida viene motivada por la necesidad de que las entidades bancarias ofrezcan **alternativas de autenticación de doble factor** distintas a los tradicionales mensajes en el móvil. Esto se debe a que el uso extendido de este último sistema se ha visto comprometido en numerosas ocasiones por la relativa facilidad con la que es posible obtener de forma fraudulenta duplicados de las tarjetas SIM (método conocido como SIM swapping), así como por casos de smishing, que son las estafas mediante mensajes de texto.

La digitalización de los servicios y productos bancarios es cada vez más común y, aunque continuamente estos sistemas van mejorando, también lo hacen las diferentes técnicas para delinquir. El SIM swapping, un método en crecimiento, implica que un ciberdelincuente suplanta la identidad de la víctima para conseguir el duplicado de su tarjeta SIM, permitiéndole después acceder a la información personal de esta. La vulnerabilidad es especialmente preocupante en el sector bancario, donde la exposición de los datos sensibles es una realidad cada más frecuente.

En la 'Memoria de Reclamaciones' de 2021 del Banco de España, este hecho aparece como destacado y como una novedosa técnica de delincuencia: "otro tipo de actividad delictiva, más elaborada, detectada por el DCE ha sido el duplicado de tarjeta SIM o SIM swapping". Este método creció también exponencialmente durante 2022 y, en el mes de febrero de ese mismo año, la Agencia Española de Protección de Datos inició cinco expedientes sancionadores a varias compañías de telefonía móvil, con penalizaciones de hasta 3,94 millones de euros por no haber protegido lo suficiente a sus usuarios, frente a delitos como el SIM swapping y por haber permitido el duplicado de tarjetas SIM de sus clientes sin verificar antes la identidad.

Es un hecho que los ataques informáticos cada día comprometen más la seguridad de los ciudadanos. Por ello, es importante **que los bancos puedan ofrecer herramientas** que protejan a sus clientes de ellos. "En Veritran siempre decimos que, en la industria financiera, sin seguridad no hay transacción. Por eso, estamos siempre en la búsqueda constante de soluciones innovadoras, que nos permitan asegurar la protección de las operaciones digitales sin comprometer la experiencia de usuario y la agilidad para operar", ha explicado Gabriela Giannattasio, Vicepresidenta para EMEA de Veritran.

El SIM swapping es un tipo de ataque que abre a los delincuentes las puertas de nuestras vidas, a través de la tarjeta SIM de nuestro móvil.

Pero ¿cómo funciona realmente el SIM swapping?

La palabra 'swap' en inglés significa intercambio, pero para entenderlo mejor deberíamos traducirlo como 'duplicado'. El SIM swapping consiste en obtener un duplicado de la tarjeta SIM de un teléfono móvil, para a través de ella **robarnos la identidad**.

Cuando se duplica una tarjeta SIM, la primera deja de funcionar y todas las llamadas, mensajes y línea de datos pasan al duplicado. Ahí es cuando la mayoría de las víctimas se dan cuenta de que algo no va bien y avisan a su operador de telefonía. Sin embargo, el problema es aún más grave. A través de la tarjeta SIM, los ciberdelincuentes pueden conseguir

un gran número de datos personales y hacerse con el control de redes sociales, cuentas bancarias o suscripciones de pago del usuario. Además, **al duplicar la tarjeta SIM y recibir tus SMS,** los delincuentes pueden hacer uso del sistema de autentificación en dos pasos y cambiar contraseñas o hacer movimientos en tus cuentas bancarias. Hay que recordar que un sistema de autentificación de doble factor consiste en mandar un SMS al móvil con una clave para verificar que eres tú quién pretende hacer cambios en la cuenta, pero en este caso la clave acabaría en manos de los delincuentes.

Realizar el duplicado es rápido y particularmente sencillo. Es un proceso que puedes solicitar tú mismo, pero necesitas tener algunos datos personales. En la mayoría de los casos son las propias víctimas las que facilitan sin querer esa información a los atacantes, los cuales habrán empleado técnicas de engaño.

Soluciones actuales

En cuanto a herramientas que podrían utilizarse para aumentar la seguridad de las plataformas digitales, destacan la biometría,

Foto: Depositphotos.com

Con la tecnología de biometría de huellas en tu móvil, la seguridad estará literalmente asegurada en tus propias manos. Este sistema se convertirá en uno de los mejores escudos para proteger tus datos frente a ataques externos.

el soft-token y las notificaciones push. La biometría se perfila como una tecnología prácticamente infalible, en lo que a seguridad de operaciones se refiere. Se trata de una solución que se basa en las **características físicas de las personas** y en sus patrones de comportamiento, para confirmar su autenticidad.

"De todas formas, si bien no existe un mecanismo que garantice una completa inmunidad ante el crimen cibernético, la multiplicidad de mecanismos de seguridad informática aumenta las probabilidades de combatir estas situaciones y brindar a los clientes una mayor garantía y confianza a la hora de llevar a cabo sus transacciones" ha afirmado la Vicepresidenta para EMEA de Veritran. El soft-token, por ejemplo, ofrece un método de validación adicional a través de una OTP (One Time Password) o contraseña de un solo uso, que intensifica los niveles de protección de los usuarios a la hora de autorizar el uso o acceso a su cuenta mediante el dispositivo verificado. Y, por último, las notificaciones push pueden facilitar un nuevo control al usuario, ya que solicitan su aprobación por medio de notificaciones en la misma app. A la vez, informan en tiempo real de los movimientos relativos a la actividad en las cuentas o tarjetas. Todo ello con la intención de advertir sobre posibles fraudes o usos no autorizados del dinero de una persona.

La seguridad es uno de los temas más relevantes para las entidades bancarias. Estas deben continuar trabajando activamente, para proteger a los usuarios y asegurarles una mejor y más segura experiencia de uso de sus plataformas digitales. ■

LAS LIMITACIONES DE LA AUTENTICACIÓN EN DOS PASOS

El inicio de sesión con la autenticación en dos pasos se considera un sistema seguro. Sin embargo, los hackers se saben trucos para burlar esta protección. Te explicamos cómo protegerte.

Para proteger cuentas online, ya no es suficiente con el simple uso de contraseñas. Esto es algo que ya sabemos todos y la solución es la autenticación de dos factores (2FA, también denominada como de dos pasos o de doble factor), que lo que hace es introducir en la ecuación **un segundo dispositivo para confirmar el inicio de sesión**. Pero incluso este sistema de seguridad tiene sus limitaciones. Los hackers son capaces de saltarse este mecanismo mediante trucos muy refinados y secuestrar cuentas e identidades digitales. Computer Hoy te aclara ahora cómo actúan los ciberdelincuentes y qué puedes hacer para protegerte de ellos.

¡El segundo factor es realmente importante!

Aunque existen trucos para burlar la autenticación 2FA, esto no quiere decir que debas renunciar a proteger tu cuenta con este sistema de doble verificación. De hecho, es muy recomendable aplicarlo. Por ejemplo, puedes utilizar la aplicación Authenticator de Microsoft para poder **legitimarte a través del sistema** de autenticación de dos factores. Una alternativa a esto son las Passkeys, un nuevo método de autenticación que no requiere el uso de contraseñas y que se basa en la criptografía asimétrica.

Ayuda en caso de emergencia

Si se diera el caso de que una persona no autorizada consiguiera hacerse con una de tus cuentas, siempre deberás actuar con rapidez. Entre otras cosas, intenta cambiar la contraseña, revisa actividad sospechosa y otras cuentas vinculadas, y contacta con el soporte del servicio.

EL SUPUESTO **MÓVIL PERDIDO**

Los hackers llaman a las líneas de soporte técnico y se hacen pasar por personas de las cuales ya han conseguido sus datos de acceso, por ejemplo, en la Darknet. Los delincuentes alegan entonces que han perdido el smartphone que utilizan para realizar la doble autenticación 2FA. Es poco probable que un equipo de soporte bien entrenado caiga en este tipo de trampas, pero de vez en cuando sucede. Si el departamento informático o el servicio de soporte restablece la autenticación 2FA, los atacantes podrán hacerse entonces con el control de las cuentas.

Cómo protegerse

Los departamentos de TI no tienen forma de controlar los despistes de su personal, pero por suerte estas situaciones raramente ocurren en la actualidad, y los nuevos vínculos de autenticación 2FA se suelen activar mediante códigos que se envían por correo. En cualquier caso, los delincuentes intentan sacar provecho de esta vía si ya tienen en sus manos el primer factor, es decir, la contraseña. Recuerda por tanto aplicar para la autenticación en dos pasos (2FA) las mismas reglas de seguridad que aplicas para tu contraseña, que deberá ser compleja e incluir números y caracteres especiales.

*****

SECUESTRO DE LA **TARJETA SIM**

En este supuesto los atacantes copian los datos de tu tarjeta SIM y con ellos generan una nueva SIM. Posteriormente la insertan en su propio smartphone e intentan engañar al proveedor de telefonía móvil haciéndole creer que son el cliente y que simplemente han cambiado de móvil. Si el truco da resultado, las nuevas peticiones de confirmación para la autenticación ya no llegarán a las víctimas, sino a los delincuentes. Esto unido a los datos de acceso conseguidos previamente podría darles acceso a la cuenta bancaria, por poner un ejemplo. ¿Parece algo complicado? De hecho lo es, ya que los atacantes necesitan tener bastantes conocimientos, buenos contactos y equipo. A los delincuentes solamente les trae a cuenta llevar a cabo este tipo de ataques si hay mucho dinero en juego que se pueda sustraer a las víctimas, o bien si se trata de políticos de nivel o personajes famosos. Sin embargo, estas dificultades implícitas no conllevan que no se utilice esta técnica delictiva: en el año 2022, el grupo Lapsus$ utilizó este tipo de ataque.

Cómo protegerse

Salvaguarda tu tarjeta SIM. Para poder llevar a cabo este tipo de ataque, los delincuentes tienen que hacerse previamente con ella de alguna forma y colocarla en un lector de tarjetas para duplicarla. Esto podría suceder, por ejemplo, si entregas tu móvil para hacer una reparación rápida o bien tienes que depositarlo en algún sitio. Lo mejor es extraer previamente la tarjeta SIM antes de entregar el smartphone. Si los atacantes tuvieran suficiente información sobre ti, podrían solicitar una tarjeta SIM completamente nueva. Esta información la recopilan de antemano mediante tácticas de phishing, llamadas falsas de asistencia, malware instalado en el smartphone y a través de las redes sociales.

DUDOSO **INTERMEDIARIO**

La estafa más peligrosa: los hackers atraen a sus víctimas mediante un correo electrónico convincente para acceder en un sitio web falso con el aspecto de Microsoft. Allí solicitan al usuario su nombre y contraseña. Estas entradas se registran y se introducen en segundo plano y de forma invisible para la víctima en la página de inicio de sesión real. Si a continuación se realiza una petición de autenticación de tipo 2FA, los delincuentes la redirigen a los usuarios. Estos introducen su código como de costumbre, y los atacantes ya tienen acceso a la cuenta. Este tipo de engaño lo suelen usar grandes grupos de hackers para robar cuentas de Microsoft. El ataque funciona de forma automática y es aterradoramente efectivo cuando se lleva a cabo de manera masiva.

Cómo protegerse

Puesto que en este caso los datos de acceso reales los introducen las propias víctimas directamente, el uso de un software antivirus es la única opción viable que proporciona protección. Este software es capaz de reconocer los sitios falsos y advertir del peligro. Para mejorar la seguridad, siempre debería comprobarse la dirección en la que se introducen los datos de inicio de sesión.

LA ESTAFA DEL **ADMINISTRADOR**

Para este método de engaño, los atacantes han tenido que robar previamente los datos de acceso correctos, es decir, el nombre de usuario, la contraseña y el número de teléfono de la víctima. En caso de que los delincuentes quieren hacer uso de esos datos, el sistema de autenticación de dos factores (2FA) entrará en acción y solicitará un código o una confirmación en el smartphone. Los atacantes basan el éxito de su ataque en la ingenuidad y confianza de la víctima, y simplemente la llaman por teléfono. Estos se hacen pasar por un empleado del departamento de administración o de servicio de soporte y te cuentan una historia aparentemente creíble, como por ejemplo que van a enviar, por protocolo de seguridad, un código al móvil de la víctima para que luego esta lo confirme de viva voz durante la llamada. La víctima colabora en el propio engaño sin ser consciente de ello.

Cómo protegerse

En este caso el primer factor de la autenticación, es decir, la contraseña, es la mejor protección. Si usas un gestor de contraseñas recibirás una advertencia en caso de que la contraseña aparezca en la Darknet. Cámbiala de inmediato y el ataque ya no funcionará. Aun así, se debe desconfiar siempre de cualquier llamada imprevista del personal de TI o de los administradores. Cuando las llamadas son legítimas, se suele comunicar con antelación que van a realizarse. Como regla general: los administradores auténticos no necesitan tus datos de acceso. Por este motivo, no facilites ningún dato de acceso ni confirmes ningún mensaje de autenticación en dos pasos (2FA) si no es para tu propio inicio de sesión.

PRUEBA UN **GESTOR DE CONTRASEÑAS**

Usar un gestor de contraseñas es cómodo y práctico de cara a proteger las contraseñas. Descubre cuál es el mejor y qué debes tener en cuenta en la página 58 de este número.

PASSKEYS: EL FINAL DE LAS CONTRASEÑAS

¿Has olvidado tu contraseña? Pues este tipo de percances pronto será historia. Passkeys hace que los inicios de sesión sean mucho más seguros y sencillos. Te hablamos de ello.

¡Nombre de usuario y contraseña, por favor! Si introduces ambos correctamente, obtendrás acceso a sitios web, aplicaciones y servicios online. Esto ha sido una práctica común durante años, aunque a veces también es la causa de muchas frustraciones y molestias. Porque cualquiera que se tome en serio las normas básicas de seguridad tiene que recordar montones de contraseñas complejas o utilizar un gestor de estas, que a menudo hay que pagar, o incluso convivir con el peligro constante de ser **una posible víctima del ataque de los hackers**. Sin embargo, todo eso puede cambiar pronto: FIDO y Passkey son las palabras mágicas. Te hablamos de lo que representan realmente.

¿Qué es FIDO?

La Fast Identity Online (FIDO) es una alianza de cientos de empresas de todo el mundo. Entre ellas hay auténticos pesos pesados del sector tecnológico: además de Google, Apple, Microsoft y Samsung, también son miembros Visa, PayPal, Mastercard y Amazon. La alianza se fundó en 2013 con el claro objetivo de facilitar y hacer más seguro el inicio de sesión en los distintos servicios de Internet. Y ya era hora: diez años después de su fundación, es obvio que el inicio de sesión tradicional ya no logra su objetivo.

En tiempos de IA y ordenadores de alto rendimiento, incluso las contraseñas más complejas son fáciles de adivinar con ataques de fuerza bruta. Por eso, los bancos hace tiempo que dejaron de utilizar barreras tan vulnerables. Hoy en día, nada funciona en las transacciones financieras sin una acreditación adicional (autenticación de doble factor). Por otro lado, muchos proveedores utilizan sus propias soluciones. Así que lo mejor sería poder disponer de procedimientos uniformes, que se utilizaran para el mayor número posible de servicios. Y FIDO quiere conseguirlo con el sistema Passkeys.

¿Cómo funciona Passkeys?

El procedimiento de inicio de sesión FIDO utiliza métodos de cifrado estándar de una forma especialmente fácil de usar, para así permitir inicios de sesión seguros: en la vida cotidiana, el usuario solo tiene que indicar a un sitio web o a una aplicación que desea iniciar sesión y confirmarlo, por ejemplo desde su móvil. Y, para ello, **ya no se necesitará una contraseña**.

> Tengo que utilizar la función ‘contraseña olvidada’ con demasiada frecuencia.
>
> **Dirk General-Kuchel**
> Redactor

No tan nuevo

¿Te suena familiar? Posiblemente, porque las aplicaciones que emplean el software Authenticator ya utilizan este procedimiento. Y esta misma tecnología también la emplean algunos servicios de Internet: si quieres iniciar sesión, tienes que confirmarlo con la aplicación Google o Microsoft Authenticator.

No todos los gigantes tecnológicos han integrado la función Passkey con tanta claridad como en el caso de Google. Sin embargo, debería implantarse en unos meses.

Pero incluso este, ya de por sí sencillo procedimiento, se está volviendo aún más fácil. Google, Microsoft y Apple están integrando firmemente la tecnología Passkey en sus sistemas operativos. El usuario se registra como antes en un servicio de Internet e introduce todos los datos necesarios. Pero en lugar de una contraseña, **el sitio genera un par de claves**. Una parte de esta clave se almacena en el servidor de inicio de sesión, y la clave privada solo en el ordenador del usuario, ya sea en la aplicación correspondiente o directamente en el sistema operativo.

Si más tarde quieres volver a iniciar sesión, comenzará un interesante proceso en segundo plano: el sitio web envía una especie de cálculo a tu ordenador o smartphone. Tu dispositivo calcula automáticamente el resultado y lo firma digitalmente con su clave privada. El paquete vuelve al sitio web. Y, con la firma, el servicio de Internet ya puede estar seguro de que realmente has recibido y resuelto la consulta. Tu identidad ya está debidamente demostrada.

Suena complicado, pero en realidad no lo es para ti. Tú solo ves un aviso de confirmación en tu smartphone y lo verificas con tu huella dactilar, PIN o Face ID. De todo lo demás, se encarga el sistema operativo en segundo plano. Ya no tienes que preocuparte por nada más.

Vamos avanzando

Google ya ha incorporado la tecnología correspondiente en el sistema operativo Android. En Apple, funciona con iOS 17 y con MacOS Sonoma, que acaba de salir al mercado. A Microsoft le llevará un poco más de tiempo, aunque Passkey ya está disponible en una versión preliminar de Windows 11 del canal de desarrolladores. Pasarán unos meses antes de que esté disponible para todo el mundo. Sin embargo, la mayoría de los usuarios probablemente lo usarán en sus móviles, porque ya se puede usar Passkeys en ellos.

La única condición: el servicio o sitio web debe ofrecer el servicio. Pero muchos proveedores ya lo hacen. En el cuadro de la derecha, puedes ver cuáles son.

Sencillo y seguro

En la práctica, este nuevo sistema solo ofrece ventajas: por fin se acabaron las contraseñas complicadas y los programas para gestionarlas. Además, las nuevas claves ya no se podrán robar tan fácilmente, ya que siempre se necesitan las dos partes para iniciar sesión.

De esta forma, si un hacker se hace con la clave pública por una circunstancia desafortunada, no tendrá la privada. E, incluso si la consigue, **el atacante seguirá sin saber para qué sirve**. Es más, no contará con el smartphone que la acompaña.

Fácilmente recuperable

Parece que esta tecnología se está poniendo de moda: en el futuro, cada vez más cuentas se pasarán a Passkeys. El modo exacto dependerá del proveedor.

Además, como las claves de acceso se almacenan en las cuentas de usuario de Apple, Microsoft y Google, se pueden recuperar. Así que no tendrás que temer por tus accesos si pierdes, cambias o dañas tu móvil.

Foto: Depositphotos.com

LOS GIGANTES TECNOLÓGICOS Y LA APLICACIÓN DE PASSKEYS

La tecnología Passkeys ya funcionan para muchos servicios de Internet. Sin embargo, en algunos de ellos hay que activar este sistema primero. Computer Hoy ha echado un vistazo a Google y Microsoft.

- **Google:** en la página de Google **g.co/passkeys**, encontrarás información sobre cómo registrarte. El proceso se completa en cuestión de minutos. Una vez implementado, podrás iniciar sesión con la aplicación Google Authenticator, por ejemplo. Si lo prefieres, también puedes configurar Passkey en tu ordenador o portátil y autenticarte en el futuro, por ejemplo, mediante huella dactilar o cámara.
- **Microsoft:** cualquiera que quiera acceder a su correo o a OneDrive ya puede utilizar Passkeys. Las instrucciones de Microsoft son todavía muy confusas, y hay que instalar la app Microsoft Authenticator en el móvil. Te aconsejamos que esperes a que la función esté integrada en Windows 11.
- **Otras empresas conocidas que ofrecen el servicio o lo introducirán pronto:** PayPal, WhatsApp, Apple, Nintendo y X (Twitter).

TU HUELLA DACTILAR Y TU CARA

LA CODICIADA MONEDA DEL MERCADO NEGRO DE LA DARK WEB

Los datos biométricos son extremadamente difíciles de replicar o falsificar, lo que los convierte en un apreciado activo para los ciberdelincuentes, quienes pueden aprovecharlos en tu contra.

La autenticación biométrica, como **escanear tu cara** para **desbloquear el móvil** o usar la huella dactilar para acceder a la app de tu banco, se está promocionando como una forma totalmente segura de proteger tus datos personales. Sin embargo, investigadores de la empresa NordVPN han descubierto que más de 81.000 huellas dactilares comprometidas se encuentran disponibles en foros clandestinos de ciberdelincuentes, lo que deja claro que este sistema **no es tan seguro como parece**. Adrianus Warmenhoven, experto en ciberseguridad de NordVPN, señala que si bien los datos biométricos son más fiables que las contraseñas, cambiar una que se considere comprometida es posible. Sin embargo, cambiar tu cara, tu

Foto: Depositphotos.com

Foto: Depositphotos.com

En los últimos años, las contraseñas biométricas han evolucionado y permiten utilizar partes de nuestro cuerpo, como la retira o las huellas dactilares.

huella digital o incluso la voz es una historia diferente.

Las amenazas a los datos biométricos están en alza. Las técnicas más recientes, como la tecnología deepfake, se utilizan para explotar los datos de los usuarios en las redes sociales y **crear identificaciones falsas**, como caras y huellas dactilares, que luego se filtran en la Dark Web.

Si los datos caen en manos equivocadas, estás perdido...

"En el mercado ilegal, los datos biométricos son posiblemente los más codiciados, ya que no son fáciles de conseguir, y ahora con la IA pueden explotarse mejor", explica para Computer Hoy David Marqués Díaz, Head of Operations de Advens Iberia.

Esta información robada puede utilizarse, en primer lugar, para la suplantación de identidad y el fraude. Los delincuentes pueden utilizar estos datos para acceder de manera fraudulenta a cuentas bancarias, dispositivos, sistemas de seguridad y otros servicios protegidos mediante autenticación biométrica. Pero el gran problema de todo esto es que una filtración de este tipo puede perdurar en el tiempo, ya que estos datos son únicos y difíciles de cambiar. A diferencia de las contraseñas o el número de la tarjeta de crédito (que puedes cambiarlos por otros si ocurre algo), tu huella y tu cara son inherentemente personales y permanentes. Esto significa que, tras su filtración, las víctimas pueden enfrentarse a un riesgo continuo de explotación y abuso. Lo que resulta muy jugoso para los delincuentes.

Y cuando nos adentramos en el ámbito de los deepfakes y otros contenidos falsificados mediante IA, la situación se torna aún más preocupante. Se pueden aprovechar **imágenes y vídeos generados artificialmente** para engañar a las personas, incluso **manipulando a los familiares de la víctima** con un vídeo que aparentemente muestre el rostro de esta. "Actualmente, diría que el dato biométrico más valioso es la voz, ya que con la ayuda de las herramientas IA de clonación de voz puede ser usado para múltiples fraudes", añade también el entrevistado.

Foto: Depositphotos.com

Los lectores de huellas dactilares para el reconocimiento biométrico son cada vez más comunes en una gran variedad de dispositivos, como cerraduras.

Una vez que las huellas dactilares se han visto comprometidas, cambiarlas o reemplazarlas resulta algo imposible

Este tipo de datos es una mercancía muy rentable en el mercado negro, donde los criminales pueden venderlos a precios elevados o utilizarlos para obtener ganancias ilícitas. Además, con tan solo obtener la huella, el amplio acceso que esta da a cientos de aplicaciones la convierte en un activo muy tentador y valioso que los delincuentes están dispuestos a obtener como sea. Teniendo todo esto en cuenta, es evidente que las empresas y organizaciones encargadas de proteger los datos biométricos de los usuarios se enfrentan a un desafío considerable. Por ello, resulta crucial que estas entidades establezcan medidas de seguridad robustas para nuestra protección. Además, antes cualquier problema grave, deben estar preparadas para ofrecer una respuesta rápida y efectiva.

Muchas jurisdicciones tienen regulaciones específicas sobre la recopilación, almacenamiento y uso de datos biométricos, como el **Reglamento General de Protección de Datos** (GDPR) en la Unión Europea, y es importante que cumplan con estas normativas.

¿CÓMO FUNCIONAN LOS SISTEMA BIOMÉTRICOS?

Estos métodos se basan en la adquisición y análisis de la información biométrica, para así realizar una comparación entre los datos recopilados y los almacenados en una base de datos previa. El proceso de reconocimiento incluye los siguientes pasos:

1 Toma de datos biométricos: se recopilan las características físicas o de comportamiento de una persona, como su huella dactilar o su patrón facial. Para ello, se usan dispositivos específicos como escáneres de huellas dactilares, cámaras o lectores de iris.

2 Extracción de características: los datos obtenidos se analizan para así obtener las características únicas y relevantes de cada individuo. Estas se convierten en una representación digital, que también es conocida como plantilla biométrica.

3 Comparación y coincidencia: la plantilla biométrica generada se compara con las plantillas almacenadas en una base de datos preexistente, para así encontrar una posible coincidencia.

4 Verificación o identificación: en función del uso concreto que vaya dársele, la biometría puede utilizarse para verificar la identidad de un individuo (es decir, para confirmar si coincide con los datos almacenados previamente) o para realizar una identificación (para buscar una coincidencia en la base de datos y determinar la identidad de una persona que es desconocida).

ANÁLISIS DE TU HUELLA DIGITAL

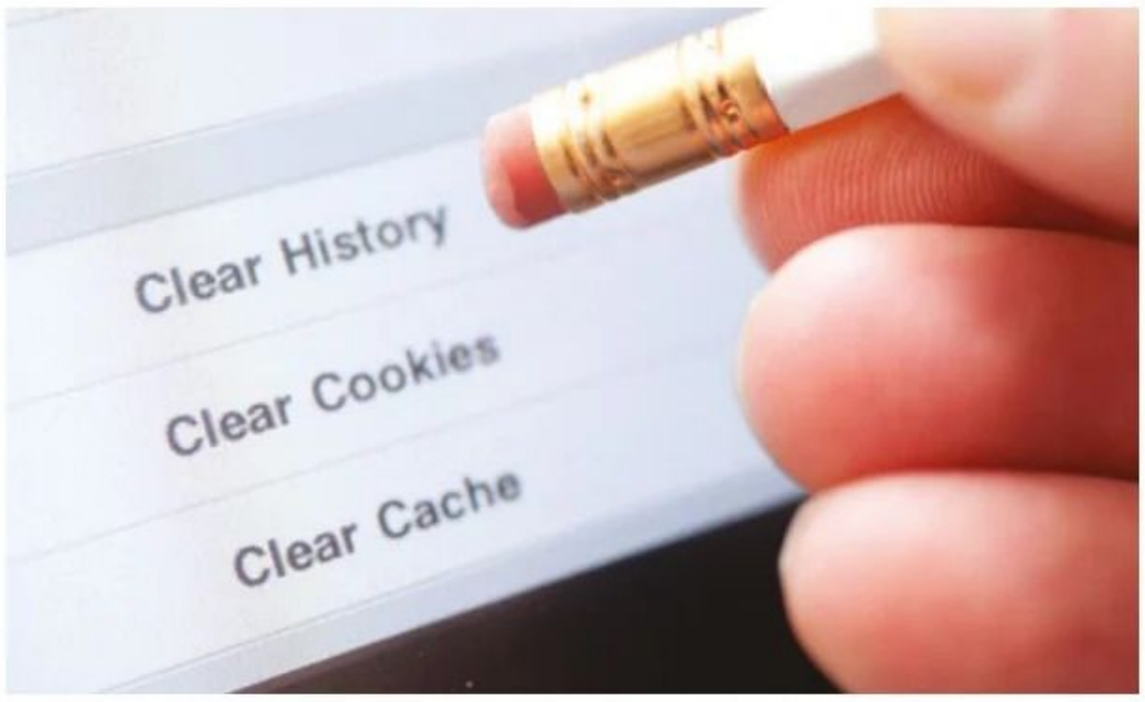
¿POR QUÉ ES CASI IMPOSIBLE DESAPARECER DE INTERNET?

Desaparecer por completo de la Red es una tarea sumamente complicada y desafiante. A medida que nuestra vida digital se va cohesionando con nuestro día a día, también se van generando una gran cantidad de datos y rastros digitales, de manera casi incontrolable.

Cada vez que llevas a cabo una tarea online, ya sea buscar en Maps una ubicación, comprar un móvil nuevo o, incluso, hacer un comentario o publicar algo en tus redes sociales, dejas una huella digital; **un rastro de ti mismo** en el inmenso universo de Internet.

Para la mayoría de las personas, esto es una consecuencia lógica e inevitable de la comodidad de tener Internet y de mantenerse conectado. Sin embargo, para otros usuarios más preocupados por su seguridad, la idea de que todo lo que hagan quede registrado en Internet es algo que les preocupa bastante.

"Toda esa información que vuelcas se ha replicado y almacenado en múltiples servidores y plataformas. Incluso si decides eliminar el contenido original, las copias almacenadas en otros lugares persisten. Esto se debe a que **los datos se copian, respaldan y almacenan** en múltiples ubicaciones para asegurarse de que estén disponibles y accesibles", explica para Computer Hoy Félix Llorente García, SAP Project Manager.



Borrar con regularidad el historial del navegador, la caché y las cookies en todo tus dispositivos te ayudará a mantener y mejorar tu privacidad.

La naturaleza de Internet hace que eliminar todos los rastros digitales sea una tarea casi imposible. "Parece muy sencillo, pero todo lo que pongas ahí fuera, no esperes nunca que vuelva a ser privado", explica Sandra Matz, investigadora de medios sociales y profesora de la Columbia Business School para la CNN. "Retirar algo de Internet, darle al botón de reinicio, es casi imposible".

Factores que dificultan el borrado completo

Según explican los expertos en privacidad, **los motores de búsqueda almacenan copias** de las páginas web y de los contenido en sus índices. Esto implica que, aunque la elimines de forma activa, tu información podrá seguir apareciendo en los resultados de búsqueda durante cierto tiempo.

Por otro lado, la interconexión de los servicios online también dificulta la eliminación completa de la huella digital, ya que las actividades realizadas en las diversas plataformas **pueden estar vinculadas, a través de información compartida** como direcciones de correo electrónico o datos de inicio de sesión.

Otro desafío importante consiste en la propagación de los datos. Una vez que compartes información online, es muy difícil controlar cómo se difunde y comparte esta. Por ejemplo, pueden existir copias guardadas en dispositivos de otras personas, capturas de pantalla realizadas por otros usuarios o archivos compartidos en diversas plataformas. "Incluso si eliminas el contenido original, estas copias van a seguir ahí", añade el experto.

Y los metadatos asociados a los archivos digitales (una simple fotografía) también pueden proporcionar información personal y seguir almacenados, incluso si se elimina el contenido original. Revelando así detalles como la fecha, la ubicación o información relativa a la creación o modificación del fichero.

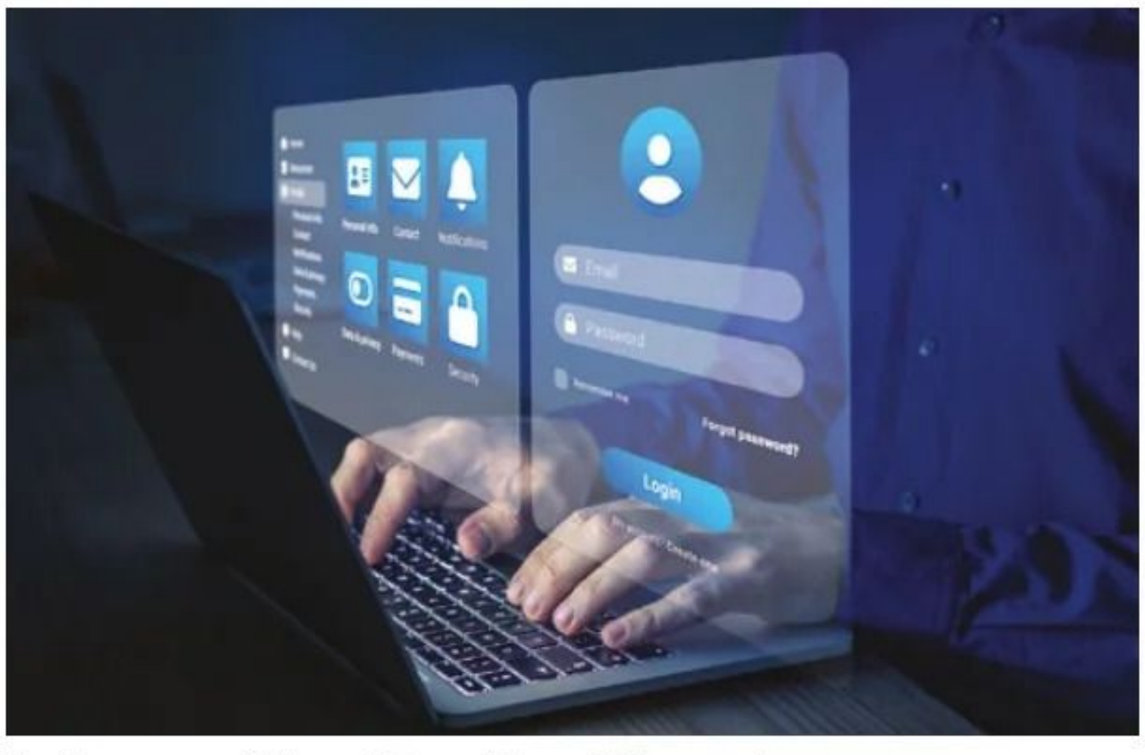
Consejos útiles para proteger tu huella digital

"Aunque es posible tomar medidas para reducir la exposición en línea y proteger la privacidad, eliminar todos los rastros digitales por completo es todo un desafío debido a la naturaleza misma de Internet y la forma en que los datos se mueven", añade Félix Llorente García. "Pero no es necesario tener miedo. Se pueden tomar medidas para controlar y gestionarlos", añade. Aquí tienes algunos consejos:

- **Evita compartir muchos datos** en cualquier sitio web, redes sociales o foros públicos. No compartas información que pueda vincularse a ti como la dirección de tu casa, tu número de móvil o incluso tu fecha de nacimiento (a menos que sea necesario, claro).
- Cuando te registres en un servicio online que requiera información personal (como puede ser Twitter, Instagram o incluso TikTok), utiliza una dirección de correo electrónico alternativa y un seudónimo en el caso de tu perfil.
- Cuando recurras a Internet, procura usar un navegador privado o una VPN, para de este modo lograr evitar que los servicios de terceros puedan rastrear tu actividad.
- Elimina también todos los datos almacenados en tu dispositivo con regularidad: borra el historial del navegador, la caché y las cookies.

"Asume que todo lo que publicas puede ser utilizado por cualquier persona, y vivirá a perpetuidad", sentencia Sandra Matz. "Se consciente de lo que compartes en línea y evalúa si es necesario o **si podría comprometer tu privacidad"**, sentencia el experto entrevistado. ¿Lo vas a tener en cuenta a partir de ahora?

Tener un perfil en la Red es tan fácil como colgar nuestra foto en Facebook o Twitter. Eso es suficiente para que ya tengamos nuestra propia huella digital.



Nadie escapa a Internet. Es casi imposible encontrar una persona que no tenga un yo virtual y que no sea parte integrante del universo de la Red.

¡MI HIJO QUIERE UN MÓVIL!

¿CÓMO LIDIAN LOS PADRES CON EL PRIMER TELÉFONO DE SUS HIJOS?

Los expertos de Qustodio han elaborado una guía para padres, sobre cómo educar a sus hijos en un uso correcto del teléfono móvil. Un primer dispositivo puede abrir la puerta a ciertos peligros, como por ejemplo la adicción o el acceso a contenido inapropiado.

Muchos centros educativos se empiezan a plantear limitar el uso del teléfono móvil a los estudiantes. La relación de los menores con la tecnología empieza a edades cada vez más tempranas. Según UNICEF, la edad media en la que los niños disponen de su primer móvil es antes de cumplir 11 años. Así, siendo habitual que muchos menores reciban su primer smartphones en el último ciclo de primaria, muchas familias se preocupan por el uso que pueden hacer sus hijos de estos dispositivos tecnológicos, además de plantearse **cuándo es apropiado regalárselo.** De hecho, el último estudio 'De Alpha a Zeta, educando a las generaciones digitales' de Qustodio, plataforma especializada en seguridad digital para familias, revela que los jóvenes pasan una media de 4 h diarias conectados.

Y teniendo en cuenta que el primer dispositivo puede abrir la puerta a ciertos peligros como la adicción o el acceso a

La relación de los menores con la tecnología empieza a edades cada vez más tempranas. Según UNICEF, la edad media en la que los niños disponen de su primer móvil es antes de cumplir 11 años.

A pesar de que se ha hablado mucho sobre el uso indebido de Internet de niños y adolescentes, prohibir la tecnología nunca es la opción adecuada.

contenido inapropiado, los expertos de Qustodio han elaborado una guía para las familias, sobre cómo educar a sus hijos en el uso apropiado del móvil:

- **Cómo hacer un uso correcto:** está claro que no se puede evitar el acceso al móvil completamente, ya que forma parte de la vida social. Por ello, es fundamental, sobre todo cuanto más pequeños son, que conozcan cómo utilizarlo de manera correcta, sabiendo qué compartir, con quién hablar, dónde buscar información... la educación digital es esencial cuando se empieza a utilizar cualquier dispositivo.
- **Establecer unos horarios:** para poder tener control sobre el tiempo y el uso que los menores dan al móvil, es importante establecer una rutina que evite el exceso. Es cierto que la tecnología es beneficiosa, pero hay que saber usarla con moderación y estableciendo un orden, sobre todo, a edades tan tempranas.
- **Dar ejemplo:** si los niños ven a sus padres constantemente con el móvil, acabarán cogiendo el mismo hábito. El ejemplo es uno de los mejores instrumentos con que cuentan las familias para educar a sus hijos. Los padres enseñan a través del ejemplo y los niños aprender a través de la imitación.
- **Plantear alternativas:** hay una gran cantidad de opciones para evitar el uso del teléfono cuando uno se aburre. Pueden buscar actividades que les gusten sin necesidad de estar constantemente frente a una pantalla: hacer deporte, dibujar, aprender a tocar algún instrumento... las posibilidades están dentro de los intereses de cada niño.
- **Compartir los espacios:** estar en la habitación solo y con el móvil es el mejor contexto para pasarse horas frente a la pantalla. Por esta misma razón, los expertos recomiendan compartir espacio con los más pequeños, y que estos hagan uso del móvil con más gente alrededor, para así tener más compañía que la de la pantalla. También, quitarles el móvil antes de dormir ayudará a mejorar su sueño y evitará que pasen más horas conectados.

Las familias han de involucrarse activamente en la vida digital de sus hijos y aprender sobre las aplicaciones, plataformas y redes sociales que usan, para de este modo poder entender sus normas de uso.

Eduardo Cruz, CEO de la compañía Qustodio, reconoce que "es inevitable que los niños acaben teniendo su primer móvil, es parte de su vida social y los avances tecnológicos favorecen a ello. Prohibirlos no es la solución, hay que saber cómo integrarlos de manera moderada y que ellos mismos sepan que **el uso excesivo acaba siendo perjudicial**. Por eso, recomendamos a los padres que se sienten y hablen con sus hijos de todos los peligros y beneficios que un uso moderado del teléfono puede acarrear".

Cuando los niños se conectan a Internet, pueden encontrarse con pornografía. ¿Cómo deben afrontarlo los padres y qué protección existe?

El pasado 6 de febrero, se celebró el Día de Internet Segura. Esta jornada de acción fue lanzada por la Unión Europea en 2008 y tiene como objetivo sensibilizar a niños, jóvenes, profesores y padres sobre los peligros de Internet. Aunque con algo de retraso, en 2024 los organizadores han abordado por fin un importante tema tabú: ¡el porno! En estas páginas, te contamos por qué esto nos concierne directamente a todos.

Un contacto con el porno cada vez más precoz

Estadísticamente, en España los niños entran en **contacto por primera vez con la pornografía entre los 9 y los 11 años**. Y esto ocurre a una escala que la mayoría de los padres no pueden imaginar, ya que ninguno lo ha experimentado en carne propia. Mientras que los padres a menudo veían por primera vez fotos de desnudos en revistas, los jóvenes de hoy en día tienen que enfrentarse a 'deep nudes' (porno generado por inteligencia artificial protagonizado por famosos), 'dickpics' (fotos no solicitadas de genitales masculinos) o, incluso, a la visión de prácticas sexuales inusuales. Y todo esto puede tener un efecto perturbador en muchos niños y jóvenes.

Por esta razón es tan importante que nosotros, como padres, hablemos con nuestros hijos y les expliquemos de qué se

MENORES Y PELIGROS EN LA RED

PORNO EN

APPS DE PROTECCIÓN

Existen aplicaciones de control parental para Windows, macOS, Android e iOS. Estas apps, por ejemplo Norton Family (ver imagen), ofrecen filtros de contenido, cuotas de tiempo, informes sobre la actividad online de los niños, localización con historial, zonas seguras (alarmas para los padres, si los niños las abandonan) y muchas otras características útiles. Es recomendable tener instalada una aplicación de este tipo en el teléfono móvil o PC de tus hijos. Explícales qué hace exactamente la aplicación y por qué tienen sentido las normas. Puedes ajustarlas en cualquier momento y permitir excepciones.

trata y cómo deben afrontarlo. Aunque estas **conversaciones no sean fáciles** y los niños intenten a menudo bloquearlas, es importante que los menores se den cuenta de que las representaciones en Internet son a menudo exageradas y tienen poco que ver con la realidad. También ayuda que los pequeños sepan cómo defenderse de la pornografía forzada y que puedan hablar de ello abiertamente. En la columna de la derecha, encontrarás consejos para afrontar este tipo de conversaciones.

Cómo proteger a tu hijo en la era digital en la que vivimos

Para los niños pequeños en particular, encontrarás disponibles **programas y aplicaciones de control parental** como Norton Family (ver cuadro superior). Este tipo de software permite bloquear contenidos pornográficos y otros igualmente inapropiados. Estas aplicaciones también ofrecen otras funciones que resultan verdaderamente útiles para los padres, como restricciones de tiempo, funciones de localización y mucho más.

¿Por fin se está actuando?

Ya hay acontecimientos políticos en curso: la UE obliga a los operadores de sitios porno a introducir restricciones de edad más estrictas en 2024 (véase más abajo). Sin embargo, por desgracia, esto no es muy eficaz. La normativa solo afecta a los sitios web con más de 45 millones de usuarios al mes.

El contacto es inevitable

Independientemente de todas estas medidas o incluso aunque mantuvieses a tu hijo alejado de los dispositivos con acceso online, no se podría evitar la exposición a la pornografía. Los niños encontrarán formas de eludir los bloqueos, podrán acceder a dispositivos sin restricciones o tendrán amigos que les compartan esos contenidos. Por ello, es tan importante hablar con ellos. Si en algún momento tu hijo sufre acoso sexual en su entorno escolar, por ejemplo a través de 'dickpics', podrás encontrar **ayuda y asesoramiento gratuitos** llamando al teléfono 900 018 018 o en el chat cifrado y confidencial de la fundación ANAR, **www.anar.org**.

El Gobierno toma las riendas

Los datos han disparado la alarma y España ha querido ir más allá de las medidas europeas (por el momento insuficientes), para restringir la edad de acceso a las plataformas de pornografía (véase recuadro inferior).

Entre las medidas españolas, la Agencia Española de Protección de Datos (AEPD) presentará este verano una **herramienta de verificación de edad** más eficaz. Además, el Ministerio de Juventud e Infancia ha anunciado la creación de un plan que proteja a los menores de estos riesgos. Esta batalla es muy necesaria y no ha hecho más que empezar.

RESTRICCIÓN DE EDAD: ¿UNA MEDIDA EFICAZ?

La UE ha obligado a Pornhub, Xvideos y Stripchat, entre otros, a establecer restricciones de edad efectivas antes de que termine este mes. Sin embargo, los portales ya han anunciado que no cumplirán con estas medidas, por lo que es probable que sean bloqueados. Aunque se trata de un paso en la buena dirección, seguramente tendrá poco efecto. Es improbable que los visitantes quieran verificar su identidad por videoconferencia y lo más fácil es que migren a otros sitios, ya que la normativa solo afecta a aquellas webs con 45 millones o más de usuarios al mes. Hay alternativas más que suficientes que habrá que considerar.

CONSEJOS PARA EL DIÁLOGO

Sin castigos

Deja claro a tu hijo que no le vas a castigar si acude a ti en busca de ayuda sobre contenidos pornográficos, aunque haya incumplido las normas antes de llegar a la situación problemática. Y muy importante: ¡cúmplelo! Solo así te asegurarás de que el niño acuda de verdad si algo va mal. Muestra interés al escucharle y pregunta a tu hijo lo que piensa y siente.

Explica la realidad

En el porno, las mujeres siempre tienen ganas, las hermanastras siempre están interesadas en el sexo, los hombres casi siempre son dominantes y las mujeres son objetos reducidos al sexo. Explica al niño que esto es una escenificación y que la realidad es diferente.

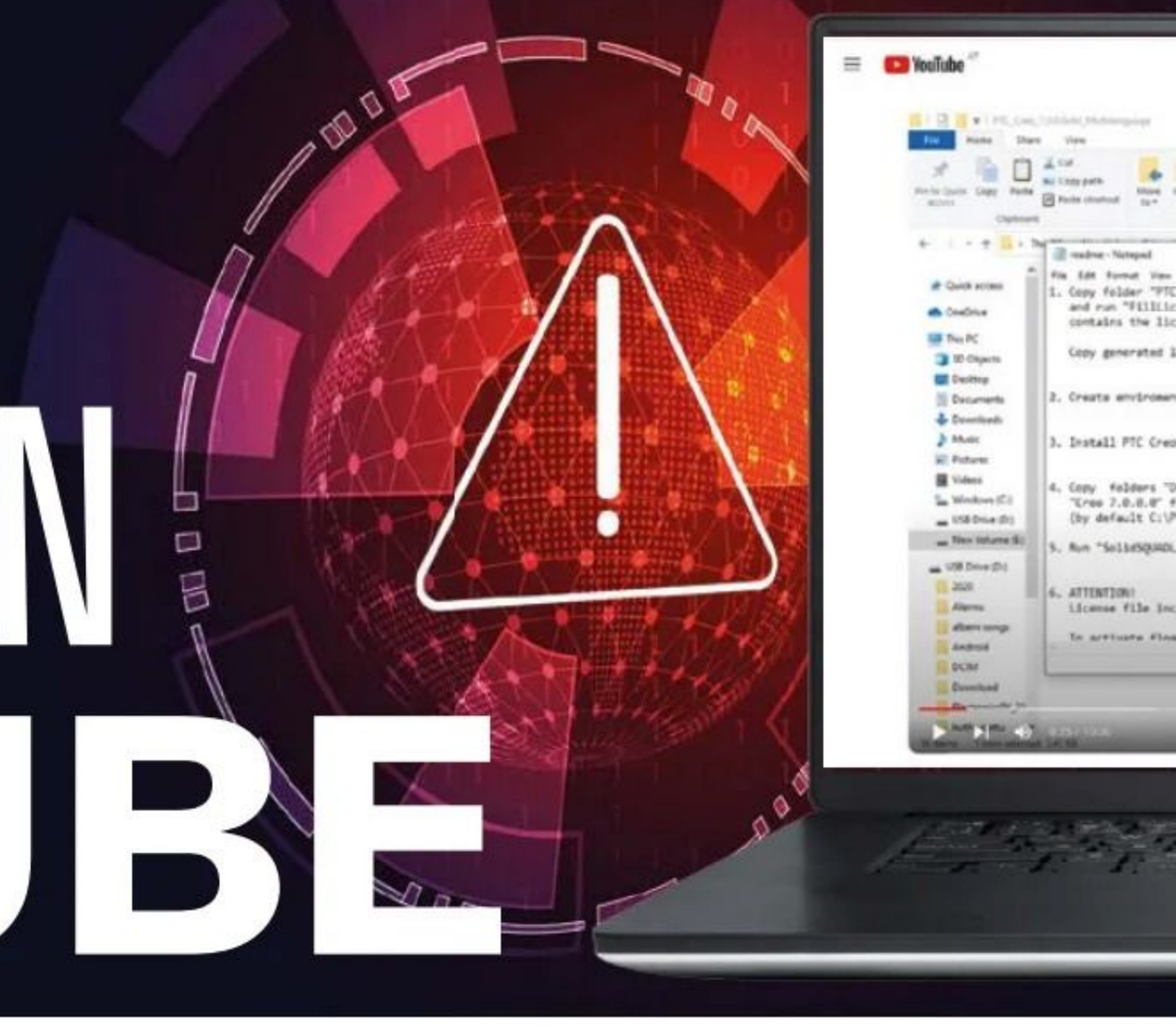
Anticipa cualquier señal de acoso

Las niñas, en particular, se enfrentan muy a menudo al acoso, incluso en juegos o aplicaciones y mensajes que tienen lugar en entornos supuestamente inofensivos. Explica a tu hijo o hija que debe acudir a ti en esos casos y que entonces podréis tomar medidas juntos, como denunciar el delito o denunciar cuentas de usuario. Háblales también de peligros como los pedófilos.

Fotografías de desnudos

Los compañeros de colegio de tu hijo podrían pedirle fotos íntimas o en las que esté desnudo. Explícale que nunca debe hacerlas o compartirlas, por mucha confianza que tenga con quien se las ha pedido. A menudo, las fotos no tardan en circular por el colegio y perseguirán a tu hijo para siempre.

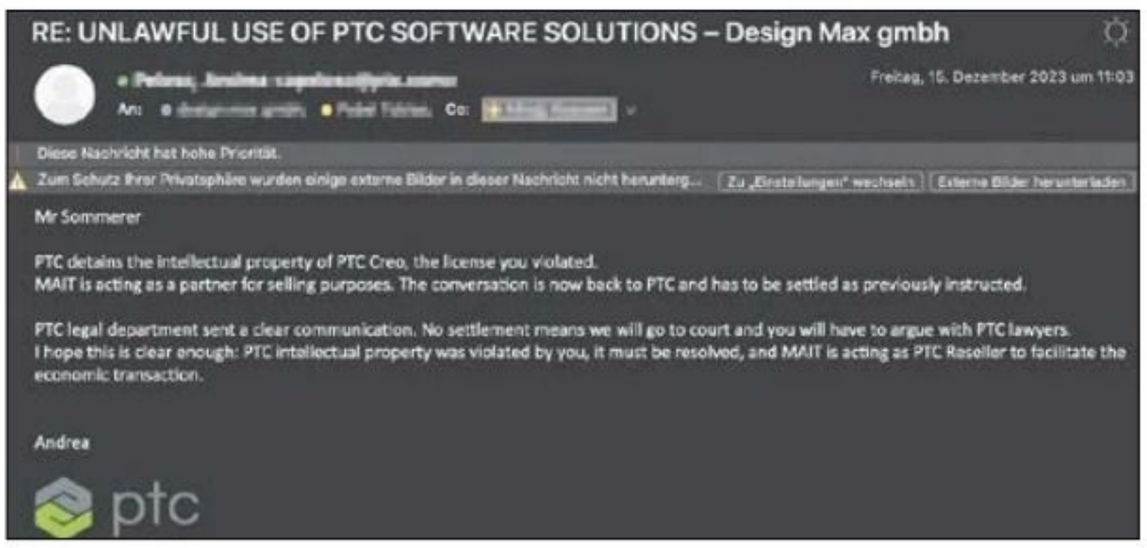
PELIGRO EN YOUTUBE



¿Descargar software bueno y gratis? Si te encuentras estos cantos de sirena en YouTube, deberías desconfiar.

Cómo puedo montar un armario? ¿Cómo reparo mi lavadora? Hoy en día, es muy sencillo encontrar tutoriales en YouTube para hacer todo tipo de cosas. Max Sommerer, propietario de una pequeña empresa en Austria, aprendió a la fuerza que **seguir consejos equivocados puede ser peligroso** y, además, salirte muy caro.

La disputa comenzó a finales de 2023, cuando el proveedor de software PTC se puso en contacto con Sommerer: el programa de diseño 3D 'Creo' de PTC llevaba usándose más de 16 meses sin su correspondiente licencia, en uno de los ordenadores de la empresa. Así sucedieron los acontecimientos: un joven empleado de Sommerer quería usar el programa y lo había descargado a través de un enlace que se incluía en un vídeo de YouTube. Conocía este software de la academia técnica local, en la que los estudiantes lo usaban de forma gratuita. PTC reclamó a Max Sommerer la friolera de 210.000 €, en concepto de compensación por tener un empleado usando el programa Creo sin una licencia en vigor. Sommerer quedó aterrado y se puso en contacto con un abogado. Este aceptó el caso y pudo ayudarle: a pesar de todo ello, Sommerer tuvo que hacer frente al pago de 5.000 € por el uso del software. Y dado que PTC llegó a un acuerdo extrajudicial para reclamar el pago de 12.000 €, Sommerer también tuvo que afrontar una sanción por importe de 7.000 €. Además, tuvo que negociar un contrato con PTC para adquirir una licencia del software Creo durante un periodo de dos años. Coste: 3.750 € por año.



Este es un fragmento del correo electrónico que Max Sommerer recibió de la empresa PTC. El tono es sorprendentemente elevado.

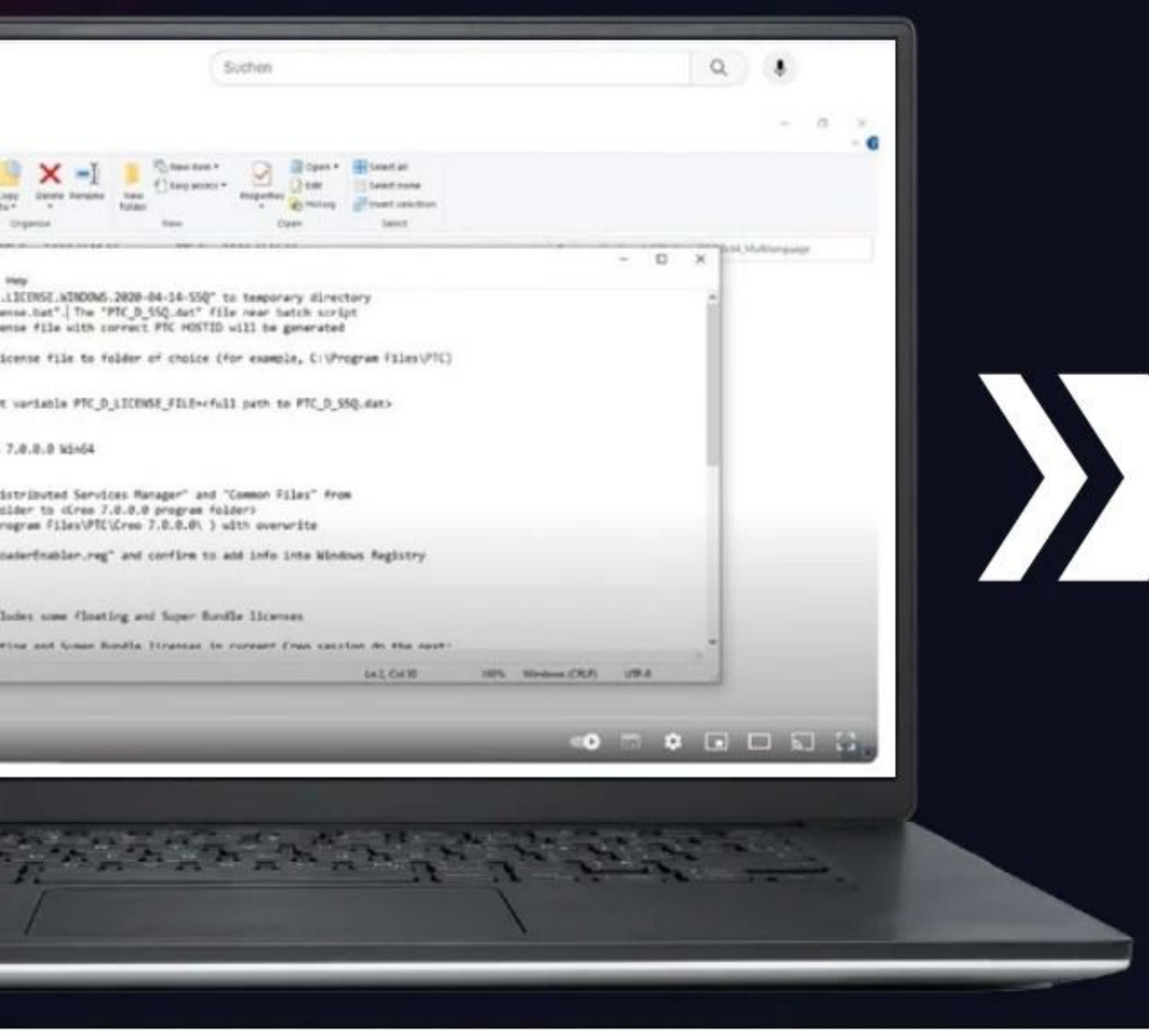
Un vídeo y muchas preguntas

Sommerer se comunicó con nuestros compañeros de Computer Bild, y el equipo editorial le solicitó por escrito a PTC que explicara su posición. En el mensaje también se incluía el enlace al vídeo de YouTube con el que el empleado de Sommerers cayó en la trampa de la licencia. Sospechoso: poco después de que Computer Bild realizara su comunicación, ya no se podía visualizar el vídeo de YouTUbe. La plataforma mostraba: "Este vídeo ya no está disponible debido a una reclamación por violación de derechos de autor de PTC Inc". En otras palabras: las indicaciones del vídeo mostraban una forma ilegal de activar el software. **El vídeo estuvo en línea durante dos años y medio**: se subió el 22 de septiembre de 2021, y cuando se eliminó había alcanzado más de 16.000 visitas. Esto supone que PTC era conocedor de la existencia de este extraño vídeo desde mucho antes: dentro del contexto del conflicto, PTC remitió a Max Sommerer a un representante legal de la empresa austriaca. Sommerer le envió un correo electrónico con fecha del 30 de noviembre de 2023, en el que le advertía de la existencia del vídeo y del enlace al mismo. Pero ¿cómo es que no se eliminó el vídeo hasta que llegó la comunicación de Computer Bild? ¿No tendría que haber actuado PTC ya en aquel primer momento?

El comportamiento de PTC es cuestionable

Max Sommerer tampoco comprende por qué la empresa PTC habría dejado pasar tanto tiempo antes de dirigirse a él para reclamarle una cantidad tan elevada. Preguntado por Computer Bild, PTC no dio ninguna respuesta que dejara las cosas claras. Las cuestiones de la piratería de software son complejas. Y como cada supuesto es único, la detección y el acuerdo o solución final son diferentes en cada caso, declaró la empresa. ¿Con qué frecuencia se dan casos en PTC como el de Max Sommerer? El proveedor de software tampoco pudo dar una respuesta concreta a esta otra pregunta.

Computer Bild conversó también con un confidente que deseaba permanecer en el ano-



Todo esto es bastante sospechoso: aunque Max Sommerer advirtió a PTC sobre la existencia del vídeo en YouTube, este fue eliminado únicamente cuando Computer Bild llevo a cabo su consulta.

nimato. Este les aseguró que se había enterado por mediación de una persona dentro de la empresa, de que PTC obtiene ahora más ingresos con la persecución de infracciones de derechos de autor que con las ventas regulares. De todas formas, en la redacción no disponen de pruebas que puedan respaldar esta afirmación.

¿Víctima de una conducta comercial reprochable?

La pregunta clave sigue siendo la siguiente: ¿por qué la empresa esperó 16 meses para reclamar a Sommerer una sanción tan elevada? ¿Acaso se esconde detrás de todo esto una **práctica comercial cuestionable**? En Internet no hemos encontrado ningún indicio de ello.

Preguntamos también al abogado especializado en derecho digital Christian Solmecke.

> Dadas sus posibilidades a nivel técnico, PTC podría haber respondido más rápidamente

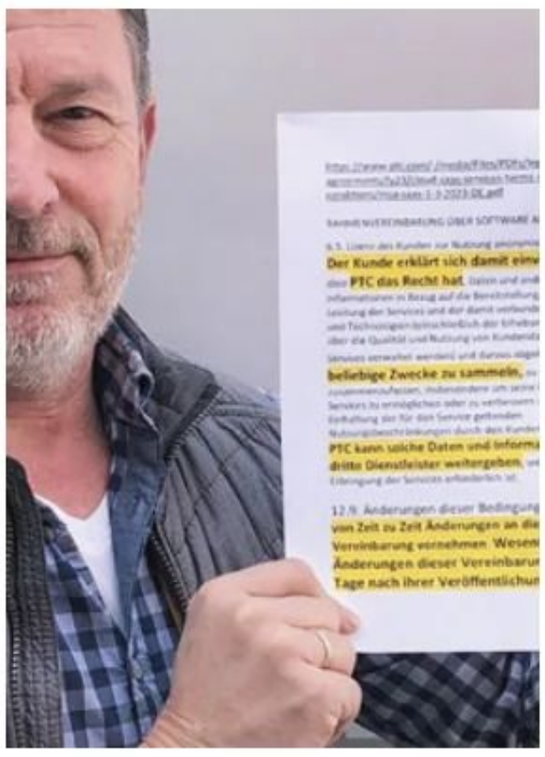
Christian Solmecke
Abogado especializado en derecho digital

Christian cree que PTC podría haber reaccionado con mayor celeridad para reconocer la infracción de la licencia, dada su capacidad técnica (recuadro a la derecha). Por esta misma razón, pudiera parecer que el largo periodo de tiempo esperado tendría una naturaleza meramente táctica, que les permitiría reclamar posteriormente una indemnización mucho mayor.

No obstante, el despacho de abogados de Solmecke, WBS, tiene conocimiento de la aplicación de este tipo de prácticas en otras empresas de software. Por ejemplo, Solmecke posee algunos clientes que han recibido reclamaciones por daños y perjuicios inusualmente elevadas de la empresa Allplan.

Disfrutar, pero con cautela

Max Sommerer contactó con Computer Bild porque quería advertir a otros del peligro a través de su historia. No es posible demostrar que PTC haya dilatado la espera más de lo normal, pero sin duda resulta más que sospechoso. ¿Por qué motivo PTC no eliminó el vídeo justamente después de que Sommerer informara al representante austriaco de PTC? ¿Es este proveedor de software uno de los artífices de una práctica cuestionable bien conocida ya por el despacho de abogados WBS?



Max Sommerer se encuentra indignado: la controversia con PTC ya le ha costado mucho dinero.

Lo que queda bastante claro es que se deben tomar precauciones a la hora de descargar software a través de enlaces mostrados en vídeos de YouTube. No es raro encontrar indicaciones e instrucciones para activar software de manera ilegal, y a tenor de los a menudo elevados costes por llevar a cabo la compra legal, es una situación que desgraciadamente tiene bastante aceptación entre el público. A pesar de todo, aquel que lo haga, **se arriesga a sufrir muchos problemas**, que a veces pueden llegar pasados muchos meses después de iniciar su uso. En algunos casos, los problemas pueden producirse incluso 16 meses después.

¿CÓMO SIGUEN LOS FABRICANTES EL **RASTRO**?

Historias como estas hacen que surja inmediatamente la pregunta: ¿cómo hacen los fabricantes de software para rastrear el uso ilegal de su software?
En la actualidad, prácticamente todos los programas se conectan a los servidores web del fabricante. Esto suele producirse cuando se instala e inicia el software, pero también en otras ocasiones con independencia de su uso. El objetivo de estas conexiones es, por un lado, comprobar si existen posibles actualizaciones pendientes del programa, y por otro, hacer una validación de la licencia. En cualquiera de los casos: el usuario deja rastros durante este proceso, como por ejemplo la dirección IP o una 'huella digital' específica del ordenador. Estos 'datos telemétricos' con frecuencia son analizados por empresas especializadas, para así detectar usos indebidos. Esto es precisamente lo que ocurrió en el caso del software Creo aquí descrito.

SMART TV
¿Sistema operativo actualizado? ¿Son tus contraseñas seguras?

PROTEGE BIEN TU SMARTHOME

TENABLE: HACKERS PROFESIONALES

Tenable es una empresa de seguridad con sede en Columbia, Maryland, en los Estados Unidos. Esta compañía está especializada en detectar y eliminar vulnerabilidades de seguridad, y asesora a otras empresas sobre cómo proteger sus sistemas contra ataques de piratas informáticos. Tenable es también el fabricante del escáner de vulnerabilidades Nessus, que utilizamos en nuestro experimento. Nessus ofrece varios escaneos personalizables y enumera todos los dispositivos y vulnerabilidades encontrados en una red. También puede realizar análisis desde dentro y fuera, simulando lo que vería un atacante que aún no está en el sistema y lo que ve una vez que ha accedido. Puedes encontrar una versión de prueba de Nessus en **es-la.tenable.com**. Sin embargo, el software solo está disponible en inglés y es difícil de entender para los usuarios no expertos. No obstante, si estás más familiarizado con los temas de seguridad, puedes utilizar el programa para recrear el experimento de Computer Hoy y escanear tu propia red doméstica.

Lo que hace unos años sonaba a ciencia ficción, ya se ha convertido en realidad en muchos hogares españoles: dispositivos y ayudantes cotidianos como **cerraduras de puertas, robots aspiradores, televisores inteligentes u asistentes de voz**, que están conectados directa o indirectamente a Internet y que se comunican entre sí y con la Red. Pero ¿hasta qué punto esto es seguro? ¿Puede un extraño controlarlo todo a distancia e, incluso, abrir la 'puerta' y acceder al sistema?

Una vez más, Computer Hoy ha querido comprobarlo y ha puesto en marcha un interesante experimento junto con la empresa de ciberseguridad Tenable (ver recuadro a la izquierda): ¿conseguirá el experto en seguridad de Tenable acceder a la red doméstica de uno de nuestros redactores?

La meta ideal

Nuestro redactor, como no podía ser de otro forma, es un apasionado de la tecnología. Él y su familia utilizan numerosos dispositivos inteligentes. Esto convierte su red doméstica en un objetivo muy atractivo para los hackers. Matthias Fraunhofer, SE Manager Central Europe de Tenable, le echó un vistazo de cerca a esta. Equipó una Raspberry PI con **la última versión del software Nessus** (ver recuadro a la izquierda) y la utilizó para escanear durante horas la red de casa de nuestro redactor, todo ello con el fin de identificar vulnerabilidades de seguridad.

Los peligros

Además del uso de contraseñas de fábrica que no son seguras, las vulnerabilidades de seguridad del software de los dispositivos inteligentes son la ma-

LÁMPARAS INTELIGENTES
¿Utilizas contraseñas seguras?

Cada vez más dispositivos inteligentes conquistan nuestros hogares. Pero con la tecnología también llega el peligro: las vulnerabilidades de seguridad pueden favorecen los ataques desde el exterior. Computer Hoy te explica cómo protegerte.

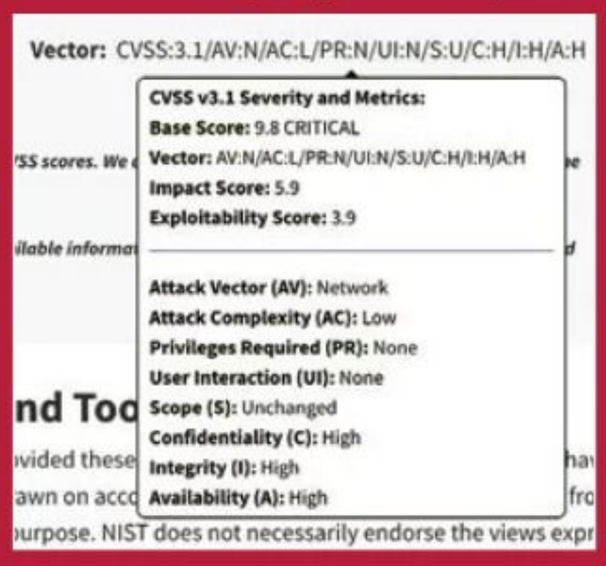
yor amenaza. Con herramientas como Nessus, los posibles atacantes pueden ver rápidamente qué dispositivos y con qué software están activos en la red. Una rápida comprobación en Internet le muestra directamente al atacante a qué vulnerabilidades de seguridad son susceptibles esos dispositivos. Y **en los foros de hackers**, también pueden encontrar exploits listos para usarse. Estos son pequeños programas maliciosos que aprovechan las brechas y dan así acceso a los atacantes, sin mucho esfuerzo.

Un experto 'decepcionado'

Tras la prueba, Matthias Fraunhofer se mostró algo decepcionado. Solo encontró dos vulnerabilidades de seguridad críticas en la red. Una en el NAS de Synology, que se debía a una actualización que faltaba y podía solucionarse rápidamente, y otra en las lámparas inteligentes. Aunque esta segunda brecha no puede cerrarse, tampoco hay malware para ella. Por lo tanto, el experto en seguridad calificó la red del redactor de inusualmente segura. Sin embargo, la prueba práctica tuvo un pequeño punto débil: nuestro redactor está especialmente familiarizado con los problemas de seguridad. Por ello, actualiza regularmente su red, cambia sus contraseñas, cierra las posibles vías de ataque y apaga los dispositivos que no utiliza. En los hogares españoles, este enfoque es más la excepción que la regla. Por experiencia, Computer Hoy y Matthias Fraunhofer pueden llegar a afirmar que, para la mayoría de los particulares, la situación es bastante diferente y **existen innumerables lagunas de seguridad**.

¿CUÁLES SON LAS **VULNERABILIDADES DE SEGURIDAD** DEL SOFTWARE?

Las vulnerabilidades de seguridad del software son una constante del mundo digital. Por ejemplo, recientemente ha habido muchos informes sobre la vulnerabilidad de seguridad Move-it, que ha causado filtraciones de datos en Deutsche Bank, Postbank, Shell, BBC, British Airways y muchas otras empresas. Para los profanos, no siempre está claro de qué se trata exactamente. Y si quieres saber más, necesitas el llamado número CVE de la vulnerabilidad de seguridad. Si lo buscas en Google, encontrarás una entrada en el National Institute of Standards and Technology. Además de una descripción y otros enlaces, también contiene un 'Base Score', que indica el nivel de peligrosidad de la vulnerabilidad (10 es la más peligrosa). También hay un 'vector', que contiene información importante. El vector de vulnerabilidad de Move-it es: ***CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H***. Esto significa que el ataque funciona a través de la red, no es especialmente complejo, no requiere derechos ni interacción del usuario, no puede extenderse a otros dispositivos, tiene un alto impacto en la estabilidad y confidencialidad del sistema, y los correspondientes exploits (programas maliciosos o malware) son fáciles de obtener. Puedes ver toda esta información pasando el ratón por encima de ***Vector*** al lado de la vulnerabilidad (imagen inferior).



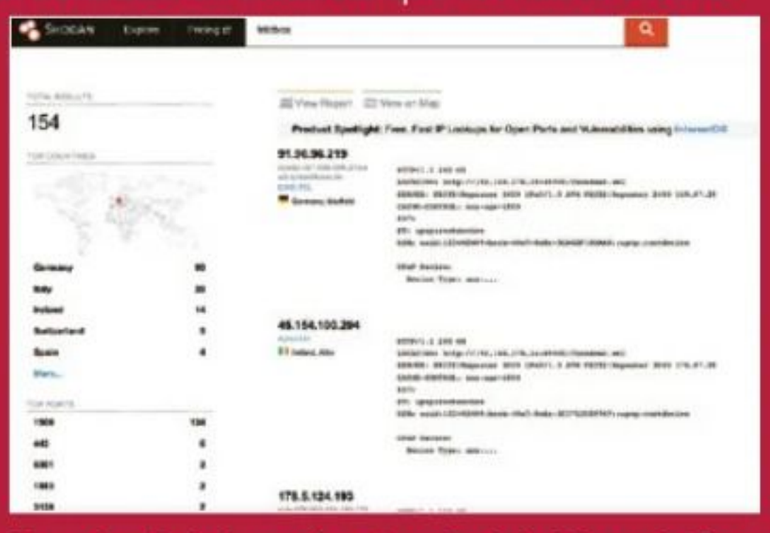
PORTÁTIL
¿Tienes actualizado Windows y el software? ¿Dispones de antivirus? ¿Empleas contraseñas seguras?

CÁMARA DE VIGILANCIA
¿Tiene acceso desde Internet? ¿El firmware está actualizado?

ROBOT SEGADORA
¿Firmware actualizado? ¿Empleas contraseñas seguras?

SHODAN: BUSCADOR PARA HACKERS

Shodan.io es un sitio web en el que se pueden buscar dispositivos conectados a Internet. Los resultados también contienen la dirección IP con la que se puede acceder al hardware. Basta con introducir esa dirección en el navegador, para acceder a los dispositivos. Los sistemas bien protegidos requieren una contraseña. Sin embargo, muchos usuarios no utilizan una contraseña segura o solo emplean contraseñas estándar que los hackers conocen. La dirección IP también puede utilizarse para lanzar ataques contra las vulnerabilidades de seguridad. Este motor de búsqueda es popular entre los piratas informáticos, porque facilita la búsqueda de objetivos.



Una simple búsqueda a través del sitio web Shodan localizó más de 100 routers FRITZ!Box.

¿Son realistas los ataques?

Es poco probable que alguien vaya a tu casa e intente piratear tus dispositivos. Las vulnerabilidades de seguridad que solo pueden explotarse localmente son las menos críticas. La única excepción son las relacionadas con las cerraduras inteligentes. Si se pueden vencer, es bastante probable que los ladrones puedan acceder. Por lo tanto, has de tener especial cuidado en este caso.

Sin embargo, los piratas informáticos no tienen por qué situarse en la puerta de tu casa para encontrar un dispositivo desprotegido. **El sitio web Shodan puede utilizarse para buscar específicamente dispositivos** inteligentes que estén conectados a Internet. Podrían ser accesos online a routers o a los datos de las cámaras de vigilancia (ver recuadro a la izquierda).

Ademas, si un atacante consigue acceder a la red, el resto de vulnerabilidades que pueden explotarse localmente también vuelven a ser relevantes. Por ejemplo, sería posible **hackear el SmartTV y atacar desde ahí el disco duro del router o el NAS**. Los datos capturados y el acceso a documentos u otra información podrían utilizarse entonces para causar más estragos.

Así te proteges

En las siguientes páginas, encontrarás los consejos y trucos más importantes, para que tu red sea más segura. Así nadie podrá acceder a ella fácilmente.

ASÍ ASEGURAS TUS DISPOSITIVOS

1 SOBREMESAS Y PORTÁTILES

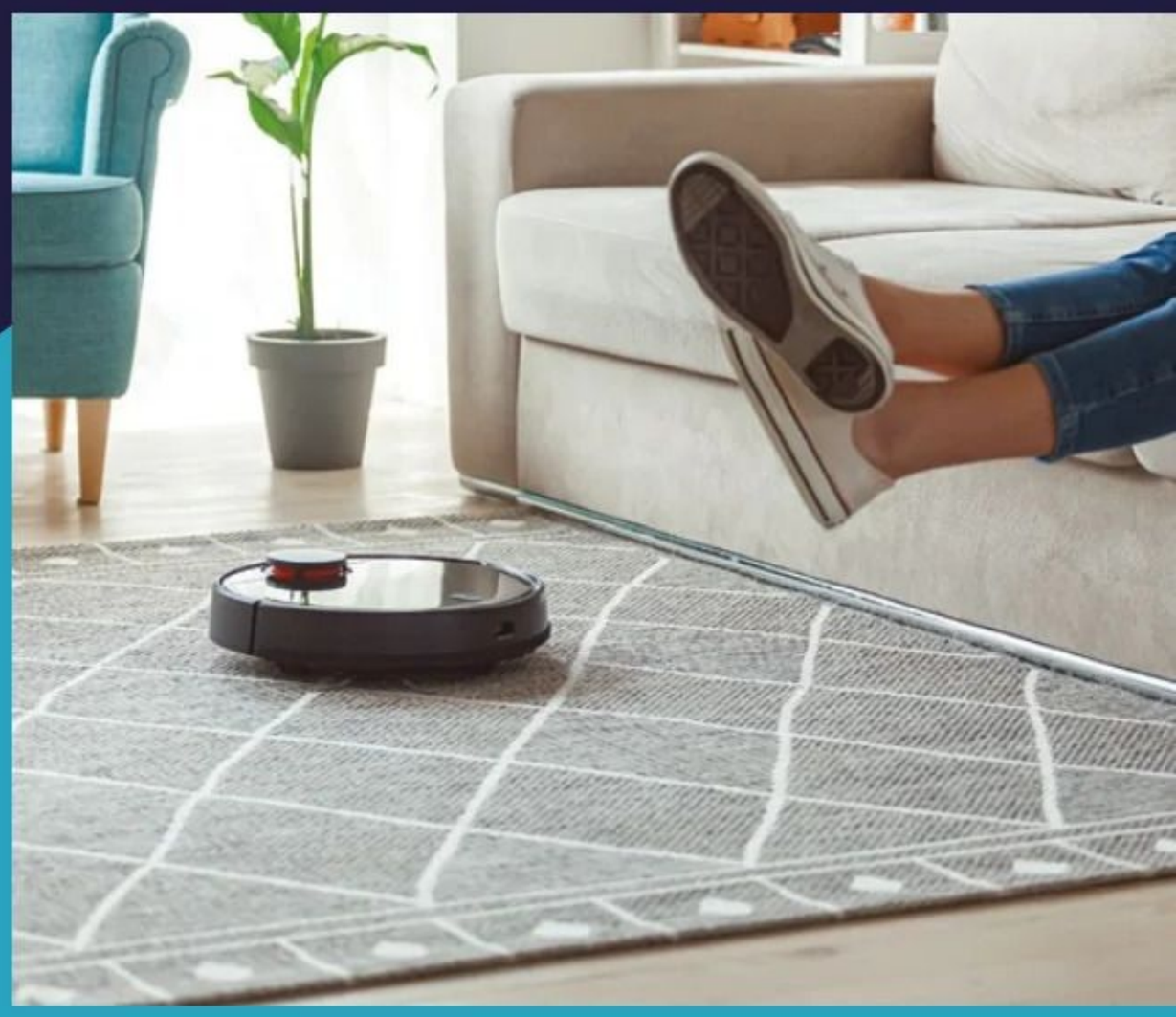
Si los atacantes consiguen acceder a un PC o portátil, casi nada en la red estará a salvo. Para proteger estos dispositivos, debes instalar un programa antivirus actualizado. También tienes que mantener el software actualizado. La mejor forma de hacerlo es con un actualizador automático. Por otro lado, las cuentas de administrador deben estar protegidas con contraseñas seguras. Actualiza también de manera regular el sistema operativo (en Windows, puede hacerse a través de Windows Update). Instala además solo programas de fuentes fiables y apaga el ordenador cuando no lo utilices. Así no solo ahorrarás electricidad, sino que lo alejarás de la 'línea de fuego'.

2 EL ROUTER

Este dispositivo es el centro de control de la red. Si se ve comprometido, los atacantes pueden causar muchos daños. Por lo tanto, deberías actualizar el firmware regularmente. Con FRITZ!Box, por ejemplo, puedes desde la página **http://fritz.box** en tu navegador e iniciando la actualización allí. Protege tanto el router como la red WiFi con una contraseña segura, que no se pueda adivinar fácilmente.

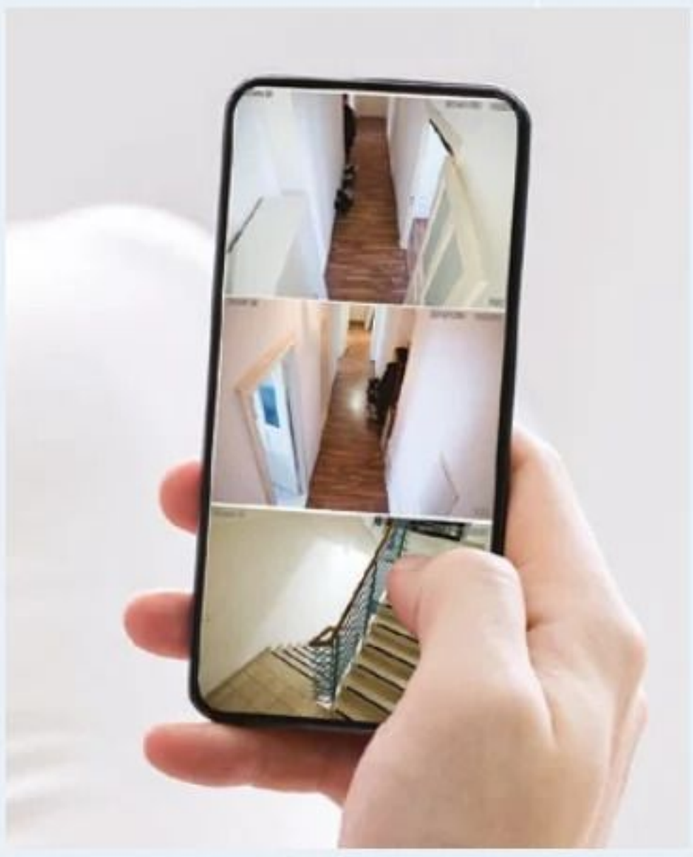
3 DISCOS DUROS EN RED

Los discos duros en red o sistemas NAS no solo son muy prácticos para la familia, sino también para los hackers. ¡Ahí es donde suelen almacenarse los datos más valiosos! Con los sistemas NAS, es muy importante mantener el firmware actualizado. Esto puede hacerse mediante un acceso como administrador. También es aconsejable apagar el dispositivo o desconectarlo del router cuando no lo necesites. Aunque esto no resulta especialmente cómodo, sí que ofrece bastante protección.



4 DISPOSITIVOS CON INTERNET

Algunos dispositivos de tu red doméstica están conectados a Internet, para que puedas acceder a ellos cuando estás fuera (este es el caso de las cámaras de vigilancia). Con estos dispositivos, es extremadamente importante asegurar el acceso con una contraseña segura y mantener el firmware actualizado. De lo contrario, son puertas de entrada perfectas para los atacantes. La contraseña se establece al configurar los dispositivos y se cambia luego en los ajustes. Por desgracia, hay muchos proveedores, sobre todo en dispositivos de bajo coste, que no actualizan el firmware o no lo hacen durante mucho tiempo. Averigua qué hace el fabricante de tus dispositivos. Si no hay actualizaciones, las brechas de seguridad seguirán abiertas. En el caso de los aparatos con conexión a Internet, deberías plantearte sustituirlos. Esto también se aplica a los dispositivos antiguos de fabricantes conocidos.



5 DISPOSITIVOS SIN INTERNET

Si el dispositivo solo puede controlarse localmente a través de la red doméstica, como un robot aspirador, es menos importante protegerlo. Aunque haya brechas de seguridad o las contraseñas sean muy sencillas, el atacante debe haber entrado primero en tu red para causar daños. Y luego, por supuesto, surge la pregunta de qué querría hacer un hacker con esos dispositivos. Los atacantes no suelen estar interesados en apagar las luces, subir la calefacción o pasar la aspiradora por el pasillo. Sin embargo, sí les interesan las cerraduras inteligentes de las puertas. Estas no están conectadas a Internet y solo se abren cuando el móvil está cerca. Sin embargo, si hay lagunas de seguridad, los ladrones podrían entrar en una casa fácilmente. Aquí es extremadamente importante que actualices el firmware.

¿UN COCHE HACKEADO?

Los coches son ahora una especie de ordenadores rodantes. Permiten que la conducción sea más agradable, pero también llaman a los hackers a escena. ¿Estamos seguros al volante?

Control de distancia de seguridad, asistente de frenada de emergencia, programa electrónico de estabilidad, ordenador de a bordo, sistema de entretenimiento, llaves inteligentes, sistemas de localización y cámaras de salpicadero o dashcams, etc. Esto es tan solo una fracción de la tecnología que actualmente se incluye en los coches modernos. Todos estos sistemas ayudan a conducir de una forma mucho más relajada y segura, pero esta tecnología tiene también su lado oscuro, que no es otro que permitir que ahora se puedan llevar a cabo ataques que hace 20 años habrían parecido extraídos de una película de ciencia ficción.

Los ciberdelincuentes pueden entonces penetrar en los sistemas, **manipularlos y robar los datos.** A continuación, aclaramos la dimensión del peligro al que nos enfrentamos y te explicamos cómo protegerse de él.

Muchos experimentos de éxito

Seguro que has oído hablar alguna vez de los robos de coches sin llave. En esos casos, un atacante permanece cerca de la ubicación del conductor, captura la señal de radio de la llave y la envía a un cómplice que se encuentra cerca del coche. Entonces, el cómplice usa la señal capturada para abrir la puerta. Sin embargo, esto no es todo lo que pueden hacer los ciberdelincuentes. Por ejemplo, el experto en ciberseguridad Sam Curry, se ha especializado en descubrir las vulnerabilidades que tienen los vehículos en Estados Unidos. Si visitas su página web (**samcurry.net**), podrás comprender las verdaderas posibilidades que existen a la hora de hackear un vehículo, ya que contiene listados de vulnerabilidades de prácticamente todos los fabricantes. En multitud de ocasiones logró desbloquear, bloquear, rastrear los vehículos, **arrancar o apagar sus motores a distancia...** y mucho más. En algunos casos lo único que necesitaba para lograrlo era el número de chasis, que es perfectamente visible en el parabrisas de los vehículos más nuevos.

Muchos otros investigadores especializados en seguridad han realizado con éxito ataques muy parecidos. Todos estos experimentos demuestran una preocupante realidad: nuestros coches son igual de vulnerables que los PC o los smartphones.

El interés de los hackers va a ir aumentando

La empresa de seguridad VicOne, una filial del fabricante de software antivirus Trend Micro y fabricante de sistemas de seguridad para automóviles, quiso saber sobre qué tipo de ataques hablan los ciberdelincuentes en la Darknet y, para ello, **estudió numerosos foros clandestinos.** Las buenas noticias son estas: en la actualidad, los ciberdelincuentes no están particularmente interesados en hackear vehículos. Solamente les interesa el desbloqueo de funciones premium que son de pago, pero esto es algo que puede cambiar en breve.

El robo de vehículos no es algo preocupante

Aunque el ejemplo de la llave sea el experimento más famoso, el robo de vehículos no resulta interesante para los delincuentes. El motivo es que los coches modernos están prácticamente siempre **conectados a los sistemas del fabricante.** Esto quiere decir que cada coche puede ser rastreado en todo momento, lo que para el caso de Tesla implica que se recupera prácticamente el 98 % de los vehículos.

Si el ladrón desconecta el vehículo, tampoco podrá deshacerse de él porque las funciones más importantes dejarán de funcionar. Por este motivo, es muy poco probable que alguien robe tu vehículo inteligente ni ahora ni en un futuro próximo.

Extorsión y robo de datos

El mayor peligro se encuentra, principalmente, en la extorsión y el robo de información. El robo de datos continúa siendo relativamente inofensivo porque 'sencillamente' se trata de dinero. Los ciberdelincuentes pueden, a través de los sistemas del coche, robar los datos de acceso y de pago en las compras de aplicaciones, para después hacer adquisiciones a tu cargo.

Con la cuestión de la extorsión la cosa se vuelve más peligrosa. Los ataques de ransomware, un malware que cifra los datos y solo los libera a cambio del pago de un rescate, apuntan en la actualidad a los sistemas informáticos de empresas y particulares. Y los coches también pueden ser un buen objetivo de estos ataques. Es posible pensar en toda una serie de escenarios terroríficos que se derivan de este hecho. Imagina, por ejemplo, que circulas por la autopista en tus vacaciones. De repente, el coche acelera y ya no puedes controlar la dirección. En la pantalla aparece un mensaje que exige el pago de 1.000 € a través de PayPal en los próximos cinco minutos; de lo contrario, en el siguiente quitamiedos el coche se estrellará a toda velocidad. Bueno, también podría tratarse de una situación menos drástica: quieres ir a trabajar por la mañana pero, en lugar de arrancar el motor, tu coche muestra únicamente un **mensaje que te informa de que los sistemas están cifrados** y que solo podrás volver a conducir si pagas un recate. Obviamente puedes hacer que restablezcan los sistemas del coche en el taller, pero eso también tiene un coste y será, como mínimo, extremadamente molesto. Este tipo de ataques ya son posibles con los agujeros de seguridad encontrados por el investigador de seguridad Sam Curry.

> Es importante comprender que los ciberataques a vehículos no son ya una ensoñación del futuro, sino una realidad perfectamente actual.
>
> **Max Cheng**
> CEO de VicOne

Cómo protegerse

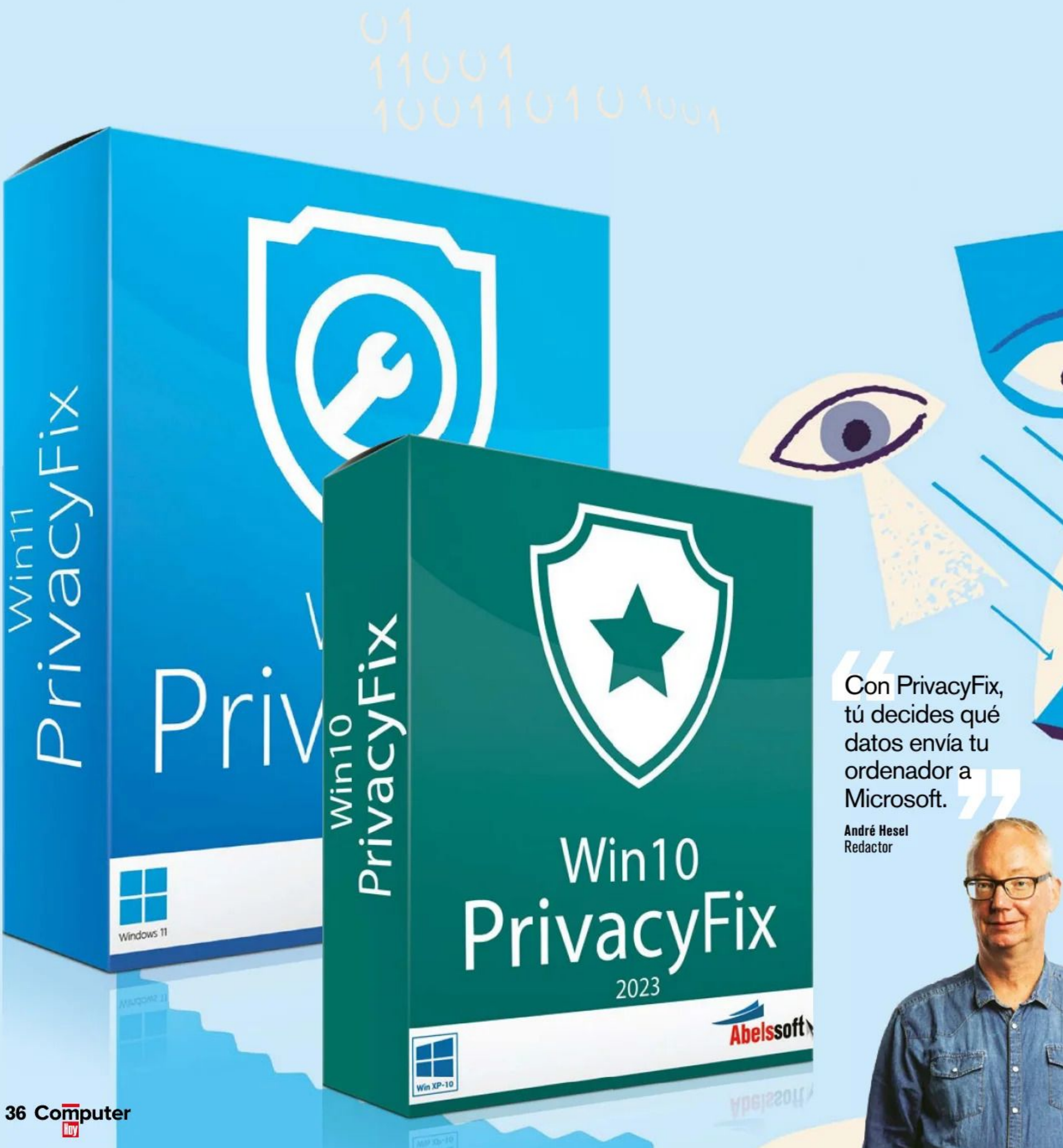
Para protegerte de todo esto, la solución es instalar un sistema de seguridad integral para el coche. Es lo mismo que el programa de protección de tu ordenador: este controla quién accede a los sistemas, bloquea actividades sospechosas y detecta el malware que los atacantes quieran usar para hacerse con el control del vehículo. Lamentablemente, esto es algo que no puedes hacer por ti mismo. Para ti, ademas, esto supondrá primero averiguar qué sistemas de protección ofrece el vehículo. Las buenas noticias: prácticamente todos los fabricantes incluyen sistemas de protección, aunque no todos advierten de las **aplicaciones dañinas o de los sitios web infectados.** Todavía queda mucho por hacer. ■

Un buen sistema de protección del coche también avisa de apps dañinas o de sitios web infectados. Esto es algo realmente importante, para impedir que los atacantes puedan tener acceso al sistema del vehículo.

práctico
Asegura tu privacidad

iOS

LAS APLICACIONES QUE ESPIONAJE



"Con PrivacyFix, tú decides qué datos envía tu ordenador a Microsoft."

André Hesel
Redactor

NECESITAS PARA DETENER EL EN TODOS TUS DISPOSITIVOS

Protege tu intimidad: con estos trucos y programas, podrás evitar el espionaje de datos en el ordenador y en el móvil.

Cuando Microsoft lanzó Windows 10 hace ocho años, las funciones de espionaje que incluía fueron motivo de protesta a nivel mundial. A día de hoy, no ha cambiado mucho en lo que respecta al espionaje. Su sucesor, Windows 11, también se queda con cada clic que haces en el ordenador, **recopila de forma constante los datos de uso y los transmite en segundo plano** a la empresa estadounidense. Como las opciones de responsabilidad están muy ramificadas en la configuración, a aquellos que no sean expertos les resultará complicado comprender el alcance del control que tiene Windows. El programa PrivacyFix de Abelssoft lo hace mucho muy fácil: enumera de forma clara alrededor de 50 ajustes de protección de datos relevantes en Windows, y ofrece recomendaciones que puedes aplicar con tan solo hacer clic. De este modo, podrás resolver el caos de Windows y esquivar también a Microsoft. Y lo mejor: te presentamos dos software antiespías para Windows 10 y 11 en este mismo artículo.

Optimiza Windows 10 y 11

Si quieres saber exactamente qué es lo que pasa en tu ordenador, puedes configurar de forma manual todos los ajustes de espionaje con PrivacyFix. Y no solo eso: este programa también desinstala las aplicaciones innecesarias de Microsoft y optimiza la configuración en el propio Windows y en el Explorador. Si ya te has pasado a Windows 11, también podrás desactivar con él nuevas funciones que consumen mucho rendimiento, como los widgets, o alinear la Barra de tareas a la izquierda, como en las versiones anteriores. Puedes obtener más información sobre el resto de opciones que ofrece PrivacyFix y cómo funciona en el apartado correspondiente.

Importante: la protección de datos en el ordenador

Windows no es la única amenaza que desafía la privacidad en tu PC. El historial de navegación y los archivos guardados también revelan mucha información personal sobre ti. En este artículo, encontrarás una serie de trucos y consejos sobre cómo proteger el navegador y los archivos confidenciales, sobre cómo **navegar por Internet de manera anónima** y sobre cómo almacenar contraseñas de forma segura.

La protección de datos en cualquier lugar

Los móviles también son unos verdaderos 'mercaderes' de datos. Por ello, en este artículo te explicamos cómo proteger tu privacidad en dispositivos Android e iOS. También podrás averiguar, entre otras cosas, cómo **evitar la vigilancia no deseada de los sitios web (rastreo)**, cómo enviar correos electrónicos anónimos y cómo ocultar debidamente tu ubicación.

práctico
Asegura tu privacidad

DETÉN LAS FUNCIONES DE ESPIONAJE

PROTECCIÓN DE WINDOWS

¡Di adiós a la recopilación de datos! Estos programas desactivan las funciones de espionaje en Windows 10 y 11 con tan solo hacer clic.

Sabías que Windows vigila tu actividad en el ordenador, se queda con cada clic y **recopila todos los datos de uso?** Gran parte de esta información se utiliza para mejorar la fiabilidad y uso del ordenador y permanece en el disco duro (este es el caso del historial de archivos). Otra se transmite, sin que tú lo sepas, a los servidores de Microsoft en Internet y se analiza allí. Así, gracias a estos datos de telemetría y diagnóstico, la empresa conoce, entre otras cosas, las especificaciones de tu hardware y software, la dirección IP e incluso el contenido de la memoria RAM en caso de que el ordenador se bloquee. Así también podrá saber qué programas descargas de la Microsoft Store, dónde vives y qué escribes en la búsqueda de Windows.

La practicidad de la optimización con un 1 solo clic, irápida y efectiva!

La lista de funciones de espionaje es muy larga y casi imposible de controlar para el usuario medio. Algunas pueden desactivarse, pero están tan integradas en la configuración de Windows que la mayoría de los usuarios tienen que aceptar a regañadientes que **la recopilación de datos es un hecho**. Los programas Win11 PrivacyFix y Win10 PrivacyFix del fabricante Abelssoft te devuelven el control sobre los datos y la privacidad. Te indican de forma clara todas las funciones de espionaje de Windows y restablecen los ajustes recomendados con un solo clic. Si quieres saber cómo hacerlo, consulta esta página. En el recuadro de la izquierda, encontrarás información sobre cómo instalar el programa de forma gratuita.

Mejora Windows

Si lo necesitas, puedes proteger de forma manual Windows contra el espionaje, activar también las **mejoras ocultas o deshabilitar las aplicaciones preinstaladas** de Microsoft. Para saber cómo, sigue leyendo.

DESCARGA E INSTALACIÓN

Ve a la página oficial del programa (en este caso, en **bit.ly/40ohqu4** para Windows 10 y en **bit.ly/3MwMCIf** para Windows 11) y haz clic en ***Free Download***. Tras la descarga, ejecuta el Asistente de instalación y sigue las instrucciones. Después solo tienes que registrarte. ¡Y listo! Ya puedes disfrutar de las ventajas de PrivacyFix.

OPTIMIZACIÓN EN **1 CLIC**

Optimización en 1 clic: desactiva las peores funciones de espionaje de Windows con un solo clic.

¿No tienes tiempo ni ganas de afrontar las decenas de funciones de espionaje incluidas en Windows? Entonces, la herramienta Optimización en 1 clic es justo lo que necesitas. Así funciona:

1 Inicia la optimización: si no lo has hecho ya, abre el programa PrivacyFix. Si no se abre de forma automática la ventana que aparece en la imagen superior, pulsa sobre ***Optimización en 1 clic***.

2 Configúralo como quieras: en esta ventana que tienes ante ti, haz clic ahora en la opción que quieras:

- **Recomendada:** con esta función, sigues las recomendaciones del fabricante y obtienes una buena combinación de protección de la privacidad y facilidad de uso del sistema operativo Windows.
- **Camuflaje:** esta opción desactiva de manera automática todas las transferencias de datos desde Windows. Sin embargo, es posible que algunas aplicaciones y programas del sistema dejen de funcionar como de costumbre.
- **Windows (Predefinida):** haz clic en esta opción para restaurar la configuración predeterminada de Windows. Resulta útil, por ejemplo, si te has equivocado al configurar algo y el sistema operativo ya no funciona como esperas.

3 Aplica los cambios: por último, haz clic en la ***X*** para cerrar el programa y reinicia Windows. Los ajustes que hayas seleccionado se activarán entonces.

MODO EXPERTO DE FORMA MANUAL

¿Quieres comprobar una por una todas las funciones de espionaje de Windows y desactivarlas si es necesario? En ese caso, ve a la ventana principal de PrivacyFix, donde se muestra lo que hay detrás de cada botón y cómo cambiar las opciones correspondientes. Hay cinco categorías en total:

Protección de datos

Aquí encontrarás las clásicas funciones de espionaje de Windows, como ***Telemetría***, ***Datos de diagnóstico*** e ***ID de publicidad***, que Microsoft utiliza para ofrecer publicidad personalizada. Desde ahí también puedes controlar el acceso desde Windows y otros programas a tus datos de localización, cámara, micrófono, contactos y citas.

Explorador

En esta sección, puedes restringir las cómodas funciones del Administrador de archivos de Windows y, por lo tanto, controlar qué información revela el Explorador de Windows sobre el uso del ordenador. Por ejemplo, puedes desactivar la búsqueda en la Barra de tareas y el acceso rápido a determinados archivos, ocultar iconos y archivos del sistema o desactivar la visualización de carpetas y archivos de uso frecuente.

Sistema

Desde aquí puedes activar el bloqueo numérico del teclado del ordenador, para que esté directamente disponible cuando te conectas a Windows. Es una función que resulta muy práctica si por ejemplo la contraseña de Windows contiene dígitos.

Ajustar

En este apartado, puedes desactivar esa pantalla de bloqueo de Windows tan molesta para poder introducir la contraseña, que aparece directamente después de encender el ordenador. Además, es posible activar la opción ***No rastrear*** de los sitios web, alinear la Barra de tareas de Windows 11 hacia la izquierda o desactivar los nuevos widgets en Windows 11.

Programas

En esta lista, si lo necesitas, puedes desactivar directamente todas las aplicaciones preinstaladas de Windows. Este es el caso concreto de por ejemplo Bing, Skype, OneNote, la aplicación Xbox o Paint.

Lista de opciones

En esta sección, encontrarás todas las categorías descritas anteriormente con sus respectivas opciones. Si un ajuste coincide con la recomendación, aparecerá en verde; en caso contrario, en rojo.

Grado de protección

Aquí el programa muestra en porcentaje el grado de protección de datos de Windows, con la configuración actual que tengas. ¡Cuanto más alta, mejor!

Botones de selección

Desde aquí se activan o desactivan las funciones de Windows. Si colocas el cursor sobre el símbolo de información, aparecerán los ajustes de Windows y la recomendación del programa. Es muy estricto y puede diferir de las recomendaciones de la Optimización en 1 clic.

TAMBIÉN PARA WINDOWS 10

Si todavía utilizas Windows 10, también puedes instalar el programa Win10 PrivacyFix en tu dispositivo. Aunque tiene un aspecto un poco diferente (ver la imagen), funciona exactamente igual que la versión de Windows 11. Win11 PrivacyFix también ofrece opciones adicionales específicas para Windows 11.

práctico
Asegura tu privacidad

DOCUMENTOS Y DATOS SEGUROS

ORDENADOR PROTEGIDO

Asegura por completo tu equipo: aprovecha estos tres trucos para lograr protegerte a ti y a tus archivos de los peligrosos espías de datos.

Con los programas de las páginas anteriores, ya habrás evitado que Microsoft se ponga a cotillear tu información. No obstante, **si compartes tu ordenador con otras personas**, lo más seguro es que también quieras protegerte de las miradas indiscretas de compañeros, familiares o amigos. Porque la confianza no debe sobrepasar algunos límites y porque tus documentos y datos son solo para ti.

Tres trucos para aumentar el grado de seguridad

Los tres trucos que describimos en estas páginas no requieren mucho tiempo ni esfuerzo por tu parte, pero te garantizarán una mayor seguridad en el ordenador en el futuro. Y lo mejor: **se pueden probar fácilmente con versiones gratuitas**, ¡así no tendrás que gastarte ni un solo céntimo, y lograrás mucha privacidad extra en tu PC!

DESACTIVA EL HISTORIAL

¿Varias personas utilizan tu ordenador para navegar? En ese caso, deberías establecer que el historial del navegador se elimine automáticamente. Hazlo así desde tu navegador:

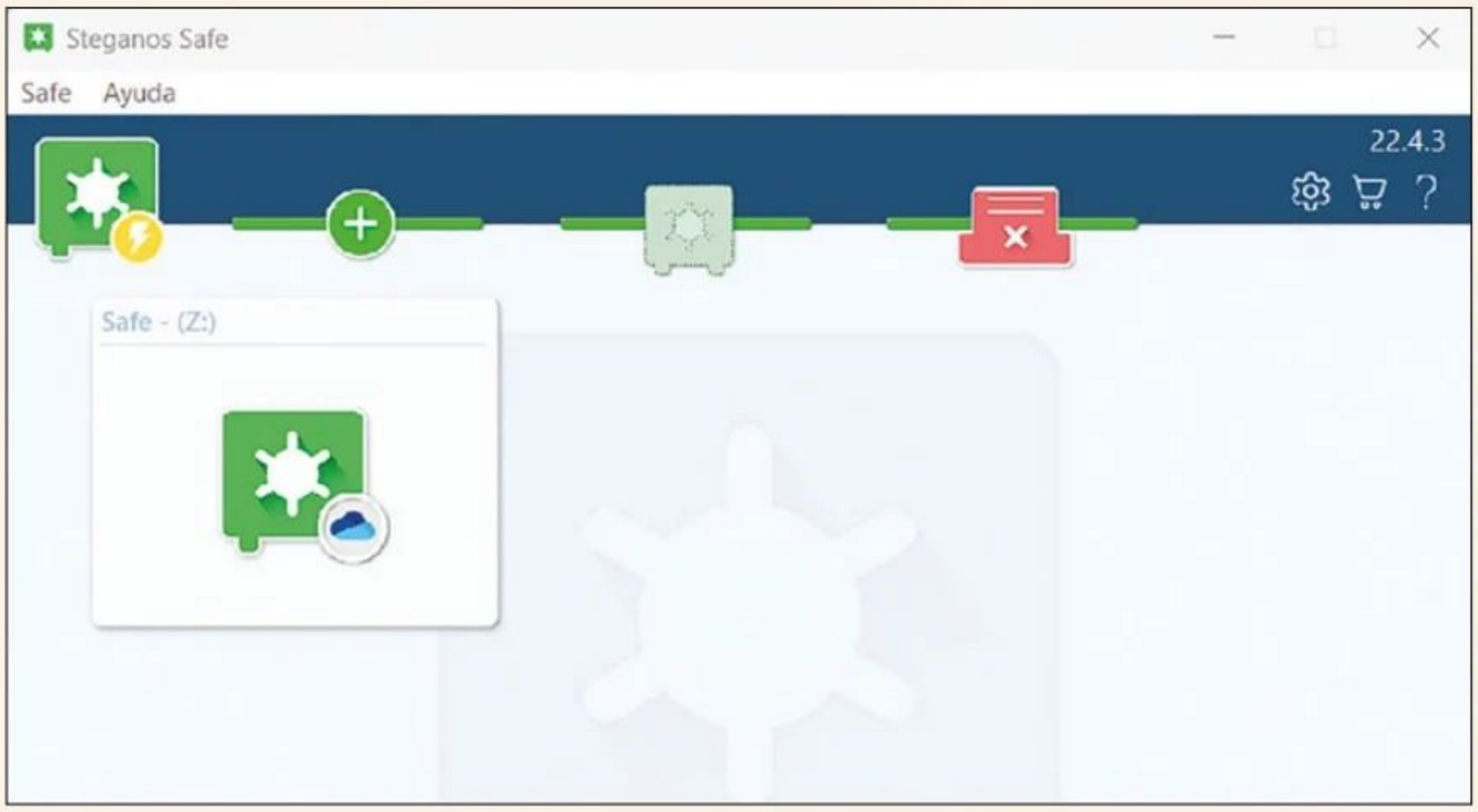
- **Firefox**: ve a ***Ajustes*** y haz clic en ***Privacidad & Seguridad***. Luego, desde la sección ***Historial***, haz clic en ***Recordar el historial*** para abrir el menú desplegable. Pulsa en ***Usar una configuración personalizada para el historial*** y marca la casilla ***Limpiar el historial cuando Firefox se cierre***.
- **Edge**: accede a ***Configuración*** y haz clic en ***Privacidad, búsqueda y servicios***. En el apartado ***Borrar datos de exploración***, haz clic en ***Elegir qué se debe borrar cada vez que se cierra el explorador*** y activa la opción ***Historial de exploración***.
- **Chrome:** no ofrece una opción independiente para eliminar el historial. Sin embargo, puedes adaptarlo fácilmente con la extensión gratuita Click&Clean (ver imagen), disponible en la página web **bit.ly/40oOkuo**.

PROTEGE TUS DATOS EN EL ORDENADOR

Con Steganos Data Safe, puedes cifrar archivos confidenciales de forma segura en una 'caja fuerte digital' a la que podrás acceder de forma tan sencilla como a una unidad de disco. Así proteges todos tus documentos y datos confidenciales de los curiosos. Este programa de seguridad, que puedes probar de forma gratuita durante 30 días en **bit.ly/465Krf8**, protege los datos con un algoritmo de cifrado AES-XEX de 384 bits. Además de una contraseña de acceso, que también está protegida contra ataques de fuerza bruta, también puedes utilizar dispositivos externos, como memorias USB. Por otro lado, puedes 'ocultar' datos codificados en vídeos y archivos de audio o utilizar 'cajas fuertes' que, además, no solo pueden almacenarse en local, sino también en soportes portátiles como memorias USB o en sistemas de almacenamiento en la nube como Dropbox, Microsoft OneDrive o Google Drive.

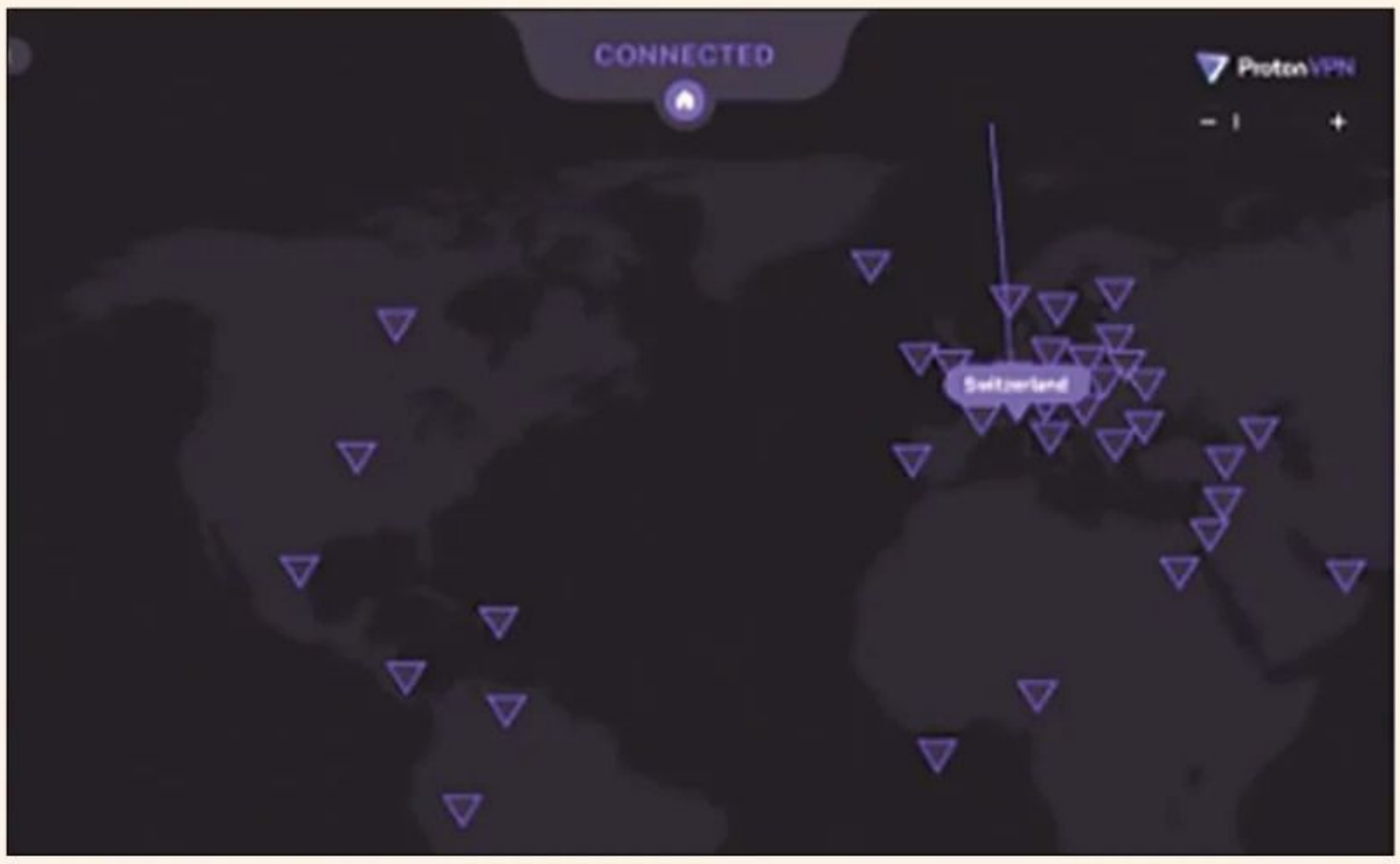
Cómo se instala

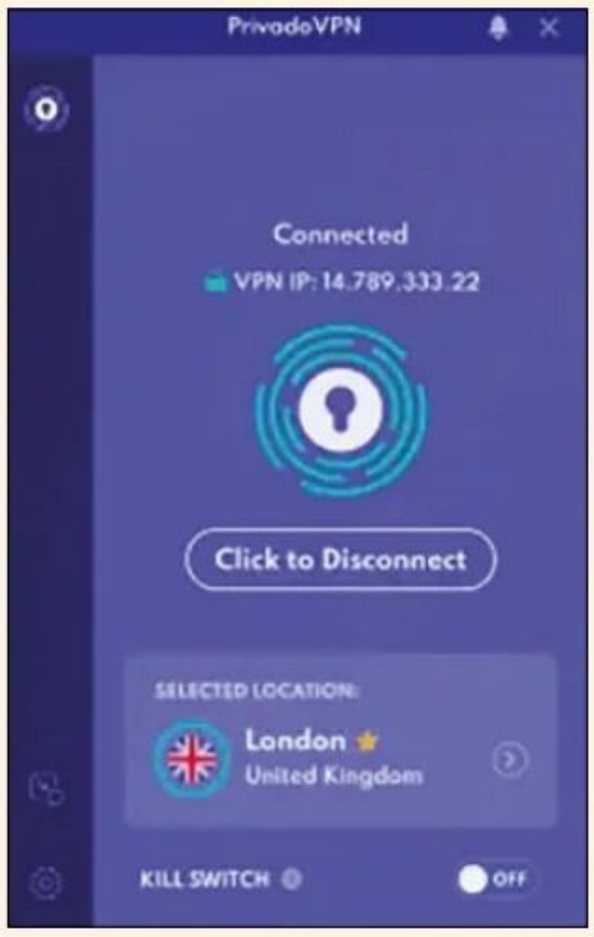
Visita la página web anterior y haz clic en ***Probar (30 días)***. Y, tras la descarga, ejecuta el Asistente de instalación y sigue todas las instrucciones que se te indiquen para que se lleve a cabo la instalación. Luego podrás acceder a Steganos Data Safe.



Tus documentos confidenciales se cifran de forma segura en la caja fuerte de datos y están protegidos contra el espionaje. Además, su interfaz muy estructurada lo convierte en un software intuitivo y fácil de usar.

NAVEGA CON UNA VPN





ProtonVPN y PrivadoVPN son dos servicios de red privada virtual (VPN), con los que puedes garantizar la privacidad del ordenador y la navegación de forma totalmente anónima en Internet. Tus datos permanecerán seguros, incluso en conexiones públicas o que no sean seguras.

Si no quieres revelar tu actividad en Internet o quieres librarte de los bloqueos de ciertos países, necesitas una red privada virtual (VPN, por sus siglas en inglés). Este tipo de aplicaciones ocultan tu dirección IP real y ofrecen varias ventajas: con ellas, puedes navegar por Internet de forma más segura, proteger tu privacidad online e, incluso, a veces tendrás acceso a servicios bloqueados por ciertas regiones. Además de varias soluciones de VPN que puedes contratar mediante una suscripción anual de pago, también hay algunas opciones gratuitas que difieren de forma significativa en términos de seguridad y funcionalidad. En Computer Hoy, te presentamos ahora dos de las mejores soluciones gratuitas por las que puedes optar:

Proton VPN

Está considerada una de las VPN más seguras entre los servicios de camuflaje gratuitos. El proveedor no registra ningún dato y tiene su sede en Suiza, un país favorable a la protección de datos. Auditores de seguridad externos ya han probado varias veces el servicio en busca de vulnerabilidades y no han encontrado ninguna. Proton VPN es uno de los pocos proveedores de VPN que publica sus aplicaciones bajo una licencia de código abierto. También da acceso a todos los protocolos VPN importantes en la versión gratuita, y la protección contra filtraciones integrada evita las fugas accidentales de datos. Sin embargo, si se produce un problema imprevisto, la VPN corta inmediatamente la conexión a Internet. La encontrarás disponible en **protonvpn.com/es**.

PrivadoVPN

Esta VPN también tiene su sede en Suiza. Este segundo servicio gratuito que recomendamos cuenta con una característica que normalmente solo se encuentra en las VPN de pago: este software es apto incluso para el streaming en determinadas condiciones. Con un total de diez países disponibles, PrivadoVPN se ha posicionado bien con su versión gratuita e incluye lugares como Brasil y Argentina. La única limitación son los 10 GB de tráfico de datos incluidos en la versión gratuita, que se agotan enseguida incluso con un uso normal sin streaming de vídeo. Por otro lado, para utilizar este programa, deberás tener al menos un conocimiento básico de inglés, ya que el servicio no está disponible en español. Puedes descargar este programa en la página web **privadovpn.com/es**.

CONTRASEÑAS SEGURAS **GRATIS**

Sticky Password es una caja fuerte para contraseñas y notas que normalmente es de pago, pero puedes probar la versión gratuita en **www.stickypassword.com**.

práctico
Asegura tu privacidad

SEGURIDAD PARA iOS Y ANDROID

PROTECCIÓN DEL MÓVIL Y EL TABLET

Ya sea iOS de Apple o Android de Google; ambos sistemas ofrecen toda una serie de opciones de protección de datos extra. ¡Prueba ya todos estos trucos!

CONTROL DE ACCESO

La privacidad de tu teléfono móvil es importante. Android e iOS ofrecen varias opciones para controlar el acceso.

- **iOS:** en los dispositivos móviles de Apple, la información más importante se resume en ***Ajustes***, ***Privacidad y seguridad*** y ***Rastreo***. Ahí puedes desactivar los servicios de localización o el seguimiento de aplicaciones. También puedes especificar qué aplicaciones están autorizadas a acceder a qué datos.
- **Android:** desde Android 12, Google ha agrupado todos los datos importantes sobre privacidad en un mismo panel. Entre otras cosas, enumera qué aplicaciones han accedido a la ubicación, la cámara o el micrófono en las últimas 24 h y con qué frecuencia. Estas autorizaciones pueden gestionarse en un mismo lugar. Android también ofrece la opción de desactivar el acceso a la cámara y al micrófono para todo el móvil.

NAVEGACIÓN OCULTA

Apple y Samsung ofrecen sus propios servicios para anonimizar la navegación, similares a los de las VPN, pero se necesita una suscripción para ambos sistemas.

- **iOS:** ve a ***Ajustes*** y selecciona tu nombre, ***iCloud*** y ***Actualizar a iCloud+***. Si te suscribes a iCloud+ (desde 0,99 € al mes), se activará el servicio de relay privado de iCloud, que oculta tu propia dirección IP y los sitios web que visitas y transmite la ubicación de forma más aproximada.
- **Android (solo Samsung):** en la configuración del dispositivo, selecciona la opción ***Biometría y seguridad*** y ***Wi-Fi seguro***; de esta forma, Samsung te protege de redes no seguras, tras iniciar sesión con una cuenta Samsung del modo habitual.

SEGUIMIENTO DEL NAVEGADOR

Los sitios web suelen vigilar de cerca lo que hacen los usuarios online. Apple y Google ofrecen una serie de funciones que frenan este comportamiento tan intrusivo.

- **Apple:** el navegador Safari tiene su propia configuración de privacidad. En los ajustes de Safari, puedes activar la función ***Impedir el seguimiento entre sitios*** mediante el uso del interruptor disponible, para ocultar ahí la dirección IP.
- **Android:** puedes activar la opción ***Enviar una solicitud "Do Not Track"*** o ***No hacer seguimiento*** en la configuración de Chrome, en ***Privacidad y seguridad***. Con esta configuración no impide el rastreo, pero indica a los sitios web que no deben hacerlo.

iOS: **CORREO ANÓNIMO**

La aplicación Mail de Apple ofrece muchas funciones de protección al enviar correos electrónicos. Por ejemplo, impide de forma automática la recopilación de datos, oculta tu dirección IP y no revela cuándo abres un correo electrónico. Si te has suscrito a iCloud+ (consulta el apartado 'Navegación oculta'), puedes utilizar direcciones de correo electrónico anónimas generadas de forma aleatoria. Apple reenvía entonces los correos electrónicos a tu dirección, de manera que evita que se transmita la dirección real. Para ello, abre los ajustes, pulsa en tu nombre, ***iCloud*** y en ***Ocultar mi correo electrónico***.

ANDROID: **MENSAJERÍA DUAL**

¿Tu cuenta de WhatsApp mezcla conversaciones personales y profesionales? En ese caso es mejor que crees cuentas independientes en el teléfono móvil. Con Samsung es bastante fácil de llevar a cabo:

1 Para empezar, accede a los ajustes del teléfono móvil. Abre entonces las funciones avanzadas y selecciona la opción ***Mensajería dual***. Pulsa en la aplicación que quieras clonar, por ejemplo, en ***WhatsApp***.

2 A continuación, presiona en ***Instalar*** y luego en ***Confirmar***. Con todo esto, ahora incluso podrás separar los contactos, si activas la opción ***Utilizar lista de contactos separada***. Estos ajustes se llevan a cabo por separado, para cada aplicación que se clone en el móvil.

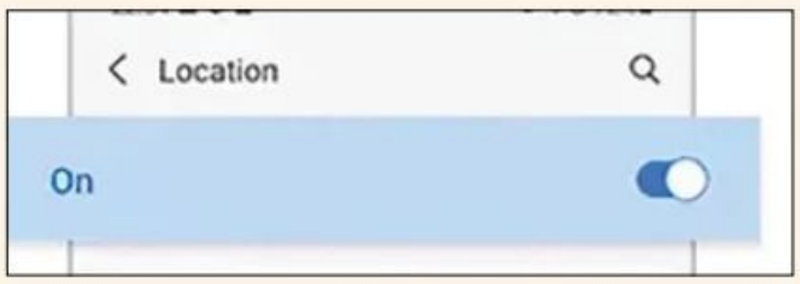
MÁS PRIVACIDAD EN EL MÓVIL

OCULTA TU **UBICACIÓN**

Los móviles rastrean tu ubicación con precisión, pero puedes desactivar este comportamiento. Así funciona en Android, iOS y Google.

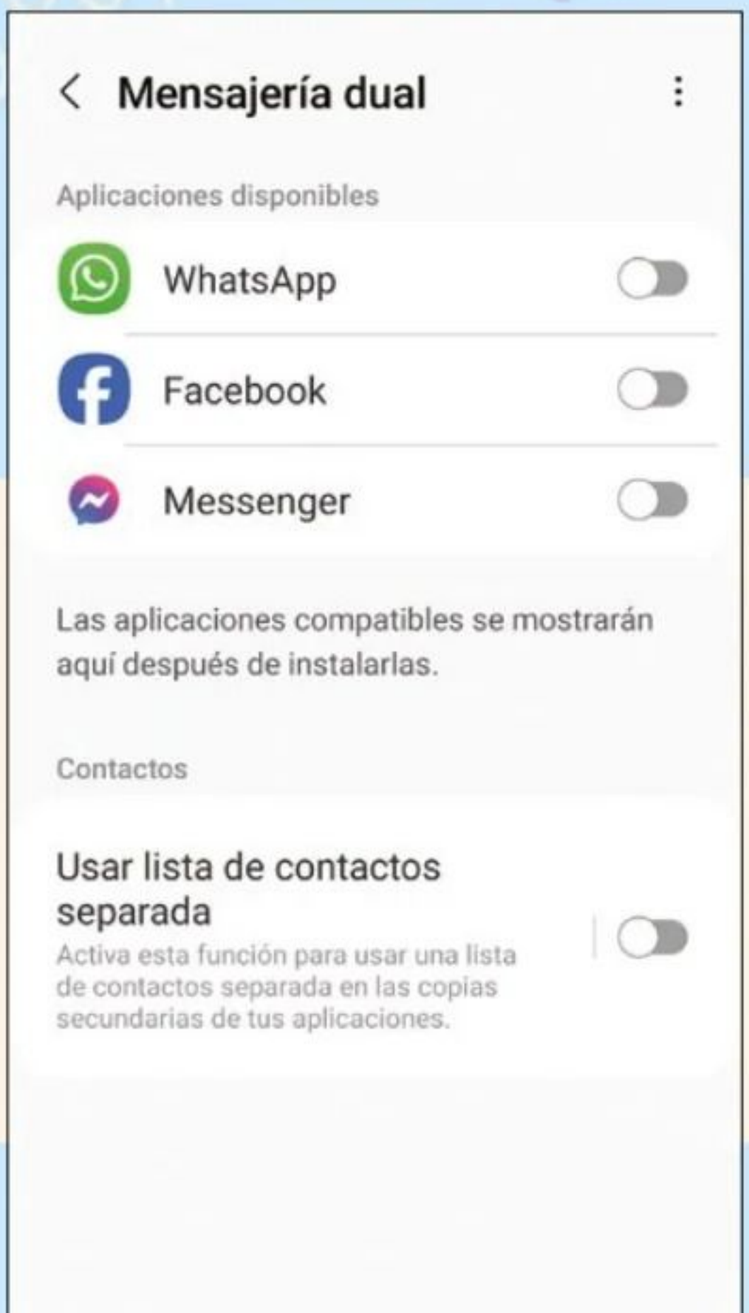
Android y Google Maps

Puedes gestionar las autorizaciones de la aplicación para el acceso a la ubicación en los ajustes de Android, en ***Ubicación***. Utiliza el regulador situado en la parte superior, para desactivar la localización para todo el dispositivo. A través de los servicios de localización y el historial de ubicaciones de Google, puedes acceder a la configuración de Google, donde puedes desactivar y eliminar dicho historial de ubicaciones.



iOS y Google Maps

El acceso a la ubicación puede gestionarse en los ajustes del iPhone, en ***Privacidad y seguridad*** y ***Localización***. Utiliza el regulador de la parte superior para detener la localización de todo el dispositivo. Sin embargo, así ya no se podrá realizar la navegación ni la búsqueda de un iPhone perdido. Por lo tanto, resulta más práctico configurar los servicios de localización de cada aplicación; para las apps importantes, la mejor opción suele ser ***Permitir al usarse la app***. Es posible que tengas que volver a activar la búsqueda del iPhone en los ajustes de iCloud. Si utilizas Google Maps en el iPhone, tendrás que desactivar el historial de ubicaciones independiente en el sitio web **myactivity.google.com**.



SAMSUNG: **CARPETA SEGURA**

No todos los archivos deben estar disponibles sin protección en el móvil. Samsung ha introducido la opción ***Carpeta segura*** para proteger los datos confidenciales, pero requiere una cuenta de Samsung. Por ejemplo, puedes proteger tu galería, contactos, calendario y notas. Utilízala así:

1 Selecciona ***Datos biométricos y seguridad*** en los ajustes del teléfono.

2 Pulsa ahora en ***Carpeta segura*** y sigue las instrucciones del asistente.

3 Después de desbloquear la carpeta segura, selecciona un tipo de bloqueo (patrón, PIN, contraseña o huella dactilar) y especifica si la protección se puede restablecer con una cuenta de Samsung.

práctico
Exprime tu smartphone

MENSAJERÍA INSTANTÁNEA

CÓMO LEER MENSAJES DE SIN QUE TU CONTACTO LO

¿No quieres que tus contactos sepan que has leído sus mensajes? Descubre ahora cómo leer mensajes de WhatsApp sin que el remitente de los mismos lo sepa.

Aprende a...

Leer mensajes de WhatsApp sin que el remitente lo sepa. Podrás hacerlo desde el modo avión, con el widget de la app, el área de notificaciones o la confirmación de lectura.

WhatsApp es en una de las aplicaciones más populares para comunicarte con amigos, familiares y otros usuarios, no en vano es **la app de mensajería más utilizada** en todo el mundo. Sin embargo, hay ocasiones en las que puede que prefieras que la otra persona no sepa que ya has leído su mensaje... quizá por curiosidad, privacidad o simplemente porque prefieres mantener un bajo perfil de partición en las conversaciones.

Sean cual sean tus razones, gracias a una serie de consejos que te vamos a indicar aquí y ahora, podrás leer mensajes de WhatsApp sin que tu contacto lo sepa. Verás así las diferentes maneras que hay ahora mismo para conseguir mantener tus **conversaciones privadas bajo control**.

01 LEE MENSAJES DESDE LA BARRA DE NOTIFICACIONES Y CON LOS WIDGETS

Estas dos primeras opciones para leer mensajes de WhatsApp sin ser descubierto son bastante sencillas y cómodas de utilizar. En ambos casos, son técnicas muy efectivas para mantener tu privacidad mientras navegas por tus conversaciones de WhatsApp. Sigue estos pasos.

Acceso desde el área de notificaciones de tu teléfono móvil Android

La primera de las opciones que tienes a tu disposición es, posiblemente, la más sencilla y visual de todas. Como bien sabrás, en el momento en el que recibes un mensaje, se abre una notificación emergente en la parte superior del terminal, a modo de alerta, la cual se integra en la barra de notificaciones.

1 En el caso de WhatsApp, cuando alguien te envía un mensajes, podrás ver en este área de notificaciones (a modo de vista previa) parte o todo el mensaje que hayas reci-

WHATSAPP SEPA

bido. Todo ello sin que sea necesario tener que abrir la aplicación WhatsApp 1.

2 Como te hemos dicho, esta notificación permite, en muchos casos, leer todo el mensaje o la mayor parte de su contenido, pero mientras no pulses sobre dicha notificación, WhatstApp no indicará de ninguna manera a la otra persona que lo has leído.

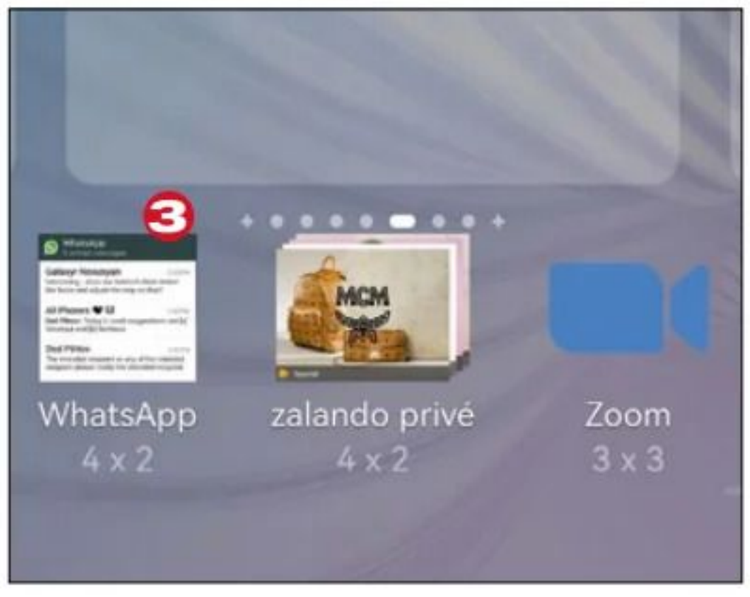
Lee los mensajes de WhatsApp gracias a los widgets de la aplicación

Otra de las características más interesantes de WhatsApp, que puedes utilizar para leer mensajes sin que la otra persona lo sepa, consiste en echar mano del widget de la propia app. Como bien sabrás, los widgets son añadidos interactivos que te brindan un acceso rápido a algunas de las funciones de las distintas apps, y todo ello desde la pantalla de inicio de tu propio terminal. La forma de lograr leer chats sin dar información de lectura a la persona que te lo ha mandado consiste en utilizar el widget de WhatsApp de la siguiente manera:

1 Dirígete a la pantalla de inicio de tu dispositivo y mantén una pulsación durante unos segundos en un espacio vacío. Hazlo hasta que aparezca un nuevo menú en pantalla y puedas seleccionar ***Widgets*** 2, ***Agregar widget***, ***Añadir widget*** o similar.

2 Busca entonces el widget denominado ***WhatsApp 4 x 2*** en la lista de opciones disponibles 3. Pulsa directamente sobre él y arrástralo hasta la zona de la pantalla de tu Android en la que quieras situarlo.

3 A partir de ese momento, en cuanto recibas un mensaje en WhatsApp, aparecerá una vista previa de él en el propio widget que acabas de añadir, incluyendo además el nombre del remitente 4. Como ves, este sistema te sirve perfectamente para saber quién y qué te han escrito.



02 ACCESO A LOS MENSAJES DE WHATSAPP CON EL MODO AVIÓN

El modo avión es una función que está presente tanto en terminales Android como en aquellos móviles equipados con iOS, por lo que vas a poder utilizarla tengas el smartphone que tengas. Se trata así de una funcionalidad que, al activarla, desactiva las conexiones inalámbricas como los datos móviles, la conexión WiFi o Bluetooth. En cualquier caso, puedes aprovechar esta característica para conseguir leer mensajes de WhatsApp sin que la otra persona lo sepa. Para lograrlo, solo debes hacer lo siguiente:

1 Para acceder al modo avión de tu teléfono móvil, desliza desde la zona superior, para así visualizar el área de notificaciones. Allí encontrarás el icono que te permite habilitar/deshabilitar este modo 5.

2 Una vez que hayas activado el modo avión en tu terminal, deberás abrir directamente la app WhatsApp y navegar hasta las conversaciones que deseas leer. Cuando termines su lectura, cierra la aplicación y desactiva el modo avión para volver a la normalidad. Recuerda también cerrar la aplicación antes de desactivar este modo, para que de esta forma no se sincronice y comunique que has entrado en el chat. Incluso es recomendable que también desactives el funcionamiento en segundo plano de la aplicación, por si acaso.

De cualquier forma, con todas las conexiones inalámbricas restablecidas, WhatsApp volverá a tener acceso a Internet y estará de nuevo sincronizada con la red. Eso sí, sin marcar como leídas las conversaciones que has visto antes desde el modo avión.

03 LA OPCIÓN PARA DESHABILITAR LA CONFIRMACIÓN DE LECTURA

WhatsApp ofrece a sus usuarios una medida de privacidad que puede ser una opción para muchos, puesto que permite leer los mensajes sin marcar el famoso doble check azul. El problema que presenta esta posibilidad es que esto también acarrea que tú tampoco puedas saber si se han leído los mensajes que tú hayas mandado, por lo que puedes perder esta capacidad tan interesante. Si aun así no te importa perder esta opción y quieres que nadie pueda saber cuándo lees un mensaje, la manera de lograrlo es la siguiente:

1 Desde tu dispositivo móvil, abre la aplicación WhatsApp y pulsa en el icono de menú (tres puntos verticales) que hay disponible en la esquina superior derecha. Pulsa entonces sobre ***Ajustes***, selecciona también la entrada ***Privacidad*** y, por último, desactiva el regulador denominado *Confirmaciones de lectura* 6.

2 Si tienes un iPhone los pasos son ligeramente diferentes, pero también te permitirán conseguir que no se marque tu lectura con el doble check azul ya tan popular.

EL DOBLE CHECK AZUL

Ya hace tiempo que el doble tick azul, símbolo que representa que un mensaje de WhatsApp ha sido visto y leído, convive con nosotros. Concretamente, fue en 2014 cuando la compañía incorporó esta nueva característica a través de una actualización. Así, la app nos avisa con un doble check azul cuando los mensajes son leídos. Y esto se aplica también a grupos y notas de voz, que aparecen marcadas con símbolo azul cuando se han reproducido. No obstante, en el caso de los grupos, hay que tener en cuenta que el popular chek solo será visible cuando todos los miembros del grupo hayan leído el mensaje en cuestión. Es decir, mientras tanto, solo aparecerá la marca del doble tick (pero no en azul) indicando que el mensaje ha llegado al dispositivo del destinatario.

MICROSOFT WORD

FORMULARIOS CON CONTRASEÑA

¿Vas a diseñar un formulario en un documento de Word y necesitas reservar un espacio para introducir una contraseña? Entonces, crea un cuadro de texto en el que se pueda teclear una contraseña, y visualiza y oculta esta a través de una casilla de verificación.

Aprende a...

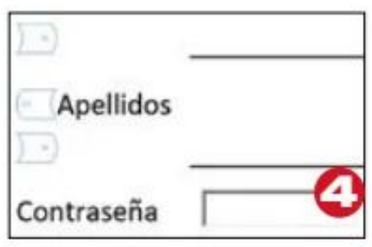
Usar código VBA en un documento de Word, para programar el comportamiento de un cuadro de texto y una casilla de verificación. Lograrás crear un formulario con un espacio reservado para la contraseña.

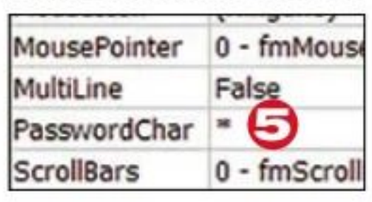
Seguro que estás acostumbrado a los habituales formularios de Internet, en los que debes introducir una contraseña para darte de alta. Lo más normal es que estos, además, vayan acompañados de un icono o casilla que te permite visualizar/ocultar el contenido que introduces en el apartado de la contraseña (normalmente para saber si la has escrito bien o para impedir que otras personas la vean si están viendo lo que escribes). Pues bien, si lo necesitas, puedes emular este mismo comportamiento en un documento de Word. Hazlo así:

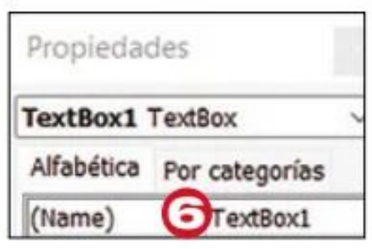
1 Abre el documento de Word que funcionará como un formulario, y coloca el cursor en la zona en la que debe aparecer la contraseña ❶. Haz clic entonces en *Archivo*, *Opciones* y *Personalizar cinta de opciones*. Luego, bajo la lista *Personalizar la cinta de opciones* de la derecha, activa la casilla *Programador* y pulsa *Aceptar*.

2 En la cinta de opciones, elige *Programador*, y pulsa en el icono *Herramientas heredadas* ❷ y luego en el botón *Cuadro de texto* ❸ del apartado *Controles Active X*.

3 Habrá aparecido una zona en la que teclear luego la contraseña ❹. Haz clic en el botón *Propiedades* superior y, en el panel que verás a la izquierda, introduce un asterisco en la propiedad *PasswordChar* ❺. En la parte superior de este mismo panel, verás un texto junto a *Name* ❻ (en este caso, es *TextBox1*). Toma buena nota de él, porque lo utilizarás más tarde.

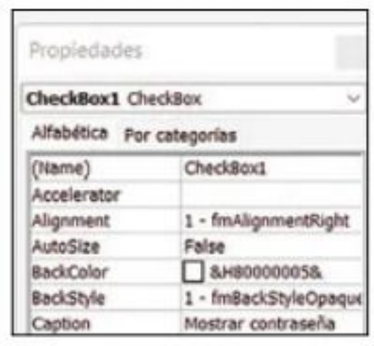




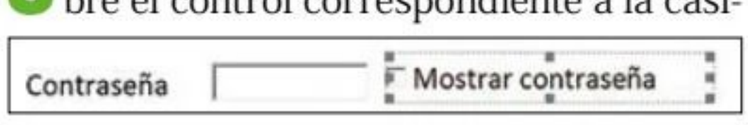


4 Sitúa ahora el cursor a la derecha de la password ❼ y repite el paso 2, pero esta vez elige *Casilla* ❽, para incluir una casilla donde situaste el cursor.

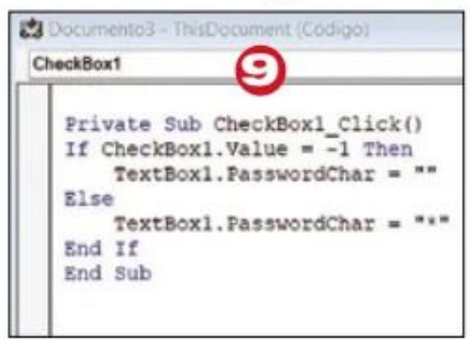
5 Toma nota de su nombre desde el panel lateral de propiedades (en este caso, *CheckBox1*) y cambia lo que aparece a la derecha de *Caption* por el texto que debe mostrar la casilla. Por ejemplo, *Mostrar contraseña*.



6 Ahora, pulsa con el botón derecho sobre el control correspondiente a la casilla y elige la entrada *Ver código*. En la nueva ventana, introduce este código VBA: ❾



Recuerda que donde pone *TextBox1* tú tendrás que poner el texto que apuntaste en el paso 3.



7 Regresa al documento, haz clic en *Modo Diseño* (para desactivarlo) y podrás probar tu formulario. Por ejemplo, introduce una contraseña y verás que aparecen asteriscos ❿. Sin embargo, si activas la casilla adjunta, verás lo que se ha tecleado ⓫. Si la desactivas, se ocultará de nuevo y verás asteriscos otra vez. ■

¡INCLUSO SI ESTÁ EN SILENCIO!

CÓMO LOCALIZAR UN MÓVIL

No saber dónde está tu móvil cuando lo pierdes es una situación muy común que puede causarte mucha frustración. La dificultad para encontrarlo aumenta si está en modo silencio. Afortunadamente, Android cuenta con una función que te permite localizarlo en minutos.

Aprende a...

Localizar tu móvil cuando se encuentra en modo Silencioso y, por ejemplo, no recuerdas dónde lo dejaste. La función 'Encontrar mi dispositivo' te ayudará en esta tarea.

El móvil se ha convertido en un elemento indispensable para la mayoría de las personas. Con él puedes comunicarte, informarte, entretenerte, trabajar y muchas cosas más. Por ende, cuando lo pierdes o te lo roban, automáticamente entras en pánico. **Perder el móvil o no saber dónde** está es algo que le puede suceder a cualquiera, y lo peor de todo es si lo tienes en modo Silencioso y no puedes llamar para escucharlo. ¿Qué puedes hacer en esta situación?

Si tienes un móvil Android, puedes localizarlo de manera fácil y sencilla. Esto se aplica también con tu tablet o reloj inteligente. Con la función llamada ***Encontrar mi dispositivo***, puedes ver la ubicación aproximada de tu smartphone en un mapa, donde podrás bloquearlo, borrar la información de manera remota o hacerlo sonar. Te contamos todos los pasos que debes seguir para lograrlo, ¡ya verás que es muy sencillo!

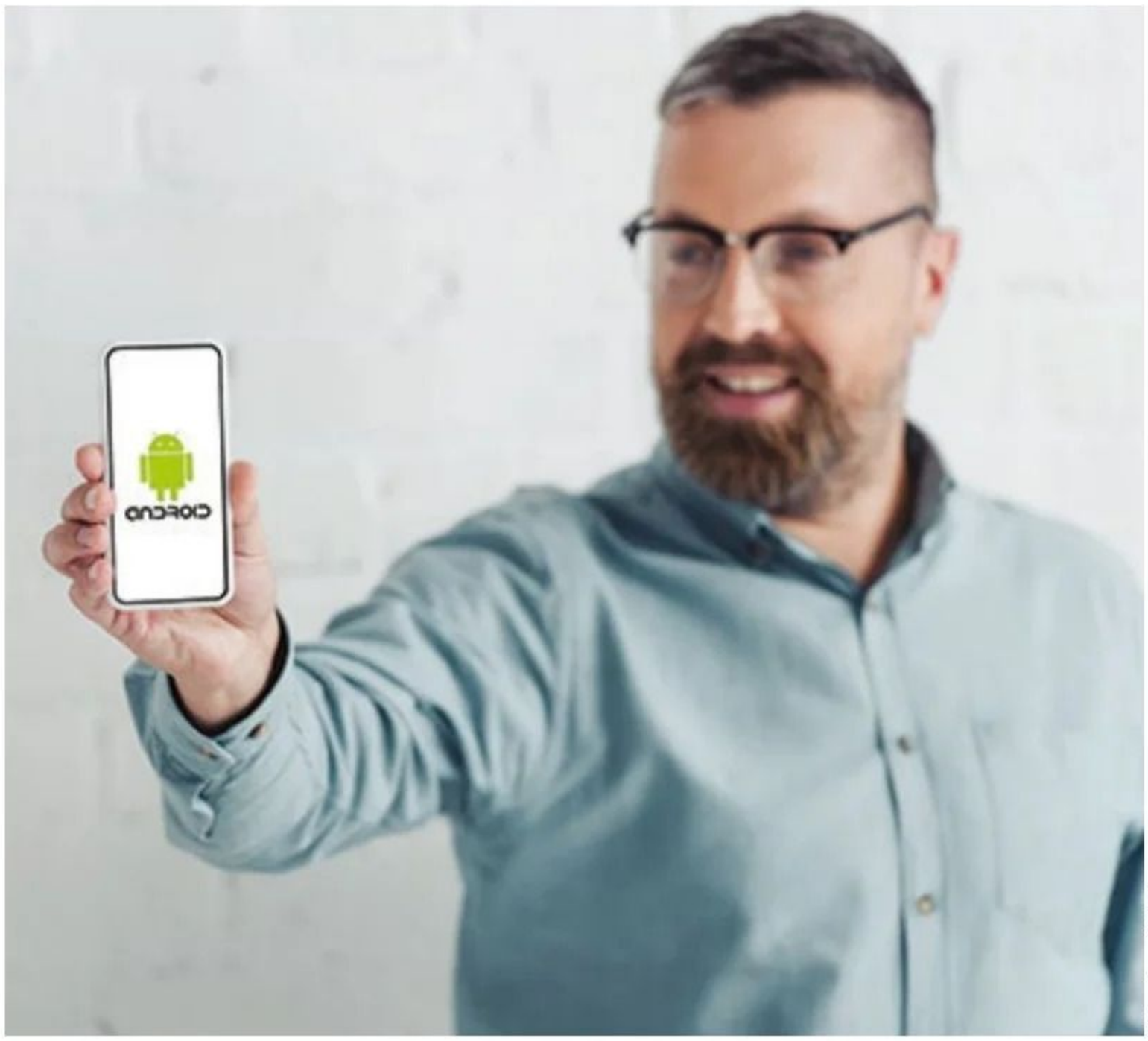


Foto: Depositphotos.com

ENCUENTRA TU MÓVIL PERDIDO

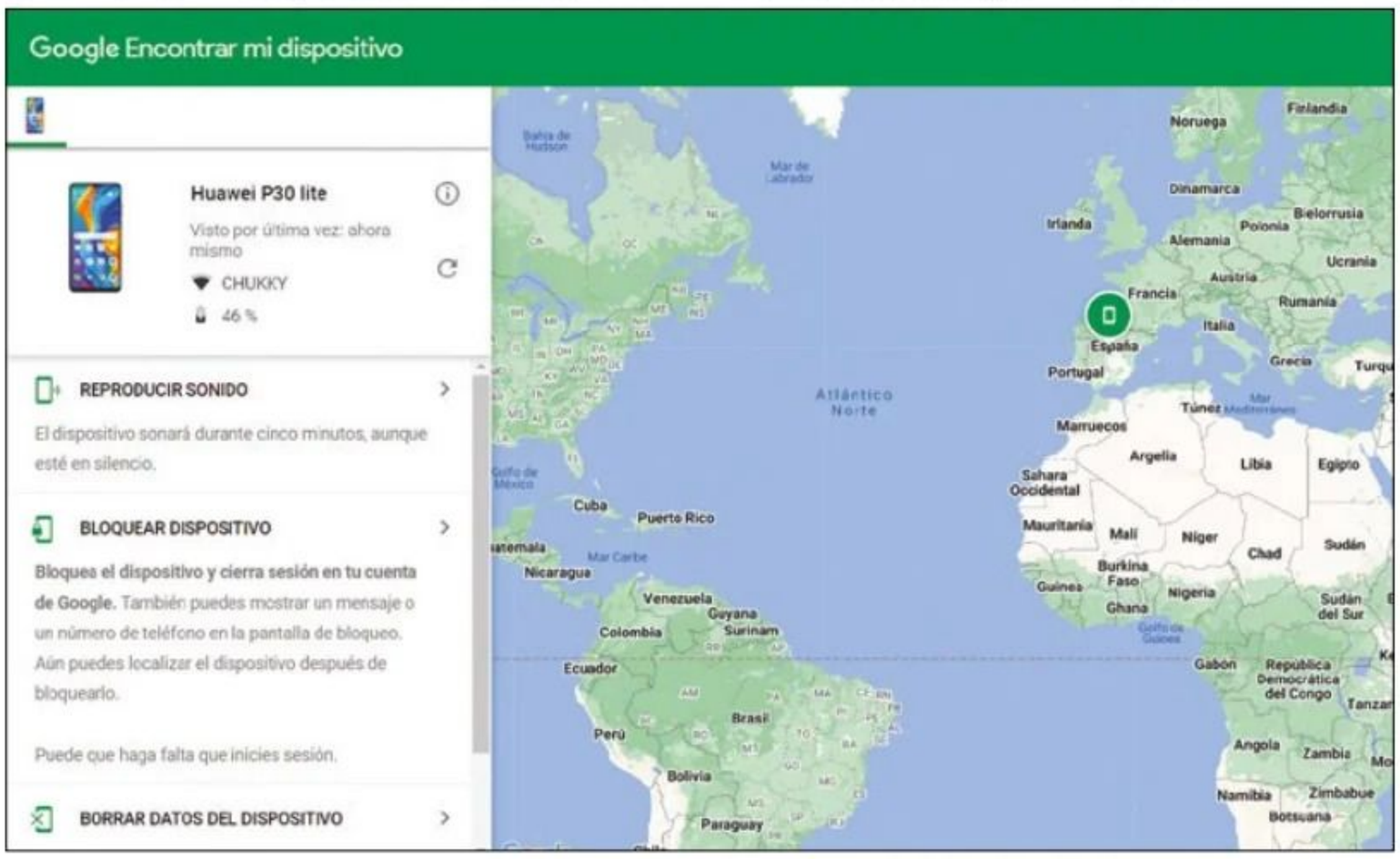
El sistema operativo Android incluye una herramienta muy completa que permite rastrear tu móvil en tiempo real, incluso si está en modo Silencioso, con unos sencillos pasos. El único requisito es contar con un dispositivo Android, así como con una cuenta de Google asociada. La función 'Encontrar mi dispositivo' está disponible en la mayoría de los smartphones Android modernos y también en algunos antiguos. En cualquier caso, debes seguir todos estos pasos:

1 Abre un navegador web en tu ordenador, portátil o tablet e, incluso, en otro teléfono móvil. Visita entonces la página web **google.com/android/find** e inicia sesión en la cuenta de Google vinculada a tu móvil perdido. Si tienes varios dispositivos asociados a esa cuenta, en la parte superior de la barra lateral, podrás elegir el dispositivo que deseas encontrar ahora ❶.

2 En unos instantes, Google localizará tu dispositivo y mostrará su ubicación en

un mapa. Utiliza la rueda central del ratón o los controles de zoom de la parte inferior derecha, para acercarte o alejarte, y así determinar con más precisión su ubicación.

crees que tu teléfono móvil está cerca de ti y necesitas ubicarlo por el sonido. Esto es muy útil cuando lo has perdido en tu hogar o en la casa de algún conocido.



3 Luego, desde el menú lateral izquierdo, selecciona ***Reproducir sonido*** ❷, si

4 Se escuchará entonces el tono habitual de tu llama en volumen alto, para que seas capaz de localizar el dispositivo. Si quieres pararlo (porque ya has encontrado el móvil), pulsa en el botón ***Dejar de hacer sonar*** desde el ordenador. Alternativamente, si has cogido ya el móvil, también puedes pulsar desde él la notificación que verás en la parte superior, y así dejará de escucharse el sonido de localización.

Ten en cuenta que la ubicación que te muestra el mapa es aproximada y puede tener un margen de error de varios metros. Además, la localización en ese momento concreto puede variar según la calidad de la señal GPS o la conexión de tu móvil.

5 Por otro lado, si necesitas bloquear el dispositivo o borrar tus datos, también podrás hacerlo fácilmente en segundos, desde aquí, seleccionando la opción ***Borra datos del dispositivo*** ❸, que también aparece disponible en el apartado de la izquierda.

¿ESTÁ ACTIVADA LA FUNCIÓN DE LOCALIZACIÓN?

Para que puedas llevar a cabo todo lo explicado en este artículo práctico (es decir, la localización de tu smartphone), es necesario que la función correspondiente se encuentre habilitada en el móvil en cuestión. Por defecto, esto suele ser así, pero nunca está de más que lo compruebes previamente, por si en cualquier momento no encuentras tu teléfono y necesitas recurrir a esta opción tan interesante. Para lograrlo, accede a los ***Ajustes*** de tu Android, pulsa en ***Seguridad***, ***Encontrar mi dispositivo*** y activa el regulador ***Activado***, que hallarás disponible en la pantalla que se habrá mostrado ahora.

SOFTWARE ANTI MALWARE

LA GRAN PRUEBA DE SEGURIDAD

En un mundo tan conectado, la protección del PC es más importante que nunca. Computer Hoy te presenta 10 programas que van más allá de la eliminación de virus.

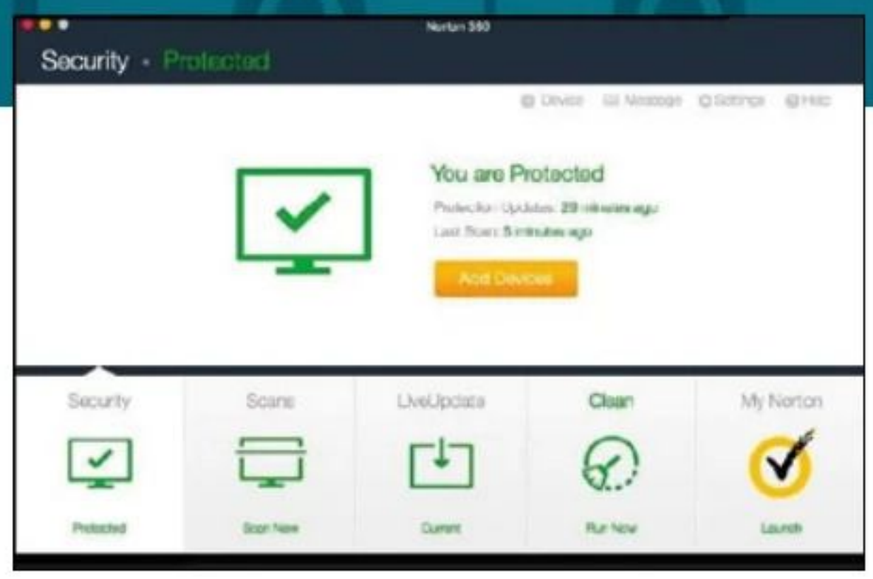
10 SUITES DE SEGURIDAD

DE 2024

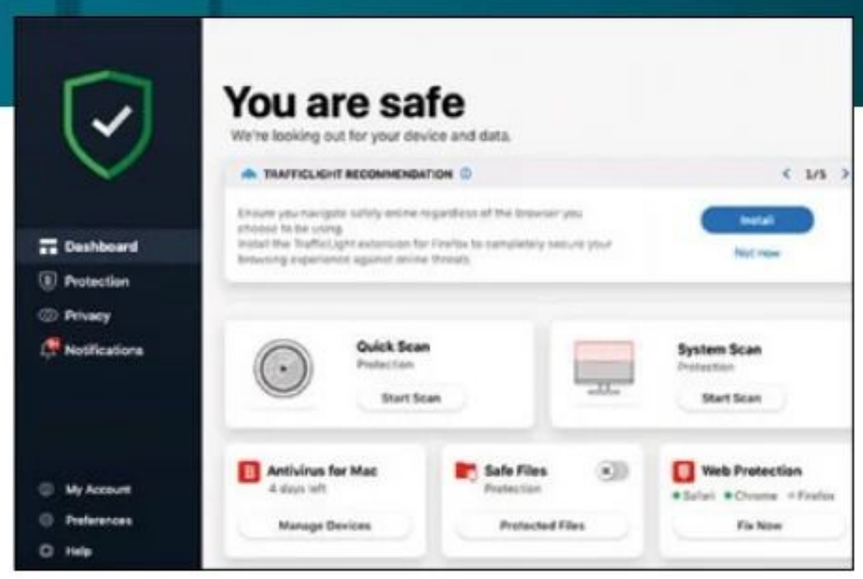
En 2024, la protección antivirus es más importante que nunca. Los delincuentes **encargan malware a grupos de hackers** y la inteligencia artificial se utiliza cada vez más como arma. Casi todos los días hay nuevos intentos de phishing o fraude que los profanos ya no pueden esquivar. Todo ello causa cada vez más perjuicios económicos a particulares y empresas. Con un programa antivirus, puede dejarse la seguridad del PC y otros dispositivos en manos de los profesionales, para seguir navegando, comprando y trabajando con tranquilidad. En esta ocasión, **analizamos en detalle los 10 programas** de protección más importantes. También se incluyen consejos sobre qué tener en cuenta a la hora de adquirir un software antivirus.

Suites completas

La protección antivirus pura resulta suficiente en casos excepcionales. Estamos en 2024 y las amenazas se han diversificado. Por ello, los paquetes completos son protagonistas de esta prueba. Además de antivirus, también se incluyen **módulos adicionales** para proteger la identidad, un gestor de contraseñas, un escáner de vulnerabilidades, protección del entorno y muchas otras herramientas. La gama exacta de funciones difiere de un fabricante a otro. Por tanto, conviene prestar atención a todas las funciones añadidas o a las más necesarias.



El ganador de nuestra prueba, Norton 360 Advanced, ofrece una interfaz de usuario moderna y clara.



Bitdefender Premium Security Plus impresionó en la prueba con sus numerosas funciones adicionales.

Detección de virus

Con la excepción de Eset Home Security Ultimate, todos los candidatos de la prueba recibieron una **calificación buena en detección de virus**. Solo el de Eset quedó un poco por detrás. Esto significa que todos los programas de prueba cumplen su tarea principal de detectar y eliminar malware. No obstante, hay algunas diferencias importantes cuando se entra en detalle. Por ejemplo, el **rendimiento en el laboratorio** del ganador de la prueba, Norton 360 Advanced, es muy bueno y la detección de virus en páginas web reales infectadas del tercer clasificado, Avast One, también destaca frente al resto. Por el contrario, el **análisis sin conexión** a Internet de Microsoft Defender y McAfee+ Ultimate es insatisfactorio. Eset Home Security Ultimate, por su parte, apenas pasó del aprobado en la detección de sitios web muy infectados. Nuestro consejo es, por tanto, echar un vistazo a la tabla completa antes de comprar, para ver si el programa deseado cumple con todo.

Norton vuelve a ganar

Norton 360 Advanced vuelve a salir victorioso y es el merecido ganador de la prueba de este año. La razón principal es el mejor rendimiento de protección, aunque no llegue a ser excelente. Solo Avast One puede igualarlo aquí. Las características de Norton fueron otro factor a su favor. Además, no falló en ninguno de los apartados del test. Sin embargo, la ventaja se está reduciendo con el tiempo. Los nueve primeros candidatos de la prueba de este año **están en un rango muy ajustado** dentro de la clasificación y todos reciben una calificación de notable. Por tanto, este área empieza a ser realmente competitivo y parece que el foco pasará a otras funciones, junto a la invasión de la inteligencia artificial.

Microsoft Defender funciona

La tecnología que Microsoft integra de serie en sus sistemas operativos Windows también recibió una calificación global de notable. La **protección sin coste añadido** se mantiene competitiva en la tasa de detección, en las pruebas de laboratorio. Sin embargo, falla sin conexión a Internet. Además, cuando se trata de detectar malware en sitios web infectados, no alcanza el nivel de los mejores programas de pago. No obstante, ofrece una sólida protección básica en general.

Por otro lado, quien se conforme con Microsoft Defender tiene que prescindir de muchas de las funciones adicionales que contienen los otros programas. Además, el funcionamiento de Defender sigue siendo una cuestión de gustos, ya que el programa está un poco oculto en la configuración de Windows. La interfaz independiente del programa solo está disponible con una suscripción de Microsoft 365, a partir de 69 € al año. Esta es también la única forma de extender Microsoft Defender a los sistemas operativos macOS, Android o iOS.

Innovación con Bitdefender

Todos los candidatos de la prueba contienen mecanismos para detectar phishing y fraudes. Pero Bitdefender es el único fabricante que va un paso más

CUÁNTO CUESTA LA PROTECCIÓN DE TUS DISPOSITIVOS

La jungla de precios de los programas de seguridad es casi imposible de penetrar. No solo las ofertas de los distintos fabricantes difieren enormemente, sino que el número de licencias por paquete tampoco está estandarizado. Para no tener que echar mano de la calculadora, Computer Hoy ha elaborado un resumen en el que se muestra cuánto cobra cada fabricante por el nivel de protección que ofrece y se necesita. Es posible ahorrar mucho dinero, sobre todo adquiriendo un gran número de licencias para varios dispositivos a la vez.

Producto / Precio*	1 LICENCIA	5 LICENCIAS	10 LICENCIAS	20 LICENCIAS
AVAST ONE FAMILY	45,00 €	45,00 €	59,88 €	59,88 €
AVIRA PRIME	59,95 €	59,95 €	119,90 €	129,95 €
BITDEFENDER PREMIUM SECURITY PLUS	**79,99 €**	**79,99 €**	**79,99 €**	**159,98 €**
ESET HOME SECURITY ULTIMATE	119,99 €	119,99 €	144,99 €	289,98 €
F-SECURE TOTAL	69,99 €	99,99 €	199,98 €	399,96 €
G DATA TOTAL SECURITY	49,95 €	81,95 €	163,90 €	327,80 €
KASPERSKY PREMIUM	34,99 €	42,99 €	59,99 €	67,99 €
ESET HOME SECURITY ULTIMATE	119,99 €	119,99 €	144,99 €	289,98 €
MCAFEE+ ULTIMATE	119,95 €	129,95 €	129,95 €	129,95 €
MICROSOFT DEFENDER	N/A[1]	N/A[1]	N/A[1]	N/A[1]

*** Mejor oferta disponible al comprar un número determinado de licencias en la página web del fabricante. / [1] Microsoft Defender está incluido en Windows y, por lo tanto, no hay pago extra.**

allá. Y todo ello gracias a Scamio. Con esta solución, se añade **un chatbot apoyado por inteligencia artificial**. Sirve para ayudar a los usuarios si no están seguros de si algo es fraudulento o no. Pero hay más, porque no es solo para clientes de Bitdefender, ya que está disponible para todo el mundo de forma gratuita. Esta característica ha servido para otorgarle el premio a la innovación en esta edición.

El procedimiento de prueba

La seguridad sigue siendo uno de los temas más importantes para los usuarios de PC. Por ello, las pruebas del software antivirus son fruto de un **intenso y costoso proceso** por parte de AV-Comparatives y esb Rechtsanwälte. Esta es la única manera de garantizar que los programas hacen su trabajo de forma fiable y protegen a sus usuarios contra todas las amenazas de Internet.

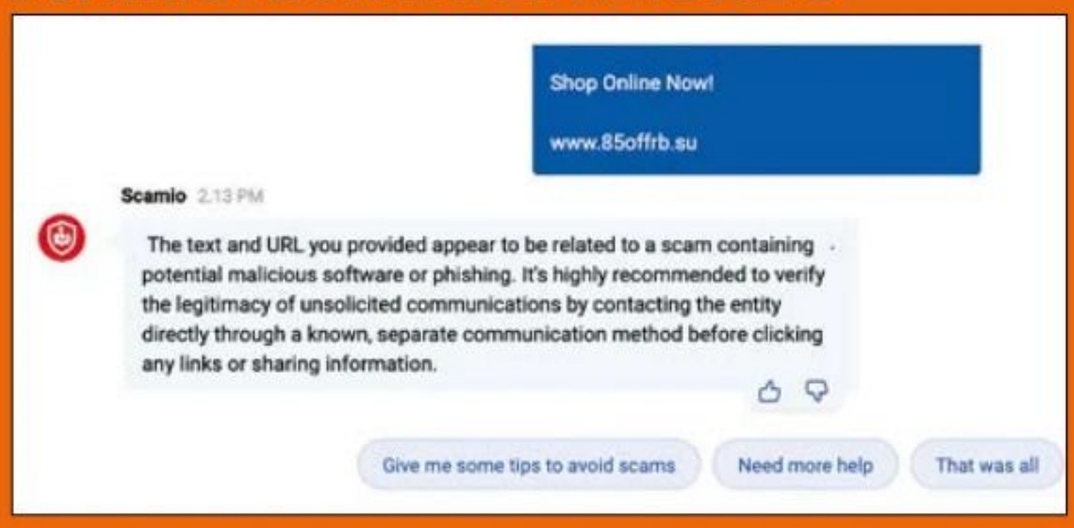
El anonimato de las VPN

Muchos de los candidatos de la prueba ofrecen ahora la opción de una VPN, como función adicional para conectarse de forma anónima. Esto crea un vínculo codificado con los servidores del fabricante, a través de un país seleccionable. Los usuarios pueden utilizarla para protegerse en redes WiFi públicas, por ejemplo, y evitar que se rastreen sus actividades o se creen perfiles publicitarios. Sin duda, se trata de un complemento útil para un programa de seguridad. Sin embargo, los fabricantes de seguridad **se centran en la protección del usuario**. Quien desee utilizar la VPN para ver películas en streaming desde el extranjero o para jugar, puede que le convenga más un software VPN independiente. Suelen ofrecer más funciones y también están diseñados para el consumo de streaming de contenidos multimedia.

CONCLUSIÓN

Todos los programas de la prueba ofrecen un nivel de protección decente. Se trata de un cambio positivo en comparación con el año anterior, que además es urgentemente necesario dada la situación actual de las amenazas en Internet. Una vez más, Norton se sitúa en cabeza con el mejor rendimiento. Bitdefender muestra a los demás fabricantes cómo innovar e introduce una potente función contra el phishing y el fraude en Internet con el chatbot Scamio, que además es gratis y funciona con terceros. La prueba también demuestra que es importante prestar atención a los detalles al comprar un programa de protección, para encontrar la solución adecuada y evitar caer en trampas de pagos innecesarios.

SCAMIO CONTRA **FRAUDES**

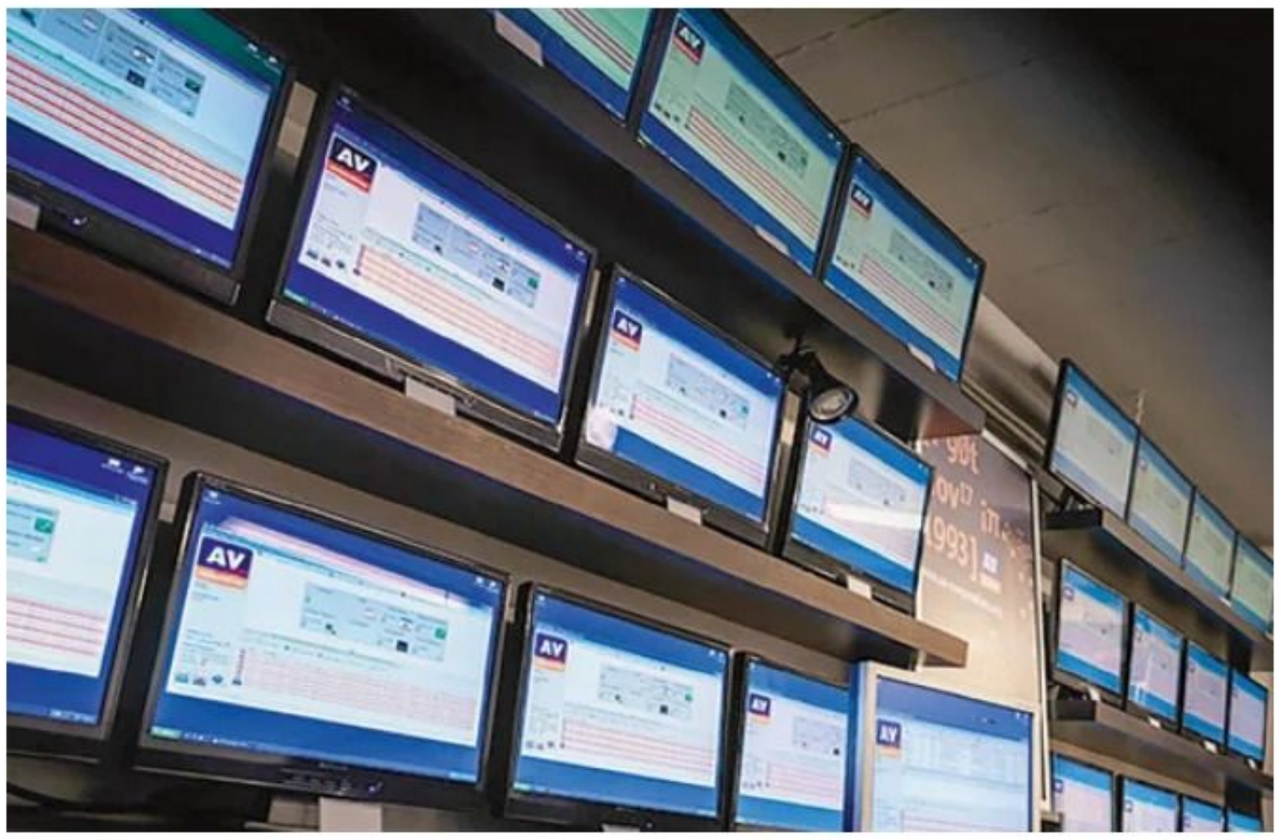


El chatbot Scamio de Bitdefender es una innovación realmente útil. Este bot basado en IA sirve como punto de contacto para cualquiera que no esté seguro de si un correo electrónico que ha recibido es auténtico o una estafa. Los usuarios explican brevemente al bot de qué se trata y luego le envían capturas de pantalla del email. El bot analiza el mensaje y lo compara con estafas conocidas de phishing y fraude. También comprueba criterios laxos, como las fórmulas típicas utilizadas por los ciberdelincuentes. Por supuesto, analiza los enlaces que contiene. A continuación, evalúa si el mensaje es una estafa o si es muy probable que proceda realmente del remitente especificado. Se trata de una función de software antivirus única, de gran ayuda y que puede evitar daños económicos, así como un enorme estrés en el peor de los casos. Por ello, Computer Hoy ha galardonado a Bitdefender Premium Security con el Premio a la Innovación. Scamio es gratuito y un complemento perfecto para todos los candidatos a la prueba. Por el momento, el chatbot solo está disponible en inglés, pero también reconoce el spam y el fraude en otros idiomas. Se puede acceder a él desde la web del fabricante: **bitdefender.com/solutions/scamio.html**.

ASÍ PRUEBA EL LABORATORIO DE COMPUTER HOY

Los programas antivirus son el software más importante en un PC, ya que son la mejor defensa contra todos los peligros de Internet. Por ello, Computer Hoy comprueba intensamente sus funciones de protección. La redacción colabora con el prestigioso laboratorio de pruebas AV-Comparatives. Los candidatos de la comparativa tienen que reconocer y eliminar correctamente **20.022 amenazas de malware durante varios meses** en el laboratorio. Además, en la prueba práctica, que también dura varios meses, hay 1.032 casos en los que los programas tienen que detectar y bloquear archivos en sitios web realmente infectados. Solo los programas que alcanzan índices de detección muy elevados en ambas baterías de pruebas pueden aspirar a una buena clasificación en la tabla.

Es importante que no haya demasiados falsos positivos, ya que los usuarios naturalmente no quieren que se bloqueen o incluso eliminen programas inofensivos. Los encargados analizan, mediante pruebas comparativas, si el software antivirus ralentiza el trabajo diario en el PC. También se comprueba en nuestro propio laboratorio la gama de funciones y la facilidad de uso del software. Incluso el mejor programa de protección es de poca ayuda si los usuarios no entienden lo que tienen que hacer. Ulrich Emmert, abogado especializado en TI de esb Rechtsanwälte, se encargó de supervisar los términos, condiciones y las disposiciones sobre protección de datos.



En el laboratorio de AV-Comparatives, los programas se ejecutan de forma sincrónica y se enfrentan simultáneamente a las amenazas más recientes y peligrosas de Internet.

TRUCOS Y CONSEJOS

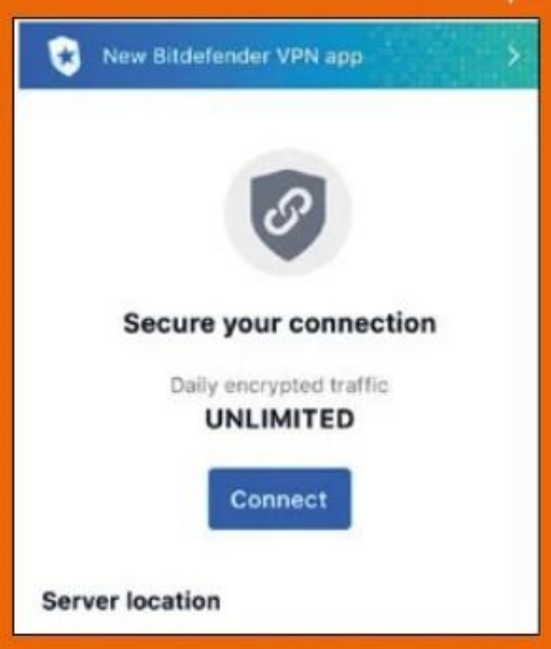
RESPUESTAS A TUS DUDAS

Los resultados de las pruebas son importantes, pero también hay otros factores en los que debes fijarte a la hora de adquirir un programa de seguridad.

¿PARA QUÉ **SISTEMAS OPERATIVOS** SE NECESITA **PROTECCIÓN EXTRA**?

Los sistemas operativos más comunes son a veces muy diferentes. En algunos casos, tanto que las aplicaciones y programas de protección también tienen funciones diferentes. Computer Hoy ofrece aquí una visión general de los sistemas operativos que requieren protección antivirus.

- **Windows:** la protección antivirus es esencial en los sistemas Windows. Son el principal objetivo de los ataques y ofrecen innumerables oportunidades de intrusión. Microsoft Defender o los programas gratuitos pueden considerarse una alternativa a un programa de pago.
- **macOS:** está menos extendido y más compartimentado que Windows. Existen programas antimalware para macOS, pero son menos numerosos. Además, el software de protección no es tan importante para macOS como para Windows. Sin embargo, en macOS te encontrarás con el mismo número de intentos de phishing y fraude, por lo que las funciones adicionales de un programa de protección también garantizan una mayor seguridad en equipos Mac.
- Android: este sistema ofrece aún menos seguridad que Windows. El sistema operativo es bastante abierto, se pueden instalar aplicaciones desde cualquier lugar y a menudo se encuentra malware en la tienda oficial Play Store, disfrazado de aplicaciones útiles. Lo peor de todo es que las actualizaciones de seguridad se publican en diferentes momentos dependiendo del fabricante, y a veces no se lanzan en absoluto. No todos los dispositivos son actualizados por su fabricante mientras son funcionales. Esto es un paraíso para los ciberdelincuentes, por lo que una aplicación antivirus es esencial en Android.
- **iOS:** el sistema operativo de Apple para móviles y tablets está diseñado de tal forma que las aplicaciones individuales solo pueden acceder a otras y a tus datos de forma muy limitada. Esto garantiza que el malware apenas pueda causar daños. Apple ha calificado los antivirus para iOS de superfluos y los ha prohibido a través de sus tiendas oficiales.



¿QUÉ **VERSIÓN DEL SOFTWARE** ES MEJOR?

La mayoría de los fabricantes ofrecen programas de seguridad en tres versiones, que están dirigidas a distintos grupos de usuarios. La más idónea para cada caso dependerá de ciertas necesidades concretas:

- **Antivirus puro:** esta variante suele denominarse simplemente antivirus y también incluye algunos programas gratuitos. Únicamente ofrece protección antimalware, es decir, en tiempo real y sin extras. Por lo general, el PC estará tan bien protegido contra virus como con las variantes más caras. Estos paquetes están dirigidos a quienes solo necesitan una protección mínima o ya utilizan programas de otros fabricantes para los extras que faltan.
- **Seguridad en Internet:** los paquetes de gama media suelen ofrecer protección antivirus, pero también un cortafuegos y algunos extras como funcionalidad VPN o un gestor de contraseñas. Están pensados como una solución general y no incluyen funciones que no sean realmente esenciales para un programa de seguridad.
- **Suites completas:** los paquetes avanzados contienen todo lo que ofrece el fabricante y, por tanto, son soluciones todoterreno sin preocupaciones. Incluyen, por ejemplo, copias de seguridad en la nube, funciones de ajuste y asistencia premium. Estos paquetes están dirigidos a personas que lo quieren todo de un solo proveedor.

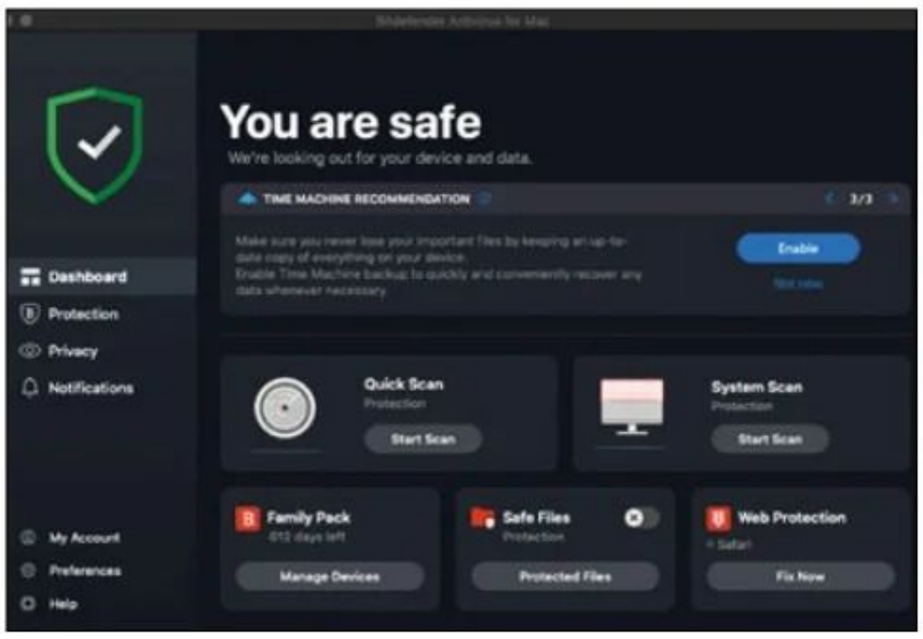
¿MERECE LA PENA **PAGAR POR UN ANTIVIRUS?**

Invertir dinero en protección antivirus depende de lo que se espere de lo que viene a ser una inversión más. Microsoft Defender se ha llevado una nota buena, en general. Las versiones gratuitas de los fabricantes de antivirus suelen utilizar el mismo motor para detectar malware que las versiones más caras. Si solo se quiere detectar malware, estas alternativas pueden ser suficientes. Sin embargo, para quien busque un programa en el que confiar y que se ocupe de todos los aspectos de seguridad, la solución pasa por gastar dinero. Dependiendo del fabricante y del paquete, las versiones adquiridas ofrecen muchas más funciones y advierten de intentos de fraude. También protegen a los menores de contenidos inapropiados. Además, aseguran las contraseñas, encuentran vulnerabilidades en otros programas, mantienen Windows actualizado, avisan si tus datos de acceso han sido pirateados y mucho más. Aparte, los índices de detección de la mayoría de los fabricantes de antivirus son mejores que los de Microsoft Defender. Para Computer Hoy, la solución ideal es un paquete completo, por lo que el fin de esta comparativa es encontrar cuál es el mejor.

¿EN QUÉ HAY QUE FIJARSE **AL COMPRAR?**

Por supuesto, habría que echar un vistazo a la tabla de pruebas antes de comprar. Así se puede asegurar la adquisición de un programa que también ofrezca una protección razonable. Sin embargo, también hay algunas trampas que pueden llegar a costar más de lo necesario:

- **Número de licencias:** la mayoría de los paquetes permite instalar el software en varios dispositivos. El número exacto de licencias lo determina el fabricante. Antes de comprar, por tanto, es importante asegurarse de que se incluyen suficientes licencias para toda la familia y tomar nota de la comparación de los precios finales, para así no invertir demasiado dinero innecesariamente si no procede.
- **Funciones:** las soluciones adicionales también difieren de un fabricante a otro y de una variante a otra. Por eso, hay que asegurarse de que se incluyen todas las necesarias. También, comprobar si existe una versión más barata con las funciones deseadas. Si ya tienes una VPN, por ejemplo, puede haber un paquete al que solo le falte la VPN.
- **Modelos de suscripción:** con muchos fabricantes, junto a la compra se contrata también una suscripción renovada automáticamente. Esta incluye las licencias para solo un año. Aunque dejarla activada es cómodo, la mayoría de los precios de suscripción solo son válidos durante el primer año, después del cual suelen ser más caros. Si se cancela para aprovechar otra oferta, se puede ahorrar mucho dinero.



¿QUÉ **FUNCIONES** SON REALMENTE **ÚTILES?**

Los antivirus ofrecen cada vez más funciones. Muchas de ellas mejoran la seguridad, mientras que otras suelen quedar completamente infrautilizadas. Extras como un gestor de contraseñas, VPN, copia de seguridad, protección de identidad, escáner de vulnerabilidades y actualizador de controladores y software son recomendables para todo el mundo. Mejoran notablemente la seguridad y deberían utilizarse si el paquete los incluye. Otras características como el control parental, la destrucción segura de datos, las funciones para ocultar fotos, el tuneo y similares solo son realmente útiles para determinados usuarios. En general, sin embargo, ningún fabricante integra herramientas completamente inútiles en los paquetes. En este sentido, no es mala idea usar todo lo que se incluye. Bitdefender Premium Security Plus es el más completo.

> A la hora de comprar programas antivirus, hay trampas al acecho en las que no se debe caer.

Carlos Gombau
Redactor Jefe

¿QUÉ DICEN LAS **CONDICIONES LEGALES?**

En Computer Hoy se presta mucha atención a las condiciones generales y la política de privacidad. Estas son revisadas por un abogado. Mientras que la política de privacidad se ocupa de los datos personales y su uso, las CGC regulan la utilización del programa y la responsabilidad. Las malas calificaciones de las CGC casi siempre significan que las cláusulas de responsabilidad no son válidas. Esto suele ocurrir cuando los fabricantes solo traducen las disposiciones del inglés, pero no las adaptan a la legislación española. Si una cláusula de responsabilidad no es válida, significa que en su lugar puede aplicarse lo que haya estipulado el legislador. En la mayoría de los casos, esto es mejor para el cliente final que lo que no es válido. Si se tiene un litigio con un fabricante cuyas condiciones generales son deficientes, es aconsejable consultar a un abogado y no dejarse engatusar con una referencia a las condiciones generales. Al fin y al cabo, el fabricante puede ser responsable. Sin embargo, esto solamente merece la pena si el importe en litigio supera los honorarios del abogado.

Foto: Depositphotos.com

LA PRUEBA EN DETALLE

Índices de detección, funciones adicionales, uso... Hay mucho a tener en cuenta con los programas antivirus. Aquí está la comparación de los 10 candidatos de la prueba.

1 NORTON 360 ADVANCED

Precio: 39,99 €
Otra opción: 14,99 €

Compatibilidad: Windows, macOS, Android e iOS

Norton impresiona en la prueba con la mejor protección antivirus y grandes prestaciones. El software apenas ralentiza el PC. El único punto de crítica importante es la detección de virus sin conexión a Internet. En general, el producto sigue siendo el mejor programa de protección del mercado y, por tanto, el merecido ganador de la prueba.

+ La mejor protección antivirus, la mejor prueba de laboratorio, extras.

− Detección deficiente sin conexión a Internet.

2 AVIRA PRIME

Precio: 59,95 €
Otra opción: ninguna

Compatibilidad: Windows, macOS, Android e iOS

Es ligeramente peor que Norton, en lo que respecta a la detección de virus. Sin embargo, no hay nada que criticar del paquete de programas en ninguna categoría. Por tanto, queda justo por detrás del ganador de la prueba y ofrece un paquete completo. Es la primera elección para cualquiera que necesite escanear sin Internet.

+ Buena protección antivirus, mensajes claros.

− Nada digno de mención.

3 AVAST ONE

Precio: 45,00 €
Otra opción: ninguna

Compatibilidad: Windows, macOS, Android e iOS

Está a la altura del ganador de la prueba en la detección de virus e, incluso, le supera en la identificación de los mismos en sitios web infectados. El funcionamiento y los mensajes de advertencia podrían mejorarse. No siempre son intuitivos y fáciles de entender. Sin embargo, en general, Avast One merece estar entre los tres mejores candidatos.

+ La mejor protección antivirus, la mejor detección de páginas infectadas.

− Funcionamiento incómodo.

4 KASPERSKY TOTAL SECURITY

Precio: 34,99 €
Otra opción: 19,99 €

Compatibilidad: Windows, macOS, Android e iOS

La solución de Kaspersky sigue siendo objeto de una advertencia por parte de algunas agencias de seguridad y Gobiernos debido a su origen ruso. Por lo demás, ofrece una buena detección de virus, las mejores funciones y la menor ralentización. Un punto importante de crítica es que sus mensajes son los menos comprensibles del test.

+ Buena protección antivirus, las mejores funciones.

− Mensajes de aviso incomprensibles.

5 BITDEFENDER PREMIUM SECURITY PLUS

Precio: 79,99 €
Otra opción: ninguna

Compatibilidad: Windows, macOS, Android e iOS

Bitdefender ofrece muchos extras y demuestra una buena detección de virus que no se ralentiza incluso sin conexión a Internet. Los mensajes de advertencia son a menudo incomprensibles. En general, sin embargo, la suite es un paquete de protección fiable y es perfecta para aquellos que quieren todas las funciones de una sola fuente.

+ Buena protección antivirus, buenas e innovadoras funciones.

− Mensajes de aviso incomprensibles.

	1 NORTON 360 ADVANCED	2 AVIRA PRIME	3 AVAST ONE	4 KASPERSKY TOTAL SECURITY	5 BITDEFENDER PREMIUM SECURITY PLUS
RENDIMIENTO					
	Mejor protección en el laboratorio, buena detección en páginas infectadas, algunos falsos positivos — 8,80	Buena detección en el laboratorio y en lugares contaminados, casi sin falsos positivos — 8,00	Buena detección en el laboratorio, muy buena en lugares contaminados, casi sin falsos positivos — 8,80	Buena detección en el laboratorio y en lugares contaminados, casi sin falsos positivos — 8,20	Buena detección en el laboratorio y en lugares contaminados, casi sin falsos positivos — 8,20
FUNCIONES					
	Cortafuegos, VPN, control parental, asistente de actualizaciones, cloud backup, gestor de contraseñas — 7,60	Cortafuegos, VPN, escáner de vulnerabilidades, asistente de actualizaciones, gestor de contraseñas — 7,20	Cortafuegos, VPN, escáner de vulnerabilidades, asistente de actualizaciones, eliminador de rastro — 6,40	Cortafuegos, VPN, control parental, escáner de vulnerabilidades, asistente de actualizaciones, cloud backup, eliminador de rastro, gestor de contraseñas — 9,40	Cortafuegos, VPN, control parental, escáner de vulnerabilidades, protección antirrobo, asistente de actualizaciones, gestor de contraseñas, IA — 8,40
CARGA DEL SISTEMA					
	Casi imperceptible — 9,40	Casi imperceptible — 9,80	Casi imperceptible — 9,40	Casi imperceptible — 9,80	Casi imperceptible — 9,60
MANEJO					
	Funcionamiento algo engorroso, mensajes a veces incomprensibles — 7,00	Funcionamiento algo engorroso, mensajes fáciles de entender — 7,80	Funcionamiento engorroso, mensajes a veces incomprensibles — 4,80	Funcionamiento engorroso, mensajes raramente comprensibles — 4,00	Funcionamiento algo engorroso, mensajes a menudo incomprensibles — 4,20
Notable	8,40	8,20	8,00	7,80	7,80
	39,99 €	59,95 €	45,00 €	34,99 €	79,99 €

COMPUTER HOY RESPONDE:

¿Cuál es el tipo de malware que resulta más peligroso?

Los virus de extorsión (ransomware) son los programas maliciosos más peligrosos de Internet. Cifran y roban datos y solo prometen que los liberarán a cambio de un alto rescate.

¿Qué significa phishing?

El phishing es el robo de datos privados de acceso. Los delincuentes utilizan correos electrónicos, mensajes o llamadas telefónicas fraudulentas. Al igual que el fraude (estafa) que implica dinero, el phishing supone la mayor amenaza para los particulares.

¿Utilizan los hackers inteligencia artificial?

Cada vez más ciberdelincuentes utilizan herramientas de inteligencia artificial. Estas van desde simples traducciones de textos hasta voces o vídeos falsos. Por ejemplo, los atacantes usan voces por IA para hacerse pasar por los hijos de la víctima y exigir dinero por una supuesta situación de emergencia. O amenazan con distribuir vídeos pornográficos creados artificialmente. En algunos casos, las IA también escriben código malicioso para los hackers.

6 MCAFEE
MCAFEE+ ULTIMATE
Precio: 119,95 €
Otra opción: 49,95 €

Compatibilidad: Windows, macOS, Android e iOS

Demostró buenos índices de detección en el laboratorio y en sitios web infectados. Sin conexión a Internet, la suite falla, pues más del 22 % de todos los programas maliciosos consiguen pasar. Los otros candidatos lo hacen mejor. Sin embargo, McAfee ofrece una sólida protección antivirus para quienes siempre están conectados.

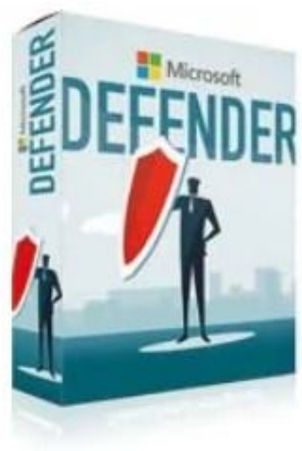
- + Buena protección antivirus.
- − Detección deficiente sin conexión a Internet.

7 G DATA
TOTAL SECURITY
Precio: 49,95 €
Otra opción: 29,95 €

Compatibilidad: Windows, macOS, Android e iOS

También ofrece una buena protección antivirus, incluso la mejor en la prueba sin conexión. Sin embargo, los mensajes de advertencia son a menudo incomprensibles. G Data también da la menor gama de funciones de la prueba. Pero, si no se necesitan los extras que le faltan, G Data Total Security también es un buen programa de protección.

- + Buena protección antivirus, la mejor protección sin Internet.
- − El equipamiento menos completo.



8 MICROSOFT
DEFENDER
Precio: gratuito
Otra opción: ninguna

Compatibilidad: Windows*

La protección gratuita incluida en Windows está a la altura de los demás candidatos en la prueba de laboratorio de este año. Sin embargo, no funciona bien en sitios web infectados y falla cuando se pierde la conexión a Internet. En general, el programa sigue obteniendo un notable y es una gran protección básica para Windows.

- + Buena protección antivirus, gratuito.
- − Poca protección sin conexión a Internet.

9 F-SECURE
TOTAL
Precio: 69,99 €
Otra opción: 49,99 €

Compatibilidad: Windows, macOS, Android e iOS

F-Secure vuelve al campo de pruebas después de mucho tiempo. Brilla con las mejores tasas de detección en sitios infectados y no comete errores importantes. En la prueba real de laboratorio, sin embargo, no puede competir con los mejores. También podría ser más intuitivo de usar. No obstante, pese a todo, resulta un buen paquete de protección.

- + Buena protección antivirus, la mejor detección de páginas infectadas.
- − Funcionamiento engorroso.

10 ESET HOME SECURITY ULT.
Precio: 119,99 €
Otra opción: 29,99 €

Compatibilidad: Windows, macOS, Android e iOS

Eset ha mejorado notablemente respecto al año anterior y vuelve a ofrecer buenos índices de detección en la prueba controlada de laboratorio e, incluso, sin conexión a Internet. Por desgracia, la defensa contra el malware en sitios web infectados cambia, con una protección limitada. Por lo tanto, en conjunto, se queda por detrás del resto.

- + Apenas hay ralentización.
- − Protección inadecuada en páginas infectadas.

Buena detección en el laboratorio y en lugares contaminados, casi sin falsos positivos	8,00	Buena detección en el laboratorio y en lugares contaminados, casi sin falsos positivos	8,20	Buena detección en el laboratorio, algo deficiente en lugares contaminados, casi sin falsos positivos	7,40	Detección algo pobre en el laboratorio, muy buena en lugares contaminados, algunos falsos positivos	7,20	Buena detección en el laboratorio, mala en lugares contaminados, casi sin falsos positivos	6,40
VPN, control parental, eliminador de rastro, gestor de contraseñas	7,00	Cortafuegos, control parental, asistente de actualizaciones, cloud backup, eliminador de rastro, gestor de contraseñas	4,80	Control parental, protección antirrobo, asistente de actualizaciones, cloud backup, eliminador de rastro, gestor de contraseñas	6,00	VPN, control parental, gestor de contraseñas	6,20	Cortafuegos, VPN, control parental, protección antirrobo, gestor de contraseñas	7,00
Casi imperceptible	9,20	Algo perceptible	9,00	Algo perceptible	7,80	Algo perceptible	8,80	Casi imperceptible	9,80
Funcionamiento engorroso, mensajes a veces incomprensibles	6,00	Un poco incómodo de usar, mensajes a menudo incomprensibles	5,20	Funcionamiento engorroso, mensajes a veces incomprensibles	6,20	Funcionamiento complicado, mensajes bastante comprensibles	6,00	Funcionamiento algo engorroso, mensajes a veces incomprensibles	5,40
Notable	7,60	**Notable**	7,40	**Notable**	7,20	**Notable**	7,20	**Bien**	6,60
119,95 €		**49,95 €**		**0,00 €**		**69,99 €**		**119,99 €**	

* Microsoft Defender para macOS, Android e iOS solo está disponible con una suscripción a Microsoft 365.

1Password bitwarden

A PRUEBA 6 GESTORES DE CONTRASEÑAS

¿DÓNDE APUNTÉ LA CONTRASEÑA?

Los gestores de contraseñas protegen las claves de tus cuentas online. Computer Hoy ha puesto a prueba los seis más importantes y ahora te revela cuál es el más fiable.

A todos nos ha pasado: cuando te conectas a una nueva página web, necesitas crear una contraseña que sea lo más segura posible. Pero por comodidad, mucha gente vuelve a elegir la antigua, quizá con un pequeño añadido que se adapte al sitio. Y es comprensible, porque nadie puede recordar una contraseña para cada una de sus **innumerables cuentas** de usuario. Aunque solo rotes unas pocas claves entre tus servicios, antes o después acabarás en el botón 'He olvidado mi contraseña' y tendrás que restablecerla.

Los gestores de contraseñas ofrecen una solución: los usuarios solo tienen que recordar una única contraseña maestra y el programa crea automáticamente una contraseña segura para cada página, además de encargarse de guardarla. Y lo mejor es que la contraseña se introduce automáticamente la próxima vez que visitas el sitio. Esa es la teoría. Computer Hoy ha probado seis de los gestores de contraseñas más importantes para comprobar su eficacia.

Más seguridad gracias a los gestores de contraseñas

Este tipo de programas no solo resultan prácticos, sino que también aumentan tu propia seguridad en Internet. Ten en cuenta que los ciberdelincuentes lanzan cada vez más intentos de **phishing y fraude** para obtener datos de acceso. Y la tasa de éxito también aumenta 'gracias' a la ayuda de la IA. Muchos sitios falsos apenas pueden distinguirse del original, y aquí es donde los gestores de contraseñas pueden ayudar. Reconocen los sitios originales e introducen allí automáticamente los datos y contraseñas almacenados. Si esto no ocurre, se da la voz de alarma al usuario: lo más probable en ese caso es que se trate de un sitio web falso.

Además, los fabricantes de los gestores de contraseñas analizados buscan en la **Darknet delictiva** datos robados y comprueban si la información de acceso del usuario aparece allí. Si es así, emiten una advertencia inmediatamente. En ese caso, será necesario actuar de inmediato antes de que los hackers accedan a las cuentas afectadas.

NordPass gana la prueba

La solución de Nord Security se impuso en la comparativa. Con una puntuación en la prueba de 'Sobresaliente' y una ventaja mínima, el programa se hizo con el primer puesto. NordPass fue el ganador principalmente porque ofrece todas las funciones importantes. Además, el programa se puede utilizar de forma intuitiva y requiere poco esfuerzo para familiarizarte.

Todos con un buen nivel

Sin embargo, los demás candidatos de la prueba también consiguieron calificaciones que van de 'Sobresaliente' a 'Notable'. La mayoría de las funciones importantes, como el inicio de sesión biométrico, la protección contra la Darknet, la sincronización entre varios dispositivos o el almacenamiento de los datos de la tarjeta de crédito y otra información importante están **incluidas en todos los candidatos** de nuestra prueba. Hay algunas diferencias en las funciones adicionales, como la facilidad de manejo y los precios. Por ello,

AÑADE LA **AUTENTICACIÓN** DE DOS FACTORES

Las contraseñas seguras son imprescindibles, pero por sí solas no bastan para protegerte. Los piratas informáticos también pueden adivinar contraseñas seguras mediante ensayo y error o robarlas tras hackeos reales. Por eso es importante un segundo factor que garantice que solo tú tienes acceso a tus cuentas. Si el inicio de sesión con dos factores está activado, las contraseñas capturadas son relativamente inútiles. Por lo tanto, activa el inicio de sesión de doble factor siempre que veas la opción, ya es posible con casi todas las cuentas online importantes.

PASSKEYS: ¿LA ALTERNATIVA A LAS CONTRASEÑAS?

Las passkeys son un nuevo método de inicio de sesión en el que solamente debes conectarte con tu teléfono móvil, sin necesidad de contraseñas, ni en un servidor ni en tus dispositivos. Funciona mediante pares de claves y es una alternativa segura a la utilización de las habituales contraseñas. Mientras que compañías importantes como Google, Apple, Microsoft, PayPal y otras ofrecen ya este método, todavía quedan muchos servicios y empresas pendientes de adoptarlo. Todo indica que pasará algún tiempo antes de que las passkeys puedan sustituir a las contraseñas.

si quieres comprar un gestor de contraseñas, lo primero que debes buscar son los extras que deseas y luego **esperar una oferta**, porque siempre terminan disponibles a precios más bajos en lanzamientos especiales.

Solamente gestores

Solo hemos probado programas independientes. Algunos navegadores y sistemas operativos también tienen sus propios **gestores integrados**, como Chrome o iOS. Son gratuitos, pero no pueden hacer mucho más que almacenar contraseñas. Por ejemplo, muchos de estos gestores no permiten hacer copias de seguridad de otros datos importantes, y sincronizar varios dispositivos puede ser engorroso. Tampoco todos avisan de contraseñas inseguras o comprometidas. En resumen, estos gestores de contraseñas no siempre ofrecen lo que los usuarios esperan. Y a menudo solamente están diseñados para su uso en un dispositivo.

¿Proveedores hackeados?

Por otra parte, a alguno quizá le sorprenderá saber que otorgamos una buena calificación a LastPass. Después de todo, **sufrió dos ciberataques exitosos**. En 2021, los delincuentes probaron en LastPass grandes cantidades de datos de acceso obtenidos de la Darknet. En 2022, hubo un hackeo durante el que los ciberdelincuentes pudieron sustraer 'bóvedas' cifradas de usuarios del programa. Esto es, por supuesto, el mayor desastre posible para un gestor de contraseñas que se supone que proporciona seguridad. El acceso al almacén de contraseñas de los usuarios fue posible porque el malware robó previamente los datos de acceso de un administrador de LastPass. Los atacantes lo usaron para acceder al sistema y copiar los datos cifrados. Sin embargo, LastPass reaccionó inmediatamente e **informó del robo de datos**.

En septiembre de 2023, surgieron sospechas de que los hackers habían descifrado las bóvedas robadas de los servidores de LastPass y las habían utilizado para saquear monederos de criptomonedas. No se sabe si esto es cierto. Sin embargo, transcurrió casi un año y medio entre el llamamiento de LastPass a los usuarios para que cambiaran sus contraseñas y el supuesto robo de las cámaras acorazadas.

Así que cualquiera que **respondiera a las múltiples advertencias de LastPass** no debería haber sufrido ningún daño, al menos en este caso. Y seamos honestos: todo sistema puede ser crackeado, lo que también incluye al resto de fabricantes. Lo importante es que los desarrolladores hacen mucho para evitar que esto ocurra y proporcionan información transparente, como el caso de LastPass. Y claro, estos gestores **siempre son mejores** que las contraseñas inseguras.

CONCLUSIÓN

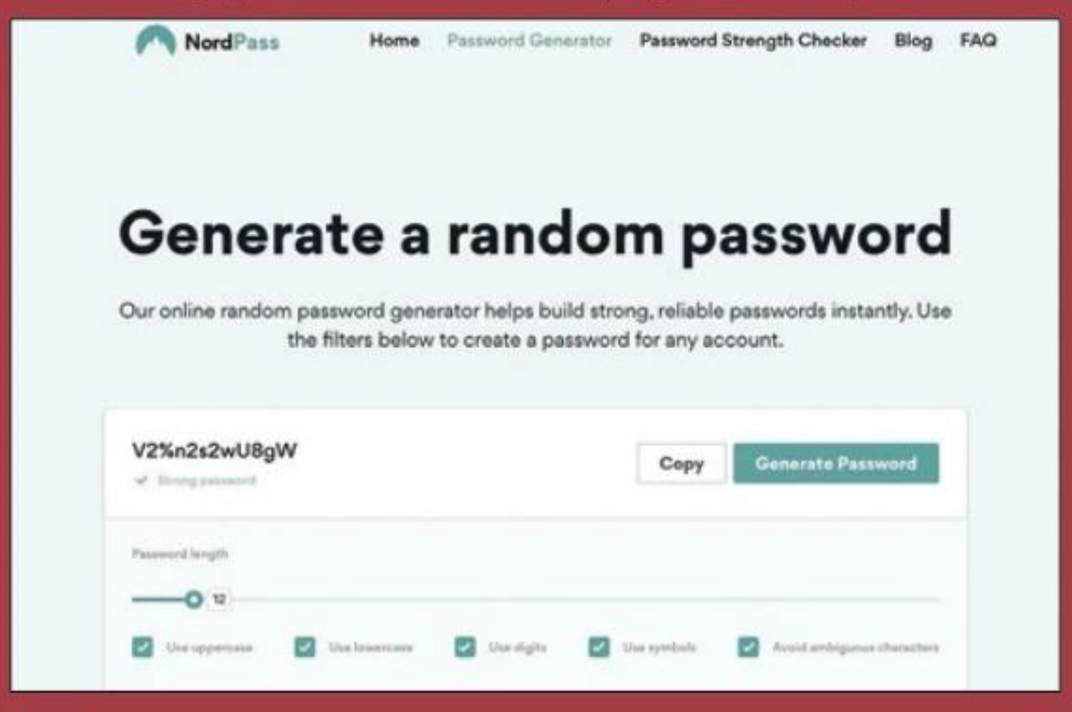
Los gestores de contraseñas hacen la vida online del usuario más cómoda y segura. En nuestro test, NordPass se ha impuesto gracias a su intuitivo menú de navegación y sus buenas funciones, pero la competencia le pisa los talones al ganador de la prueba. Todos los candidatos obtienen como mínimo un 'Notable' y están perfectamente adaptados para su uso en PC, portátiles y smartphones.

¡NECESITAS SABERLO!

Contraseñas seguras, suscripciones, extras... Respondemos ahora las preguntas más importantes sobre los gestores de contraseñas.

¿CÓMO PUEDO CREAR CONTRASEÑAS SEGURAS?

Por supuesto, un gestor de contraseñas solo tiene sentido si también utilizas en él contraseñas seguras. Por un lado, esto significa que debes utilizar una clave diferente para cada página y que realmente solo se utilice allí. En segundo lugar, no debes utilizar números ni caracteres mnemotécnicos para las contraseñas. A estas alturas no debería ser necesario recordar que debes evitar fechas de nacimiento, palabras reales o palabras en las que hayas sustituido letras por números. Esta clase de medidas facilita a los atacantes averiguar la contraseña correcta por ensayo y error o mediante la utilización de listas de palabras. Una contraseña segura se compone aleatoriamente de letras, números y caracteres especiales. La longitud también es importante: cuanto más corta sea la contraseña, más fácil será descifrarla.
Organismos expertos como el Instituto Nacional de Ciberseguridad (INCIBE) recomiendan un mínimo de ocho caracteres al tiempo que aconsejan el uso de software como el que analizamos en esta prueba. Gracias a estos programas, no tienes que escribir cada vez salvajemente en el teclado para crear o introducir una contraseña segura, ellos se encargan de hacerlo por ti. Cómo funciona esto exactamente depende del fabricante, pero cada vez que creas una nueva cuenta, el programa suele ofrecerte una clave generada que puedes simplemente adoptar o crear una diferente mediante el generador de contraseñas que encontrarás en el menú. Importante: si estrenas un gestor de contraseñas, este adoptará tus datos de acceso existentes para facilitarte las cosas. Sin embargo, lo más aconsejable es que crees contraseñas nuevas y seguras para las cuentas ya existentes, y que se renueven en las páginas correspondientes.



¿QUÉ DEBO TENER EN CUENTA A LA HORA DE SUSCRIBIRME?

Los gestores de contraseñas están disponibles en muchas versiones diferentes, con distintas funcionalidades y para distintos números de cuentas. En cuanto a la gama de funciones, consulta las preguntas de la página de la derecha. Ten presente que en estos programas, el número de cuentas no se refiere al número de dispositivos en los que se utiliza el gestor; no hay límite definido para ello. Se refiere más bien a los usuarios individuales. Necesitas una cuenta distinta para cada miembro de la familia que quiera utilizar el gestor de contraseñas. Así evitarás, por ejemplo, que tus hijos accedan a PayPal con tus datos. Por tanto, asegúrate de que se incluyen suficientes cuentas en tu plan.
Algunos fabricantes ofrecen licencias de por vida. Cuestan más o menos lo mismo que una suscripción única de dos a cuatro años. Si estás satisfecho con el programa, no hay nada que decir en contra de una licencia vitalicia o de un plan por varios años, pero fíjate bien en la suscripción: algunos de los precios solo son válidos durante un período de tiempo limitado, como el primer año o los dos primeros. Si no cancelas antes y cambias de plan, la suscripción seguirá vigente al precio más alto. Y si cobran mensualmente, muchos ni siquiera saben cuándo termina el periodo de descuento y solo se dan cuenta del aumento más tarde.

> Sin un gestor de contraseñas, te complicas innecesariamente la vida y facilitas las cosas a los atacantes.

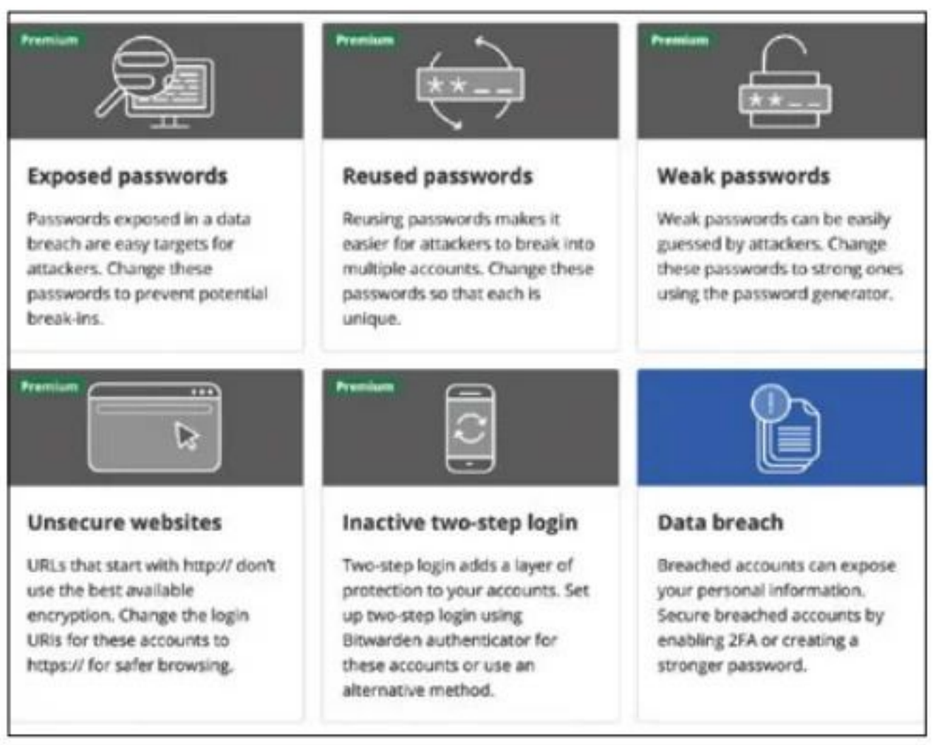
Carlos Gombau
Redactor Jefe

¿ES **GRATUITO** ESTE SOFTWARE?

También existen gestores de contraseñas gratuitos. Entre ellos están los gestores de contraseñas de navegadores y sistemas operativos (ver página anterior), las versiones gratuitas de los servicios aquí probados y programas de código abierto como KeePass. Igualmente, hay gestores de contraseñas que forman parte de programas antivirus (aunque no son gratuitos, pueden estar incluidos en la licencia). Los servicios gratuitos suelen ofrecer menos funciones y menos comodidad. Los servicios aquí probados incluyen casi todo lo que se puede esperar de un gestor de contraseñas e incluso más (ver la tabla de la página siguiente). Sin embargo, si solo te interesa guardar contraseñas y rellenarlas automáticamente, los programas gratuitos pueden ser una alternativa para ti. Por cierto, la mayoría de los de pago ofrecen una versión de prueba temporal para probar sus virtudes.

¿QUÉ HAGO ANTE UNA **EMERGENCIA**?

A pesar de los gestores de contraseñas y de todas las medidas de protección que decidas tomar, puede ocurrir que alguien se cuele en tus cuentas online y consiga acceder a ellas, ya sea a través de brechas de seguridad, hackeos o sencillamente buena suerte adivinando contraseñas. En estos casos, debes actuar con rapidez y limitar los daños. Esto significa cerrar la sesión cuanto antes, pero si no es posible restablece la contraseña. Cambia también la clave por una nueva y segura y, al mismo tiempo, si hay datos de pago almacenados en la cuenta afectada, informa a tu banco o al proveedor de tu tarjeta de crédito. A continuación, mira lo que han hecho los intrusos y toma medidas, por ejemplo, informando a tus amigos de que los correos electrónicos enviados no proceden de ti. Puedes saber qué más hacer y cómo aumentar la protección de tus cuentas con los recursos de la web de INCIBE, **www.incibe.es**.



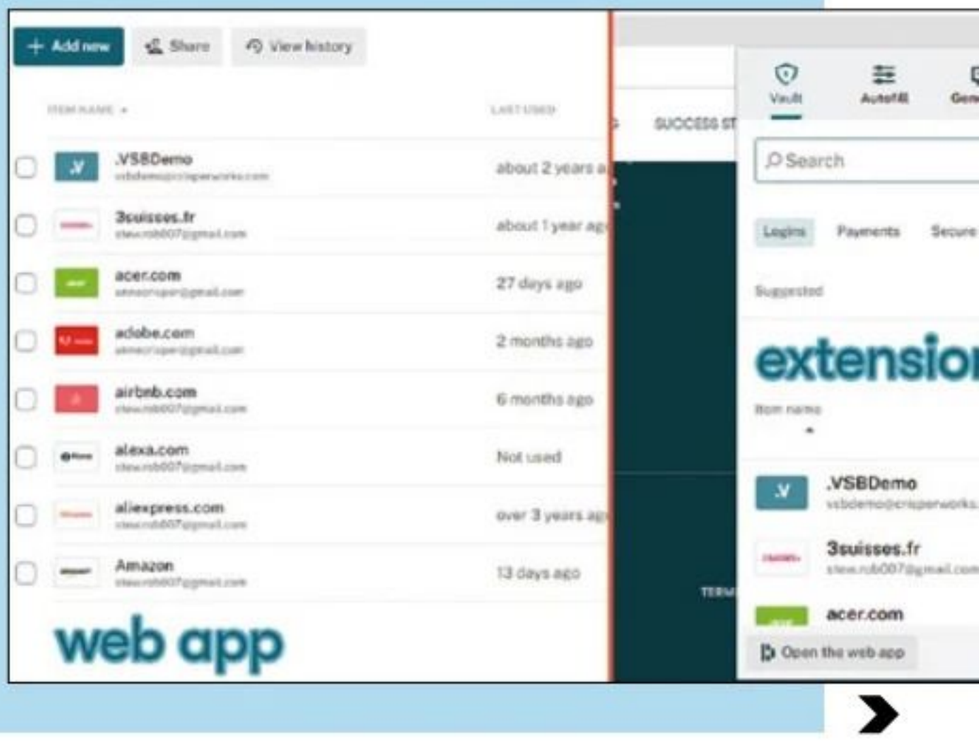
¿TIENEN **ALGÚN TIPO DE EXTRA** LOS GESTORES DE CONTRASEÑAS?

Los gestores de contraseñas ofrecen muchas funciones adicionales que van más allá de simplemente rellenar y guardar los datos de acceso. Las siguientes funciones no deberían faltar en ellos:

- **Función de recuperación:** te permite restablecer tu contraseña maestra si la olvidas. Y no es algo que puedas garantizar que no va a ocurrir...
- **Protección de dos factores:** es muy poco probable, pero no imposible, adivinar una contraseña maestra segura. Por tanto, es más que obligatorio el uso de la verificación con un segundo factor, como el smartphone.
- **Biometría:** es incluso mejor abrir la caja fuerte de contraseñas con huella dactilar o reconocimiento facial, ya que resulta más cómodo y más seguro.
- **Protección Darknet:** las alertas sobre contraseñas que hayan sido comprometidas son importantes y evitan, o al menos limitan, los daños.

¿**EXTENSIÓN** EN EL NAVEGADOR O **CLIENTE** DE ESCRITORIO?

Algunos programas, como Dashlane, funcionan completamente en el navegador. Otros, como NordPass, son programas independientes, pero pueden utilizar una extensión del navegador para introducir y guardar contraseñas. Gestionar las contraseñas directamente en el navegador puede ser más práctico que abrir un programa adicional, aunque los clientes de escritorio ofrecen ventajas de seguridad, ya que un programa autónomo está mucho más encapsulado que una extensión en el navegador. Por ejemplo, los delincuentes podrían preparar una página en Internet de forma que lance ataques una vez abierta. Además, al abrir la página con el navegador al que pertenece la extensión del gestor de contraseñas, aquella resulta mucho más vulnerable que otros programas del PC. Y también existen otras extensiones en el navegador que podrían obtener derechos de acceso. Por último, pero no por ello menos importante, los navegadores están más extendidos que los clientes de gestores de contraseñas, por lo que cada vez más hackers buscan brechas de seguridad en ellos. Esto no significa que estos programas funcionando como extensiones del navegador sean inseguros, pero entrañan más riesgos. Por ello, Computer Hoy recomienda ir sobre seguro y utilizar un cliente de escritorio independiente.



LA PRUEBA EN DETALLE

Biometría, número de cuentas, comodidad y funciones extra: los gestores de contraseñas difieren mucho en los detalles. Aquí puedes ver una comparación de los candidatos.

Extra de NordPass: para reducir el spam y la publicidad, puedes configurar direcciones de correo electrónico alternativas desechables.

A la hora de añadir y gestionar nuevos dispositivos y cuentas, resulta especialmente fácil y cómodo hacerlo con 1Password.

Con los paneles de control como este que incluye Sticky Password, es posible monitorizar la seguridad de tus contraseñas.

1 NORD SECURITY
NORDPASS PREMIUM
Precio: 1,69 €/mes

¿Versión de prueba? Sí, la prueba incluye 30 días de funciones premium.

NordPass procede de Nord Security, también conocida por su programa NordVPN. Este gestor convence en todos los aspectos: cuenta con todas las funciones importantes, el concepto de seguridad está bien pensado y el software es también el más fácil e intuitivo de usar. Por tanto, NordPass es merecidamente el ganador de la prueba y el mejor gestor de contraseñas del mercado.

+ Funcionamiento sencillo, excelentes prestaciones.

− Nada que destacar.

2 BITWARDEN
BITWARDEN PREMIUM
Precio: 0,83 €/mes

¿Versión de prueba? Sí, pero la prueba ofrece funciones limitadas.

Bitwarden es superado por poco por el ganador del test. Mientras que NordPass es un poco más intuitivo, Bitwarden también es rápido y fácil de usar. Además, el programa es la única oferta de la prueba que incluye dos cuentas sin coste adicional y, ofreciendo sus servicios por un coste mensual inferior a un euro, se revela como el merecido ganador en cuanto a relación calidad/precio.

+ Las mejores prestaciones, relación calidad/precio.

− Nada que destacar.

SEGURIDAD			
Autenticación de dos factores, función de recuperación, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	10,00	Autenticación de dos factores, función de recuperación, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	10,00
MANEJO			
Introducción y almacenamiento automáticos de contraseñas y otros datos personales, el mejor manejo de los seis de la prueba	9,20	Introducción y almacenamiento automáticos de contraseñas y otros datos personales, un manejo bastante cómodo	8,40
FUNCIONES			
Memoria muy grande, sincronización, 1 cuenta de usuario, almacenamiento de archivos, tarjetas de crédito y datos importantes, generador de contraseñas	8,80	Memoria muy grande, sincronización, 2 cuentas de usuario, almacenamiento de archivos, tarjetas de crédito y datos importantes, generador de contraseñas	9,20
Sobresaliente	9,60	**Sobresaliente**	9,40
1,69 €/mes		**0,83 €/mes**	

COMPUTER HOY RESPONDE:

¿Qué es el principio de 'conocimiento cero'?

Casi todos los proveedores recurren a una caja fuerte de contraseñas en la nube para la sincronización entre distintos dispositivos. Esta está completamente cifrada y solo puede abrirse con la contraseña maestra del cliente correspondiente. Además, el cliente es el único que la conoce: es desconocida para el proveedor de la caja fuerte de contraseñas. Esto significa que no saben lo que hay en su caja fuerte y no pueden leer, analizar o transmitir los datos. Debido a este desconocimiento por parte del proveedor, el conjunto se conoce como principio de 'conocimiento cero'.

¿Cómo de rápido se puede descifrar una contraseña?

La velocidad a la que los hackers pueden descifrar contraseñas depende del rendimiento del ordenador y de la longitud de la contraseña. Los programas especiales prueban entre millones y miles de millones de contraseñas por segundo. Por ejemplo, descifrar una contraseña con nueve caracteres y un carácter especial utilizando un ordenador con una configuración media lleva unas dos horas; ahora bien, si no has hecho uso de caracteres especiales al crear la clave, este valor se reduce a tan solo unos segundos. Con doce caracteres diferentes, tardará siglos.

3 1PASSWORD
1PASSWORD INDIVIDUAL
Precio: 2,76 €/mes

¿Versión de prueba? Sí, la prueba incluye 14 días con la totalidad de las funciones.

1Password tampoco cometió errores importantes durante la prueba. El software es fácil de usar, el programa es seguro y no faltan funciones. 1Password es especialmente adecuado para las familias, ya que permite gestionar muchas cuentas y dispositivos de forma centralizada. Por eso, 1Password también es un gestor de contraseñas muy bueno y fiable para usuarios particulares.

+ Excelentes prestaciones, buena gestión para muchos dispositivos.

− Nada que destacar.

Autenticación de dos factores, función de recuperación, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	10,00
Introducción y almacenamiento automáticos de contraseñas y otros datos personales, un manejo bastante cómodo	8,40
Memoria muy grande, sincronización, 1 cuenta de usuario, almacenamiento de archivos, tarjetas de crédito y datos importantes, generador de contraseñas	8,80
Sobresaliente	**9,20**
2,76 €/mes	

4 DASHLANE
DASHLANE PREMIUM
Precio: 3,71 €/mes

¿Versión de prueba? Sí, la prueba incluye 30 días con la totalidad de las funciones.

Dashlane es el único administrador de contraseñas del test que solo existe como una extensión del navegador en Windows. Aunque esto ahorra el cambio frecuente entre las ventanas del programa, también significa que la operación es a veces un poco más torpe que con otros candidatos. Sin embargo, en general, Dashlane también es un buen administrador y tiene excelentes funciones.

+ Excelentes prestaciones.

− Solo como extensión del navegador para Windows.

Autenticación de dos factores, función de recuperación, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	10,00
Introducción y almacenamiento automáticos de contraseñas y otros datos personales, un manejo a veces incómodo	7,40
Memoria muy grande, sincronización, 1 cuenta de usuario, almacenamiento de archivos, tarjetas de crédito y datos importantes, generador de contraseñas	8,80
Sobresaliente	**9,00**
3,71 €/mes	

5 LASTPASS
LASTPASS PREMIUM
Precio: 2,90 €/mes

¿Versión de prueba? Sí, la prueba incluye 30 días de funciones premium.

LastPass es seguro y fiable. El funcionamiento resulta a veces un poco más complicado que con la mayoría de los otros candidatos, pero sigue siendo aceptable. Desgraciadamente, hay que mencionar que los hackers robaron las bóvedas de los usuarios de los servidores en 2022 (ver página 55). Esto significa que el fabricante probablemente ha perdido confianza, pero eso no cambia la nota.

+ Excelentes prestaciones.

− Incidente de hackeo en el pasado.

Autenticación de dos factores, función de recuperación, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	10,00
Introducción y almacenamiento automáticos de contraseñas y otros datos personales, un manejo a veces incómodo	6,60
Memoria muy grande, sincronización, 1 cuenta de usuario, almacenamiento de archivos, tarjetas de crédito y datos importantes, generador de contraseñas	8,80
Notable	**8,80**
2,90 €/mes	

6 LAMANTINE SOFTWARE
STICKY PASSWORD PREMIUM
Precio: 19,95 €/año

¿Versión de prueba? Sí, la prueba incluye 30 días de funciones premium.

Sticky Password tiene un defecto que puede causar problemas en caso de emergencia: si olvidas la contraseña maestra, no hay forma de obtener tus contraseñas. Todos los demás candidatos disponen de un acceso de recuperación para esta emergencia. Además, el manejo no siempre es intuitivo. En general, con todo, Sticky Password es también un buen gestor de contraseñas.

+ Buenas prestaciones.

− Sin función de recuperación ante una emergencia.

Autenticación de dos factores, protección ante Darknet, inicio mediante biometría, Passkeys, almacenamiento en la nube	8,00
Introducción y almacenamiento automáticos de contraseñas y otros datos personales, un manejo a veces incómodo	6,60
Memoria muy grande, sincronización, 1 cuenta de usuario, almacenamiento de tarjetas de crédito y datos importantes, generador de contraseñas	8,20
Notable	**7,60**
19,95 €/año	

¡MIRAN Y

PARA INTERIOR

AQARA
CAMERA E1

BOSCH
EYES IN. CAMERA II

EUFY
S 350

EVE
CAM (2. GEN.)

RING
INDOOR CAM (2. GEN.)

Ya sea en verano o en invierno, la publicidad sobre alarmas pone en guardia a millones de personas preocupadas por su hogar. La oscuridad es aliada de los ladrones cuando hace frío, y las vacaciones lo son en verano. Por ello, unos ojos extra pueden aportar tranquilidad y, en esto, **las cámaras analizadas son incansables**.

Uso en interiores y exteriores

En la batería de pruebas de este especial, cinco modelos para interiores (Aqara, Bosch, Eufy, Eve y Ring) compiten por el puesto de vigilante eficiente e inteligente. Además, Arlo, Philips Hue y Ring Stick Up Cam son soluciones que también pueden utilizarse en exteriores. Tienen una fabricación **robusta y resistencia al agua**, ante la lluvia, viento y frío que dañan a otros dispositivos.

La forma más rápida de colocarlas es en alguna pared, alféizar o estantería. Pero siempre lejos del alcance de los cacos. Para no colocarlas de pie, un adaptador de plástico para **montaje en pared o techo** hace el apaño. Eso sí, las cámaras deben ponerse de forma que capten óptimamente el entorno y las zonas que se van a vigilar.

Batería o cables molestos

Las cámaras de interior siempre necesitan una toma de corriente cerca. Pero, según el modelo, algunas pueden funcionar sin cables. Así, las baterías recargables suministran **energía hasta por varios meses**. Algunas de ellas no se pueden extraer, como la de Philips Hue, mientras que con Arlo y Ring la batería se carga por separado. Además, algunas admiten una segunda batería en la propia carcasa. Esto garantiza una mayor autonomía y vigilancia sin interrupciones. Por otro lado, ninguna de las cámaras de la prueba lleva células solares integradas. Sin embargo, hay paneles solares disponibles como accesorios (a partir de 50 €) para que el sol recargue la batería.

Nada funciona sin un móvil

Todas las cámaras necesitan un smartphone para su configuración y muchas **obligan a registrarse** en servicios del fabricante. Es gratis, pero a menudo requieren datos como la dirección o el número de teléfono. A cambio, el proceso de instalación es detallado y claro.

Con Philips y Bosch, se puede instalar una estación base extra bajo pedido, con un coste adicional. Estos 'hubs' se conectan al router WiFi por cable, propor-

OBSERVAN!

Las cámaras de vigilancia cuidan tu casa desde la puerta de entrada al jardín. Aparte de la intimidad, ¿qué más debería preocuparte antes de comprar?

TEST: 8 CÁMARAS ENTRE 59 € Y 229 €

PARA EXTERIOR

ARLO
PRO 5

PHILIPS HUE
SECURE CAMERA

STICK UP CAM PRO

cionan más alcance y conectan en red la cámara con otra tecnología inteligente. Por ejemplo, la cámara Hue puede conectarse con las lámparas Hue; la cámara Bosch lo hace con el sistema de alarma del propio fabricante.

Vigilancia por app y voz

Las aplicaciones Eufy y Arlo ganan puntos en el uso habitual, por ejemplo, alenviar imágenes de vídeo o ajustar la vigilancia. Los menús están bien organizados y todas las opciones importantes se encuentran rápidamente. Además, se puede dejar el móvil conectado y manejar las cámaras por voz. Las de Arlo, Bosch y Eufy **entienden a Alexa y al Asistente de Google**. Aqara también reconoce Apple Home, mientras que Eve solo se siente a gusto en el mundo Apple. Las cámaras Ring son igual de limitadas, ya que solo son compatibles con Alexa. Philips Hue, por su lado, solo muestra imágenes de vídeo en la app Hue, y no había control por voz en el momento de la prueba.

Todas las demás candidatas del test pueden activarse bajo demanda. Si se dispone de un Smart Display en casa, este puede mostrar la imagen de la cámara en directo. Esto funcionó mejor en la prueba con Ring y un Echo Show, porque ambos dispositivos provienen de Amazon y, por lo tanto, se llevan bien cuando están conectados.

> Un ojo vigilante en casa o en la oficina tranquiliza y puede ahuyentar a los ladrones.
>
> **Timo Schurwanz**
> Redactor

EL MEJOR SITIO PARA LAS CÁMARAS

Campo de visión

Una cámara solo puede vigilar bien, si tiene una visión clara de todo lo esencial. Es importante montarla en una posición ligeramente elevada, para garantizar un campo de visión despejado y sin obstáculos delante del objetivo.

Evita la luz de frente

Las ventanas, las lámparas o el sol abrasador del mediodía frente a la cámara proporcionan luz, pero pueden dificultar la toma (ver foto). Hay que evitar fuentes de luz fuertes y las superficies de espejo en la imagen, que dañan la óptica y saturan la iluminación.

Detección de movimiento

Conviene alinear la cámara de modo que grabe de lado todo el frente de la puerta de entrada, para así captar el movimiento 'desde el flanco'. Esto facilita la detección del movimiento por parte del sensor. La óptima se consigue a una distancia de 1,5 m a 6 m. Sin embargo, no debe haber ningún espacio público en la imagen, como en la foto de ejemplo.

Vídeos: a veces nítidos, a veces oscuros

La mayoría de las cámaras de la prueba alcanzan hasta Full-HD (1.920 x 1.080 píxeles). Con Arlo y Aqara, es posible la resolución 2K superior (hasta 2.688 x 1.520 píxeles). Solo la **Eufy supera esta cifra con su resolución 4K** y la friolera de 3.840 x 2.160 píxeles. Todas las cámaras grabaron durante la prueba, tanto de día como de noche, sin el más mínimo problema.

En la prueba de visibilidad, sin embargo, hubo diferencias. Eufy capturó las mejores imágenes durante el día. Arlo también ofreció resultados nítidos y detallados, con movimientos fluidos. El resto, con Eve y Bosch en particular, no pudieron seguir el ritmo. Los vídeos aparecieron más o menos borrosos y pixelados en la prueba. Por otro lado, a menudo, las cámaras tuvieron problemas al grabar a plena luz del sol y en las sombras, con zonas oscuras de la imagen que aparecían pálidas y descoloridas, especialmente en los vídeos de la Eve Cam.

Incluso en la oscuridad, todos los dispositivos se esforzaron por producir grabaciones de vídeo claramente reconocibles. Además, Arlo, Philips Hue y Ring, con capacidad para exteriores, encendían automáticamente una luz LED brillante cuando había movimiento a oscuras. Esto convirtió la noche en día, especialmente con Arlo. Pero con Ring no fue posible sin un molesto tinte verde en la imagen. Por supuesto, la luz agota la batería más rápidamente. Y si quieres conservar la carga o corregir imágenes sobreexpuestas, conviene reducir el brillo en las aplicaciones o conformarse con imágenes en blanco y negro. Para ello, bastan las económicas **luces infrarrojas integradas**. Las cámaras de interior también utilizan estas para iluminar las habitaciones. Y Eufy sigue siendo la que mejor lo consigue.

Vigilancia inteligente y tipo de reacción

Cuando las cámaras están enfocadas, reconocen automáticamente movimientos en el campo de visión. Arlo (gratuito) y Bosch (con coste adicional) reaccionan también a los ruidos, si se desea. En la prueba, siempre se enviaba una notificación al móvil tras un breve momento. A continuación, las aplicaciones muestran la **imagen en directo y el retraso es pequeño**.

Todas las cámaras detectan el movimiento de forma fiable. Bosch y Philips Hue diferencian entre personas, vehículos y otros movimientos. Gracias a Apple Home, Eufy, Aqara y Eve también disponen de **reconocimiento facial**. Las caras familiares registradas pueden identificarse como conocidos. Esto reduce la avalancha de notificaciones no deseadas. Pero estas funciones tienen un coste adicional en Arlo y Ring.

Atenta y bellamente discreta

Todas las cámaras de la prueba tienen un gran campo de visión y, por tanto, una buena vista de lo que ocurre. Aqara y Eufy siempre tienen el detalle de imagen adecuado, y giran sobre su propio eje. También pueden inclinarse hacia arriba y abajo, con unos 100° de margen. Por su parte, el usuario puede **controlar los movimientos panorámicos** mediante la aplicación, y la cámara puede hacerlo automáticamente: por ejemplo, sigue a las personas que se mueven por la habitación. No obstante, esta cámaras pueden ser al mismo tiempo muy discretas: si se desactiva la vigilancia de Aqara y Eufy, ambas giran su objetivo hacia la pared, de modo que ya no miran hacia el interior de la habitación. Otras también dominan este truco, pues el objetivo de la cámara de Bosch se mete dentro de la carcasa, mientras que en la Ring Indoor se puede empujar con la mano una tapa sobre el objetivo.

Cuando no hace falta vigilar nada, las discretas cámaras de Aqara (en la imagen) y Eufy giran automáticamente su objetivo hacia la pared, para así ofrecer más intimidad.

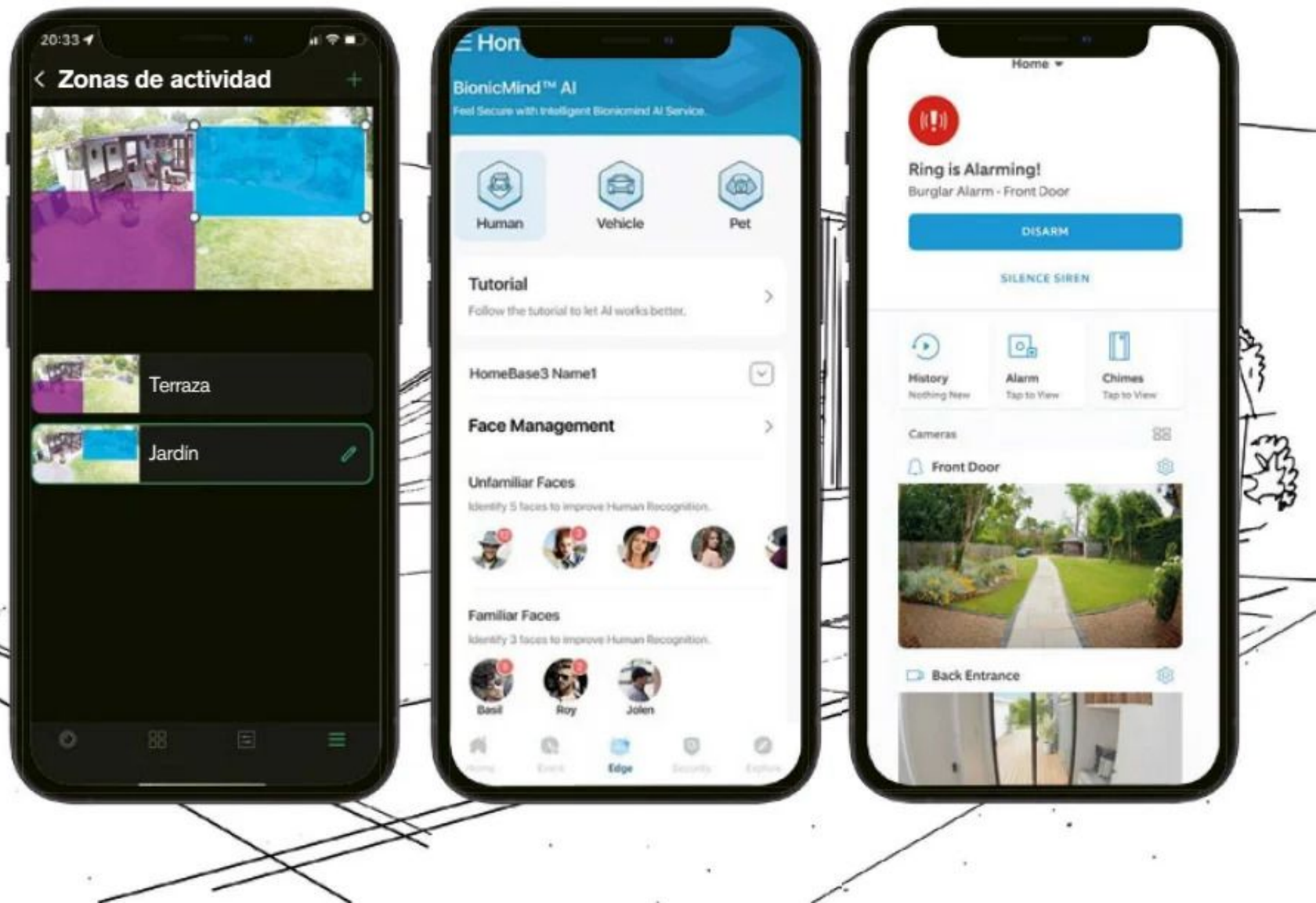
Oído atento y disuasión antirrobo

Con todas las cámaras, es fácil preguntar quién está en la habitación o en la puerta. Gracias a la **función de intercomunicador**, los propietarios pueden comunicarse con la otra persona a través del teléfono móvil. Philips Hue y Ring proporcionaron el mejor sonido en la prueba. Captaban las voces y el ruido ambiente con claridad y un nivel alto. Todos los demás modelos sonaban un poco metálicos, y las voces parecían apagadas y con excesiva compresión.

Si la voz del propietario no es suficiente para poner en fuga a los ladrones, una sirena puede ayudar. Arlo, Ring, Philips Hue y Bosch tienen una incorporada, y

APPS CON SUPERVISIÓN

Activación: desde la app (imagen: Arlo), se pueden realizar ajustes para reducir la sección de imagen o definir la sensibilidad.
Reconocimiento facial: la grabación solo se inicia cuando la cámara detecta una cara desconocida (imagen: Eufy).
Vigilancia bajo control: la luz LED y la sirena pueden ahuyentar a los ladrones, pero sin molestar a los vecinos y residentes. Para ello, se puede activar y desactivar la disuasión según las necesidades (imagen: Ring).



LA CALIDAD DEL VÍDEO: LUCES Y SOMBRAS

La Eufy fue la mejor de la prueba. Ofreció imágenes de vídeo coloridas y detalladas durante el día.

Con la cámara Bosch, los vídeos eran bastante ruidosos y los colores se mostraban exagerados.

Arlo capturó las mejores imágenes nocturnas. La luz LED incorporada añade color a la imagen.

Con Eve, se corre el riesgo de un pixelado excesivo. Las zonas oscuras aparecen claramente lavadas.

todas suenan tan estridentes y fuerte que los vecinos cercanos deberían darse por enterados.

¿Dónde se quedan las grabaciones?

Para no perderse nada, se puede indicar que la cámara no solo transmita, sino que también grabe vídeos. Los modelos Aqara y Eufy tienen una **tarjeta micro SD para almacenamiento**. El problema llega si un ladrón roba la tarjeta o la cámara, ya que también se perderían las grabaciones. Por ello, las pruebas recopiladas se almacenan de forma más segura en la nube. De ahí que las soluciones de Arlo, Ring, Philips Hue, Bosch y Eve no hagan copia de seguridad local.

Costes adicionales del servicio en la nube

El almacenamiento en la nube es práctico: permite consultar el historial de vídeo incluso días después. Esto requiere siempre una suscripción mensual de pago. Bosch incluye 100 clips, pero solo pueden durar un máximo de 15 s y no se puede acceder a ellos durante más de siete días. Para vídeos más largos y un historial de 30 días, se cobra una cuota mensual de 3 €. Ring y Philips Hue reclaman 4 € por el almacenamiento en la nube, mientras que Arlo incluso sube a 5 €. Por su parte, Eve aprovecha la nube de Apple. Esta empieza en solo 1 € para el servicio mínimo. Arlo y Ring también incluyen algunas funciones, como reconocimiento de personas y zonas de actividad, tras su muro de pago, con lo que no se limita solo a guardar fotos, sonido y vídeos.

CONCLUSIÓN

Las mejores cámaras para interiores que pueden verse en la prueba son las de Eufy y Aqara. Ambas ofrecen una buena calidad de vídeo y añaden un giro automático del objetivo. Para quien necesite una cámara para usar en exteriores, el consejo es optar por Arlo. Pero esto implica que se pagará al menos el doble por la cámara. Aparte, para gozar de todas sus opciones, es necesario suscribir y abonar un servicio mensual. Ring, Philips Hue, Bosch y Eve también piden pagar por el almacenamiento en la nube y los extras. Pero, en todo caso, es menos que contratar un servicio de alarmas y vigilancia conocido por sus anuncios omnipresentes en todo tipo de medios.

Cuando no están en uso, el objetivo y los micrófonos del modelo Bosch se desplazan dentro del propio cuerpo del dispositivo.

ACCESORIOS QUE PUEDEN VENIR BIEN

Timbre con vídeo

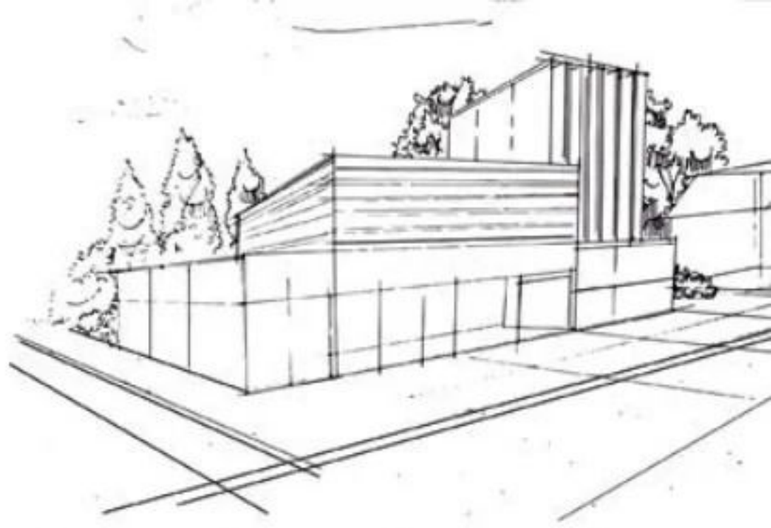
Eufy, Aqara y Ring ofrecen timbres inteligentes con cámara de vídeo incorporada, para la puerta principal. Esto facilita ver quién se pone delante para entrar y poder hablar con el visitante sin que pase a casa.
Precio: desde 80 €.

Sensor para las ventanas

Los sensores para la puerta o ventana inteligentes proporcionan seguridad adicional. Todas, excepto Arlo y Ring, están equipadas con contactos inteligentes. Si se activan, avisan a los ocupantes, al tiempo que las cámaras integradas en el sistema empiezan a grabar.
Precio: a partir de 30 €.

Alarma inteligente

Para sentirse algo más seguros, una buena idea es poner un sistema de alarma. Este combina varios dispositivos. La vigilancia puede ajustarse y activarse cómodamente, mediante un teclado o un teléfono móvil. Aqara, Eufy, Ring y Bosch ofrecen estos paquetes de protección integral.
Precio: a partir de 200 €.



LA PRUEBA EN DETALLE

¿Cable o batería? ¿Resolución HD o 4K? ¿Alexa o HomeKit? Las diferencias radican en los detalles de las cámaras. He aquí un resumen de los puntos individuales y la clasificación.

EXTERIOR

1 ARLO PRO 5

PRECIO: 200 EUROS
OPCIONES: NINGUNA

Uso: interior y exterior
Dimensiones: 8 x 5 x 9 cm
Suscripción cloud: desde 5 €/mes

La Arlo Pro 5 inalámbrica ofrece impresionantes grabaciones en 2K, vídeo cuando se detecta movimiento y visión nocturna en color gracias al LED. La función de intercomunicador y la potente sirena como elemento disuasorio la convierten en la mejor cámara para exteriores. Ofrece además almacenamiento en la nube y extras como zonas de actividad y detección de paquetes, con una suscripción que se añade al precio de compra.

+ Buenos vídeos, luminosos de noche, colocación flexible gracias al soporte magnético.

– Sonido un poco apagado, cloud y algunas funciones extra solo disponibles con suscripción.

2 RING STICK UP CAM PRO

PRECIO: 160 EUROS
OPCIONES: CON BATERÍA, 180 EUROS

Uso: interior y exterior
Dimensiones: 15 x 7 x 7 cm
Suscripción cloud: desde 4 €/mes

Para exteriores, con batería recargable, ofrece grabaciones HD buenas y detalladas durante el día. Por la noche, los usuarios pueden elegir entre grabaciones decentes en blanco y negro o imágenes en color iluminadas artificialmente, con un tinte verde. La detección de movimiento por radar y la potente sirena disuasoria le otorgan puntos extra. La nube para vídeo y la detección de personas necesitan una suscripción mensual.

+ Imágenes buenas y de alto contraste, detección de movimiento superior mediante radar.

– Vídeos nocturnos con tinte verde o en blanco y negro, nube y extras solo con suscripción.

3 PHILIPS HUE SECURE CAMERA

PRECIO: 229 EUROS
OPCIONES: CON BATERÍA, 249 EUROS

Uso: interior y exterior
Dimensiones: 9 x 8 x 8 cm
Suscripción cloud: desde 4 €/mes

Este guardián para interiores y exteriores ofrece buenos vídeos HD y muchas funciones. La cámara se integra perfectamente en el sistema Hue de Philips y funciona junto con las populares lámparas. Cuando detecta movimiento, la luz se enciende y la cámara proporciona pruebas. Sin embargo, el almacenamiento en la nube requiere una suscripción de pago y Hue Secure no reconoce (todavía) Alexa, Google y Apple.

+ Todo en una aplicación universal de Hue, con alarma luminosa y detección de movimiento.

– Sin emparejamiento con Smart Home, almacenamiento en la nube y extras bajo suscripción.

CALIDAD DE IMAGEN Y SONIDO					
2.304 x 2.096 Pix (2K), imágenes ricas en detalles y colores reales, retroiluminación pobre con HDR, calidad de sonido decente	7,60	1.920 x 1.080 Pix (FHD), imágenes nítidas y ricas en detalles, algo frías, imágenes en color con tinte verde por la noche, buen sonido	7,40	1.920 x 1.080 Pix (FHD), buenos vídeos, pero colores algo pálidos, problemas con las zonas claras y oscuras, buena calidad de sonido	7,40
RECONOCIMIENTO Y REGISTRO DE MOVIMIENTO					
Detecta bien movimientos, distingue entre personas, vehículos y animales, detección de paquetes, CO_2 y humo solo con suscripción	7,00	Registra con fiabilidad el movimiento mediante radar, detección de personas solo con una suscripción mensual de pago	6,40	Buena detección de movimiento, pero el reconocimiento de paquetes no es fiable, la grabación en la nube tiene coste extra	6,40
MANEJO Y FUNCIONES					
App clara para el móvil, manejo sencillo, soporta Amazon Alexa y Asistente de Google, nada de Apple	6,00	Muchas funciones, app algo sobrecargada, funcionamiento sencillo, solo soporta Amazon Alexa, nada de Google o Apple	5,60	Fácil de usar, muchas funciones, reconocimiento de personas y zonas de actividad por suscripción, nada de Amazon, Google o Apple	5,60
PROTECCIÓN ANTIRROBO Y CONSUMO ENERGÉTICO					
Fácil de sustraer, pruebas almacenadas en la nube (coste adicional), consumo de energía bajo (4 W), batería recargable mediante energía solar	7,80	Fácil de sustraer, almacenamiento como extra (pero con sustitución gratuita con la suscripción), el consumo de energía sigue siendo económico (5 W)	8,20	Algo fácil de sustraer, las pruebas solo se almacenan en la nube (tiene un coste adicional), bajo consumo (3 W)	8,20
Reconocimiento de ruidos	+0,30	Detección de movimiento ajustable	+0,30	También se puede usar como detector de movimiento, control de lámparas Hue	+0,30
Notable	**7,40**	**Notable**	**7,20**	**Notable**	**7,20**
200,00 €		**160,00 €**		**229,00 €**	

INTERIOR

1 EUFY S 350

PRECIO: 99 EUROS
OPCIONES: NINGUNA

Uso: interior
Dimensiones: 10 x 8 x 8 cm
Suscripción cloud: no disponible

Es una pequeña cámara con doble lente, que ofreció la mejor calidad de vídeo. Las imágenes siguen siendo nítidas y detalladas incluso con el zoom. También contribuyeron a la victoria en la prueba las numerosas funciones y el seguimiento sin interrupciones, gracias al giro e inclinación automáticos. No incluye servicio en la nube, pues guarda los vídeos localmente en una tarjeta microSD, que Eufy también incluye de serie.

+ Visión de 360°, inclinación y giro, copia de seguridad local, tarjeta SD incluida.

– Grabaciones en la oscuridad algo ruidosas, no funciona con batería.

CALIDAD DE IMAGEN Y SONIDO	
3.840 x 2.160 Pix (4K), la mejor resolución y vídeos, nítidos incluso al hacer zoom gracias a la doble lente, sonido correcto	8,20
RECONOCIMIENTO Y REGISTRO DE MOVIMIENTO	
Reconoce con fiabilidad el movimiento, distingue entre personas, caras, vehículos, animales, etc. sin coste adicional	7,40
MANEJO Y FUNCIONES	
App algo confusa, aun así fácil de usar, soporta Amazon Alexa, Asistente de Google y Apple HomeKit incluido Vídeo seguro	6,80
PROTECCIÓN ANTIRROBO Y CONSUMO ENERGÉTICO	
Fácil de sustraer, almacenamiento opcional de pruebas en la nube (coste adicional), bajo consumo (3 W), batería recargable mediante energía solar	7,80
Visión de 360°, panorámica, inclinación y zoom, Apple 'Video seguro de HomeKit'	+0,65
Notable	**8,20**
99,00 €	

COMPUTER HOY RESPONDE:

¿Cómo funciona una cámara de vigilancia inteligente?
La cámara vigila constantemente y guarda el vídeo si, por ejemplo, hay movimiento en la imagen. Gracias al WiFi, la imagen de la cámara puede consultarse a través de Internet.

¿Cómo se conecta la cámara?
Algunos modelos no tienen batería, por lo que necesitan un cable hasta la pared y un enchufe cerca. Mucho más rápidas de instalar, listas para su uso y con la opción de colocarse de forma más flexible son las cámaras con batería recargable.

¿Cuál es el consumo de energía real?
No es alto, en línea con otros dispositivos del hogar. Las cámaras tienen un modo de espera que ahorra energía. Siempre vigilan, pero solo graban cuando detectan movimiento o ruido.

¿Es legal el empleo de esta vigilancia inteligente?
Sí, pero las cámaras exteriores solo deben filmar la zona situada delante de la puerta, no el espacio público ni privado de otros. En pisos, los propietarios e inquilinos deben consentirlo.

Computer Hoy GANADOR CALIDAD/PRECIO

2 AQARA CAMERA E1
PRECIO: 60 EUROS
OPCIONES: NINGUNA

Uso: interior
Dimensiones: 7 x 10 x 7 cm
Suscripción cloud: no disponible

Proporciona imágenes detalladas en color durante el día, y clips nítidos en blanco y negro por la noche. Gracias a sus numerosas funciones, su excelente reconocimiento de personas y panorámica automáticos, la E1 siempre tiene una buena visión de la acción. Graba en tarjeta de memoria local o en la nube de Apple. El almacenamiento en línea 'Vídeo seguro de HomeKit' sale realmente económico y es muy recomendable.

+ Apple 'Vídeo seguro de HomeKit', vista de 360°, función de panorámica e inclinación.

− Grabaciones en la oscuridad algo ruidosas, no funciona con batería.

3 EVE CAM (2. GENERATION)
PRECIO: 148 EUROS
OPCIONES: NINGUNA

Uso: interior
Dimensiones: 12 x 6 x 7 cm
Suscripción cloud: desde 1 €/mes (Apple)

Quien use entornos Apple con almacenamiento iCloud verá en esta cámara un buen complemento para su hogar inteligente controlado por HomeKit. Las grabaciones se cifran en iCloud y las cuotas de suscripción se pagan a Apple. Novedades en la 2ª generación de la cámara son la alimentación a través de USB-C, la detección de movimiento con análisis de imagen y la visión nocturna optimizada, aunque necesita mejorar.

+ Funcionamiento sencillo, análisis de imagen local con Eve, alimentación mediante USB-C.

− Vídeos bastante pobres en detalle y borrosos, no se pueden guardar localmente los clips.

4 RING INDOOR CAM (2. GEN.)
PRECIO: 59 EUROS
OPCIONES: NINGUNA

Uso: interior
Dimensiones: 10 x 5 x 5 cm
Suscripción cloud: desde 4 €/mes

Este cilindro pequeño, con tapa diminuta y precio reducido, además de grabar en HD, tener detección de movimiento, sirena e interfono, pretende garantizar la privacidad. La tapa giratoria de la cámara permanece cerrada cuando los ocupantes están presentes. Sin embargo, solo puede abrirse y cerrarse manualmente, no mediante una app ni en función del tiempo. Es una solución que aporta confianza, pero no comodidad de uso.

+ Precio justo, fácil de configurar, visión nocturna, reconocimiento de personas.

− Soporte no motorizado, solo almacena en la nube y esta es de pago.

5 BOSCH EYES IN. CAMERA II
PRECIO: 185 EUROS
OPCIONES: NINGUNA

Uso: interior
Dimensiones: 16 x 7 x 7 cm
Suscripción cloud: 3 €/mes

La cámara de interior más cara de la prueba impone respeto. El objetivo sale fuera de la carcasa y la Eyes II incluso emite una fuerte alarma, en cuanto detecta movimiento. La calidad de vídeo y voz no fue tan positiva. Además, el almacenamiento gratuito en la nube solo admite clips de 15 s que se guardan durante tan solo siete días, y se llena rápidamente. Las restricciones desaparecen con una suscripción mensual.

+ Lente retráctil automática, buena conexión con Bosch Smart Home.

− La peor calidad de vídeo de la prueba, escaso almacenamiento en la nube, costes adicionales.

2.304 x 1.296 Pix (2K), rico en detalles y colores, imágenes ligeramente atenuadas por la noche, calidad de sonido decente	7,40	1.920 x 1.080 Pix (FHD), vídeos algo borrosos y lavados, demasiado oscuros de noche, movimientos fluidos, sonido decente	6,40	1.920 x 1.080 Pix (FHD), vídeos coloridos, pero no siempre nítidos, de noche graba en blanco y negro, sonido correcto	6,80	1.920 x 1.080 Pix (FHD), la peor calidad de vídeo de la prueba, pobre en detalles, borroso de noche, sonido correcto	6,20
Detecta el movimiento con fiabilidad, seguimiento muy bueno, distingue entre personas, caras y vehículos con precisión	8,00	Detecta con fiabilidad el movimiento, distingue entre personas, caras, vehículos, animales y otros con la suscripción a Apple Cloud	6,40	Registra los movimientos con fiabilidad, el reconocimiento de personas solo funciona con una suscripción mensual de pago	6,40	Reconoce bien el movimiento, distingue de todo tipo, almacenamiento gratuito en la nube con opciones de pago	6,40
App sobrecargada, aun así fácil de usar, soporta Amazon Alexa, Asistente de Google y Apple HomeKit incluido 'Vídeo seguro'	6,60	La app Eve está bien, Apple HomeKit también, funcionamiento sencillo, soporta 'Video seguro', nada de Amazon o Google	6,60	Muchas funciones, app algo sobrecargada, funcionamiento sencillo, solo soporta Amazon Alexa, nada de Google o Apple	5,20	App lenta, imagen de vídeo desde Bosch Smart Home, funcionamiento correcto, soporta Amazon Alexa y Asistente de Google, nada de Apple	5,60
Fácil de sustraer, almacenamiento en la nube (coste adicional), bajo consumo (3 W), batería recargable mediante energía solar	7,80	Fácil de sustraer, almacenamiento rentable de pruebas a través de Apple Cloud, bajo consumo de energía (3 W)	7,80	Fácil de sustraer, almacenamiento en la nube de pago, sustituyen gratis la cámara robada si se tiene suscripción, consumo de energía muy económico (menos de 2 W)	8,40	Fácil de sustraer, almacenamiento en la nube de pago, sustituyen gratis la cámara robada si se tiene suscripción, alto consumo de energía (8 W)	5,00
Visión de 360°, panorámica, e inclinación, Apple 'Vídeo seguro de HomeKit'	+0,35	Apple 'Video seguro de HomeKit'	+0,10			Buena función de alarma	+0,40
Notable	**7,80**	**Bien**	**6,90**	**Bien**	**6,70**	**Bien**	**6,20**
60,00 €		**148,00 €**		**59,00 €**		**185,00 €**	

saber más
Tecnología para todos

PRINCIPALES PELIGROS Y AMENAZAS EN 2024

A nivel mundial, durante el presente año se prevé que una gran parte del gasto IT se centre en la privacidad de los datos y los sistemas de seguridad en la nube. Te contamos cuáles son los pronósticos relativos a la ciberseguridad.

El año 2024 se vislumbra como otro desafío sin tregua para los expertos en ciberseguridad. Durante el pasado 2023, mientras se adquirían valiosas lecciones como el impacto masivo de la inteligencia artificial, la humanidad también se enfrentó a nuevos desafíos debido al aumento del teletrabajo en todo mundo.

Así, por ejemplo, un 88 % de las empresas tuvieron dificultades al implementar **medidas efectivas de ciberseguridad** en el ámbito del trabajo remoto. Para el 20 % de las organizaciones, este fue uno de sus grandes quebraderos de cabeza.

Grandes desafíos para 2024

Gartner, empresa estadounidense de consultoría e investigación de las tecnologías de la información, predice un aumento del 15 % en el **gasto destinado a ciberseguridad** para el próximo año, alcanzando los 215.000 millones de dólares. Este incremento se atribuye a diversos factores como la seguridad en la nube, el avance de la inteligencia artificial generativa y la implementación de regulaciones más estrictas. De hecho, se espera que en los próximos dos años hasta el 75 % de la población mundial esté amparada por estas nuevas normativas.

Pero a pesar de todo ello, es el momento de analizar **qué depara el futuro** al mundo de la ciberseguridad para 2024. ¡Descúbrelo ya!

1 RIESGOS EN LA INFRAESTRUCTURA ICS/OT: PROBLEMAS EN LA **SEGURIDAD INDUSTRIAL**

La complejidad y la interconexión cada vez mayores de la tecnología han dejado a la infraestructura de control industrial y a la tecnología operativa (ICS/OT) en una posición mucho más vulnerable. Los ataques a la cadena de suministro y a las redes corporativas agravan aún más estos riesgos. Los expertos enfatizan la necesidad de una colaboración estrecha entre profesionales de seguridad cibernética y OT, para así diseñar sistemas resilientes que prevengan interrupciones operativas que podrían resultar muy costosas.

Foto: Depositphotos.com

La interconexión tecnológica actual expone la ICS/OT a riesgos, todo ello agravado por ataques a la cadena de suministros.

¿Podría la IA mejorar su forma de engañar a las personas? Los expertos dicen que sí, y no dudan en alertar sobre estos riesgos.

2 LA AMENAZA DE LA **INTELIGENCIA ARTIFICIAL GENERATIVA**

La proliferación de la IA generativa plantea serias amenazas para la seguridad cibernética. Además de su capacidad para difundir información errónea, el código malicioso generado por la IA representa un grave problema. Por ello, es crucial capacitar al personal en el uso de herramientas de inteligencia artificial y establecer políticas de seguridad cibernética efectivas, para así controlar este tipo de amenazas. Además, según NordPass, la inteligencia artificial puede ser aprovechada por los piratas informáticos de muchas maneras. Por ejemplo, es probable que se utilice para mejorar la ortografía y gramática de los correos electrónicos de phishing, lo que facilitaría a los ciberdelincuentes la tarea de engañar a las víctimas para que interactúen con enlaces y archivos adjuntos maliciosos. "A medida que la inteligencia artificial se utilice más ampliamente para aumentar el desarrollo de 'software', los defensores la usarán para encontrar vulnerabilidades en su 'software'" explica Oakley Cox, director técnico analista de Darktrace.

3 INTERNET DE LAS COSAS (IoT) EN 2024

El crecimiento de dispositivos IoT conectados abre nuevas puertas para los ciberataques. Con la implementación generalizada del trabajo remoto, esta amenaza se expande a los dispositivos domésticos que los empleados utilizan para acceder a redes empresariales. La integración de sistemas de confianza cero en las estrategias de seguridad IT se vuelve cada vez más necesaria para mitigar estos riesgos. Como señala Forbes, "Más dispositivos que se comuniquen entre sí y accedan a Internet significa más posibilidades de que los ciberatacantes los aprovechen". Este enfoque revolucionario postula: "Nunca confíes por defecto, verifica siempre". Y en lugar de suponer que alguien o algo es seguro simplemente porque está dentro de la red 'protegida', la filosofía de confianza cero sostiene que todos, tanto dentro como fuera, deben demostrar constantemente su fiabilidad.

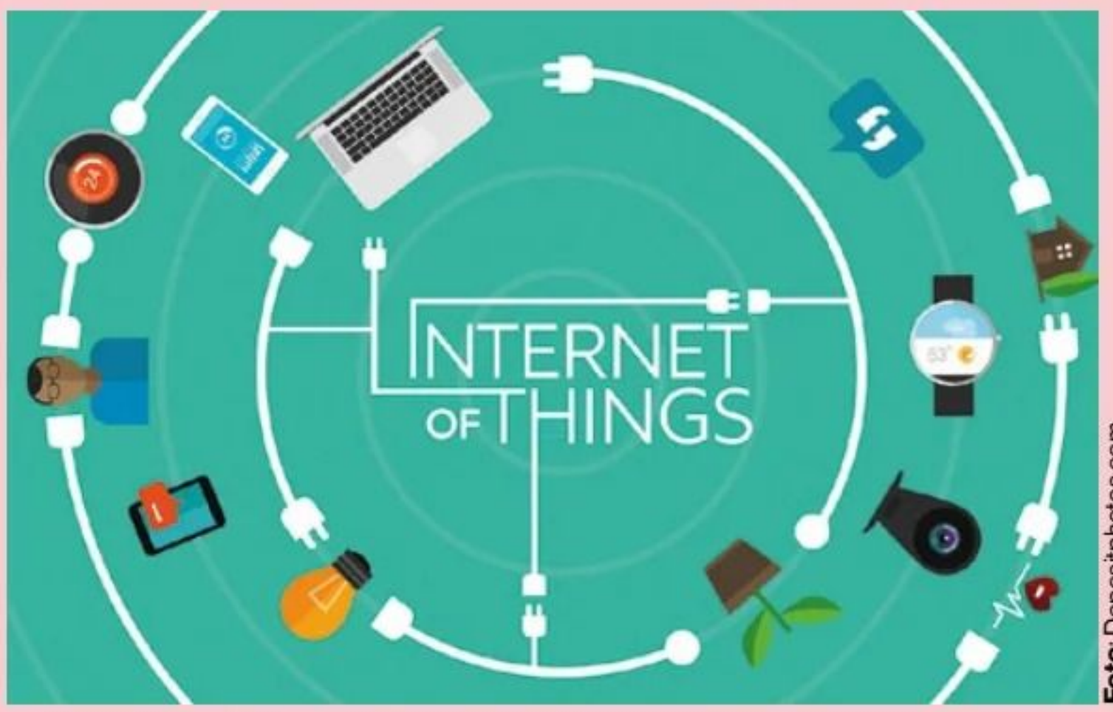


Foto: Depositphotos.com

La clave está en las herramientas que convierten a los objetos en inteligentes, permitiéndoles conectarse a Internet para ampliar sus funciones.

4 AMENAZAS A **EVENTOS IMPORTANTES** COMO LOS JUEGOS OLÍMPICOS

La proximidad de eventos masivos como las elecciones en EE. UU. de 2024 o los Juegos Olímpicos crea un entorno propicio para los ciberataques. Se anticipa así una amplia gama de actividades maliciosas como suplantaciones de correo electrónico, phishing y deepfakes, lo que subraya la importancia de la seguridad en general y la infraestructura electoral. Estos eventos serán una prueba crucial para evaluar las mejoras y deficiencias en la ciberseguridad a nivel mundial. Un ejemplo ilustrativo es el caso de los Juegos Olímpicos de Japón, que enfrentaron alrededor de 450 millones de ataques cibernéticos contra su infraestructura. Nathaniel Gleicher, jefe de política de seguridad en Meta, expresa lo siguiente: "Cuando se trata de actores de amenazas particularmente sofisticados, en el contexto de la interferencia extranjera hemos observado que algunos estados nacionales planifican y coordinan sus campañas fuera de nuestras plataformas, lo que significa que es posible que los investigadores no detecten una campaña hasta el último minuto".

Foto: Depositphotos.com

Usuarios y profesionales gastan cada día más esfuerzos y recursos en intentar mantenerse a salvo de las continuas amenazas que surgen.

Foto: Depositphotos.com

La formación continúa de sus empleados es clave para las empresas. Solo así se pueden mitigar los riesgos cibernéticos actuales.

5 VIGILANCIA DE PROVEEDORES EXTERNOS Y **CADENAS DE SUMINISTRO**

La ingeniería social y los ataques de phishing dirigidos a proveedores externos siguen representado una amenaza que no cesa, año tras año. Los atacantes emplean tácticas cada vez más sofisticadas e innovadoras, para comprometer a empleados y a todo tipo de personas. Todo esto resalta la importancia de la educación continua en ciberseguridad y la necesidad de garantizar públicamente que las organizaciones mantengan a sus empleados actualizados y bien formados en este ámbito.

6 CUIDADO CON LA **AUTENTICACIÓN BIOMÉTRICA**

Aunque la biometría se considera más segura que las contraseñas, su implementación plantea preocupaciones sobre privacidad. Por ejemplo, los hackers podrían acceder a colecciones de datos, incluidos datos biométricos de alto perfil, lo que convierte a estos en un objetivo muy atractivo. Y aunque estos datos suelen protegerse a un nivel más robusto, con la creciente presencia de la biometria, es probable que este tipo de información esté disponible en muchos más lugares, algunos de los cuales podrían no ofrecer el mismo nivel de seguridad en su almacenamiento. Sin ir más lejos, a finales de 2023, la Agencia Española de Protección de Datos (AEPD) cambió su posición sobre el uso de estos sistemas para controlar la presencia en entorno laborales y otros contextos. La AEPD ha adoptado ahora medidas mucho más estrictas, incluyendo prohibiciones y restricciones, tal y como así se describe en su Guía sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos.

Foto: Depositphotos.com

La biometría se ha convertido en una herramienta clave para lograr verificar la identidad de las personas de una manera más precisa.

¿QUÉ ES BUG BOUNTY Y POR QUÉ LAS EMPRESAS NECESITAN UN HACKER EN SU VIDA?

Los programas Bug Bounty permiten a las empresas aprovechar la comunidad de hackers éticos (de sombrero blanco) para mejorar la seguridad de sus sistemas.

Hoy en día, los ciberdelincuentes se encuentran al acecho tratando de encontrar vulnerabilidades y fallos en los sistemas, para así **aprovecharse de las empresas y de las personas** y conseguir sacar de todas ellas un buen pellizco. Por ello, los departamentos de ciberseguridad de las compañías son cada vez más vitales y necesarios. Sin embargo, el problema es que a veces es necesaria la mirada de un ojo experto que desde fuera encuentre los fallos...

Y ahí es donde entran en juego los hackers éticos, también conocidos como de sombrero blanco. Y es que no todos los hackers son malos. Según los programas 'Bug Bounty' o 'recompensa por errores'. las empresas de todo el mundo pueden aprovechar las cualidades de los hackers éticos para mantener su seguridad.

¿Qué significa Bug Bounty?

Bug Bounty, traducido como 'recompensa por errores', es una práctica en la industria de la tecnología, donde las organizaciones ofrecen dinero o reconocimiento a personas externas que descubren y reportan vulnerabilidades de seguridad en sus sistemas, aplicaciones o plataformas de software. Básicamente, es una forma de recompensar a los hackers éticos por ayudar a identificar y corregir posibles problemas de seguridad.

Así, en lugar de depender únicamente de los equipos de seguridad internos, las organizaciones abren sus sistemas a una amplia comunidad de hackers, que se dedican a ello de forma profesional, aunque también es cierto que algunos lo hacen por amor al arte.

Una vez descubierta una vulnerabilidad, los hackers éticos la comparten con la organización o plataforma de recompensas por errores, siguiendo las pautas adecuadas para la divulgación responsable. Esto incluye proporcionar información detallada sobre la vulnerabilidad, su impacto potencial y los pasos para reproducir el problema.

Incluso se realizan **competiciones a nivel mundial**, como el famoso Ambassadors World Cup que conecta grandes multinacionales con estos hackers, para poner a prueba sus sistemas y a la vez convertirlo en una competición donde cada país, representado por un equipo al estilo del Mundial de fútbol, trata de encontrar la máxima cantidad de fallos posibles para hacerse con la copa y con bastante dinero.

¿Cómo funciona?

Este tipo de proyectos generalmente funciona mediante la publicación de una lista de sistemas o aplicaciones que se exponen para pruebas de seguridad, junto con las **reglas, directrices y recompensas ofrecidas por cada fallo** reportado. Los investigadores externos pueden entonces examinar estos sistemas en busca de posibles vulnerabilidades y, si encuentran alguna, podrán comunicarla a la organización a través de un proceso previamente ya establecido.

Una vez que se recibe un informe de vulnerabilidad, el equipo de seguridad de la organización evalúa su validez y la gravedad del asunto, y luego trabaja para corregirlo. Dependiendo de la política de recompensas del programa, los investigadores que transmitieron la vulnerabilidad podrán recibir una gratificación monetaria, un reconocimiento público o, incluso, ambas cosas a la vez.

Al final, y hablando de dinero, los pagos variarán según la gravedad del fallo y pueden ir desde unos pocos miles hasta millones de dólares, según la empresa y el impacto potencial del error.

Errores y sus recompensas

Desde noviembre de 2010, Alphabet, la empresa matriz de Google, ha estado operando con Vulnerability Reward Program (VRP). Este programa tiene como objetivo incentivar la investigación sobre seguridad, para así identificar y reportar vulnerabilidades localizadas en los productos y servicios de Google, al igual que en sus plataformas subsidiarias como YouTube, Android o Google Cloud. Pero además de ofrecer recompensas en forma de dinero, Google mantiene un 'salón de la fama' público, para reconocer a aquellos investigadores de seguridad que hayan contribuido al VRP con descubrimientos clave. En 2022, Google anunció **la mayor recompensa jamás otorgada**: 605.000 $, por el hallazgo de un importante fallo de seguridad no descubierto hasta entonces. ■

AVANCE

A LA VENTA EL 30 DE AGOSTO

ESPECIAL CENTRO DE DESCARGAS

SOLUCIONES PARA TODOS, ¡Y SIN GASTAR!

Existen numerosos programas que sus fabricantes y desarrolladores ofrecen de manera gratuita en Internet. Además, sirven para todo tipo de tareas: desde la productividad a la creatividad pasando por la seguridad o el trabajo diario. En el próximo número de Computer Hoy, te hablamos de este tipo de aplicaciones y te contamos para qué puedas usarlas y cómo hacerlo.

BRECHA DE SEGURIDAD

LAS VPN EN PELIGRO

Te hablamos de TunnelVision, una técnica que explota determinadas vulnerabilidades en las redes VPN, para de este modo lograr eludir los mecanismos de seguridad de los datos transmitidos.

UNA MIRADA AL FUTURO

100 AÑOS DE IFA

Leif Lindner dirige IFA (una de las ferias más antiguas en Alemania) desde hace un año. En una interesante entrevista, nos explica cómo se encamina hacia el futuro la principal feria europea de electrónica de consumo.

LA EVOLUCIÓN DE LA CRIPTOGRAFÍA

¿ES SEGURO ALMACENAR TU VIDA EN LA NUBE?

Desde tiempos antiguos, la criptografía ha sido fundamental para ocultar mensajes y asegurar las comunicaciones. Hoy en día, sigue evolucionando en esta misma línea y, además, se adapta a la era digital actual para así garantizar la privacidad, una computación verificable y lograr la seguridad en la nube.

Computer Hoy

REDACCIÓN
Redactor Jefe: Carlos Gombau
Jefa de Sección: Fuencisla Mira
Colaboradores: Ana Abad, Carolina González, Fernando Escudero, Luis Sanz, Óscar Díaz y Tomás González

Director de Arte: Abel Vaquero
Maquetación: Paula Cuesta
Fotografía: Depositphotos.com y Getty Images

CONTACTO REDACCIÓN
computerhoy@axelspringer.es

EDITA
axel springer

EQUIPO DIRECTIVO EJECUTIVO
Director General: Manuel del Campo
Director Desarrollo Producto Digital: Miguel Castillo
Director Comercial: Daniel Chamorro
Directora Editorial: Yovanna Blanco

EQUIPO COMERCIAL
Directora de Ventas: Valle Santos
• Sales Manager Área de Tecnología: Estel Peris
• Equipo Comercial: Javier Abad y Sergio Fernández
Directora de Acciones Especiales: Susana Pardo
• Business Solutions: Susana Herreros, Lydia Rissi y Marina Cobo
Directora de Operaciones y Programática: Aitana Núñez
Sales Controler: Jessica Jaime

MARKETING
Directora de Marketing, Cultura y Personas: Marina Roch
• Social Media Manager: Nerea Nieto
• Social Editor: Noelia Santiago
• Marketing Assistant: Andrea Gómez

SISTEMAS / IT
Director de Sistemas: José Ángel González

VÍDEO
Director de Vídeo: Igoe Montes

DESARROLLO
Director de desarrollo: Javier Domingo

ADMINISTRACIÓN:
Jefa de Contabilidad y RRHH: Pilar Sanz
Responsable de Bancos y Proveedores: Cristina Nieto

Axel Springer España S.A.
Edif. Talent Garden. C/ Juan de Mariana 15
28045, Madrid
Tel. +34 915 140 600

CONTACTO PUBLICIDAD
publicidadaxel@axelspringer.es

CONTACTO SUSCRIPCIONES:
Tel. +34 915 140 600
suscripciones@axelspringer.es

CONTACTO MARKETING
marketing@axelspringer.es

DISTRIBUCIÓN EN ESPAÑA E HISPANOAMÉRICA
SGEL. Tel. +34 915 140 600

DISTRIBUCIÓN EN PORTUGAL
Urbano Press. Tel. +351 211 544 246

TRANSPORTE
Boyaca. Tel. +34 917 478 800

IMPRIME
ROTOCOBRHI. Tel. +34 918 031 676
Printed in Spain.
Depósito Legal M-37952-1998
Revista miembro de ARI

SÚPER OFERTA DE SUSCRIPCIÓN

¡UNIDADES MUY LIMITADAS!

Computer Hoy

FRITZ! Repeater 1200 AX

¡Amplía el alcance de tu Wi-Fi!

- Repetidor **Wi-Fi 6 compatible** con cualquier router Wi-Fi
- **Manejo cómodo** y aplicaciones inteligentes
- Red con un puerto **LAN Gigabit**

FRITZ!

PVP recomendado **95,99€**

por sólo **75€**

~~186,99€~~

Sin gastos de envío

+ 26 números de Computer Hoy

Puedes suscribirte por cualquiera de estos canales:

En http://store.axelspringer.es/tecnologia/revistas-tecnologia/computer-hoy/suscripcion-computer-hoy

Por teléfono: 915 140 600 / **Por email:** suscripciones@axelspringer.es

Cada suscriptor tendrá acceso gratuito a la edición digital de Computer Hoy en Kiosko y Mas. Accesible desde PC, smartphones y tablets, con sistemas Windows 8, iOS y Android


LOS 100 MEJORES JUEGOS RETRO
DESCUBRE CON RETRO GAMER LOS TÍTULOS CLÁSICOS MÁS RECORDADOS POR NUESTROS LECTORES Y ALGUNOS DESARROLLADORES
TEXTOS DE ADAM BARNES, DAVID CROOKES, WILL FREEMAN, DAMIANO GERLI, FAITH JOHNSON, DARRAN JONES, PAUL KAUTZ, GRAEME HASON, RORY MILNE Y NICK THORPE
YA A LA VENTA
¡VIEJUNO!
retro GAMER
LA PUBLICACIÓN DEFINITIVA SOBRE VIDEOJUEGOS CLÁSICOS
MARIO EN SU PAPEL MÁS AVENTURERO
REJUGAMOS LA SAGA PAPER MARIO
40º Aniversario
1984-2024
LOS 100 MEJORES JUEGOS RETRO
LA LISTA DE TITULAZOS IMPRESCINDIBLES DEFINITIVA
DINAMIC
CUATRO DÉCADAS DE TALENTO, PASIÓN Y VIDEOJUEGOS
REPASAMOS TODA UNA TRAYECTORIA DE NÚMEROS UNO
DENTRO DE GAME BOY ADVANCE
TODOS LOS SECRETOS DE SU LEGENDARIO HARDWARE PORTÁTIL
HACKERS, CRACKERS Y PIRATAS
ENTREVISTAMOS A QUIENES NOS ROBABAN LAS CINTAS EN EL MERCADILLO
GABRIEL NIETO
DE FORE A NINTENDO ESPAÑA
ADEMÁS CASTLEVANIA II: BELMONT'S REVENGE - DODONPACHI - DIABLO II - RICHARD JACQUES - ICO - LUIGI'S MANSION
¡Viejuno!
¡NOS GUSTA LO RETRO!
SI TE HAS QUEDADO SIN LOS ANTERIORES, CONSÍGUELOS EN NUESTRO STORE:
store.axelspringer.es/retrogamer*