¿Tu ordenador superaría un ciberataque?

30 NOVIEMBRE

DÍA INTERNACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

El **30 DE NOVIEMBRE** se celebra el
Día Internacional de la Seguridad de la Información.

Surgió en el año 1988, como consecuencia del primer caso de *malware* de propagación en red que se registró en el mundo. A raíz de esta situación la *Association for Computing Machinery (ACM)*, decreto que cada 30 de noviembre se recordase a todas las personas la necesidad de proteger sus datos de cualquier tipo de ciberataque.

NAVEGA DE FORMA SEGURA

Seguridad y privacidad suelen ir de la mano, una buena gestión de ambas impedirá a terceros acceder a tu información personal o a las operaciones que realices en la red. Por desgracia, la protección total no existe; pero sí podemos ponérselo más difícil a los hackers. En esta guía encontrarás consejos que te ayudarán a gestionar correctamente tu seguridad informática.

CREA CONTRASEÑAS FUERTES Y SEGURAS

Un estudio de Panda Security reveló que solo el 33 % de los encuestados usan contraseñas diferentes para cada web a la que acceden. Sin embargo, la seguridad de gran parte de la información personal que está online depende de que establezcas contraseñas complejas y diferentes para cada servicio para que estén a salvo de los hackers.

Elegir la fecha de nacimiento o los nombres de los hijos no es suficiente para evitar que tu cuenta sea hackeada y tus datos queden expuestos. Y, además de elegir una combinación fuerte, es importante que definas una diferente para cada sitio. Sabemos que a la larga puede convertirse en una tarea muy complicada, pero pueden ayudarte los gestores de contraseñas, programas que recuerdan nuestras contraseñas y las protegen bajo una sola "contraseña maestra" que será la única que debas recordar.

Pero si no te convence la idea del gestor de contraseñas, estos consejos básicos te ayudarán a evitar problemas:

- **Protege tu email principal.** Es el que se usa para recuperar todas las contraseñas de los sitios web en los que te registras. Por tanto, no utilices esa contraseña en ningún otro lugar y asegúrate de que es una realmente buena.

• **Si están disponibles, activa métodos alternativos de autenticación,** como la doble autenticación con SMS, móvil, etc.

• **Prueba alguna de las múltiples páginas web que hay en internet** para comprobar si tus contraseñas son fuertes y cuánto tiempo tardaría una máquina en averiguarlas.

• **Crea variantes de una contraseña.** Puedes tener una contraseña fácil y una difícil y amoldarlas a los requisitos de los diferentes sitios: usa las fáciles en los servicios poco importantes y la difícil restrínjala a lo importante (cuenta de correo principal, Google, iCloud...).

• **No uses la contraseña del router para nada más.** Suele conocerla demasiada gente (familiares, amigos, visitas). Tampoco las de las cuentas compartidas (Netflix, Movistar...).

• **Comprueba de vez en cuando si tus contraseñas se han filtrado** en alguna base de datos a través de páginas como https://haveibeenpwned.com; si aparecen en los listados, cámbialas.

• **Protégete del phishing,** la principal forma de robo de credenciales, con un buen antivirus. Si quieres saber cuál es el mejor, puedes consultar nuestro comparador: www.ocu.org/comparar-antivirus

LA RECETA PERFECTA PARA CREAR CONTRASEÑAS ROBUSTAS

¡Solo 39 minutos necesita un hacker aficionado para descifrar una contraseña de 8 dígitos! Así que, crear contraseñas seguras es fundamental para no poner en riesgo la seguridad de tu información personal. Una contraseña fuerte debe tener al menos 12 caracteres y mezcla minúsculas, mayúsculas, números y símbolos, y que siempre sea distinta. A simple vista, parece complicado recordar varias contraseñas de estas características, pero con estos trucos puedes conseguirlo:

TUNEA UNA FRASE

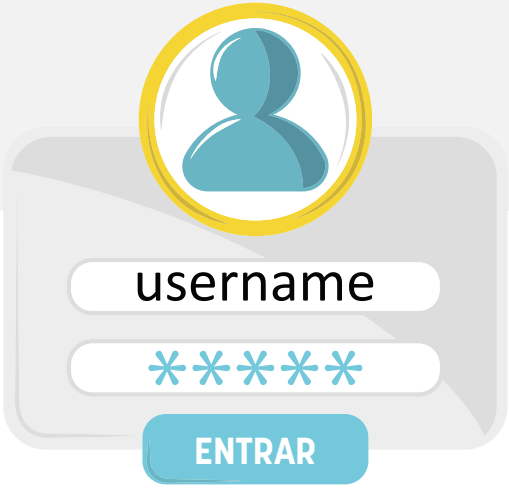
Usa una frase simple y complícala añadiendo símbolos como guiones, arrobas o mayúsculas: *Tengo 2 hijos pequeños* → Tengo-2-Hijos-Pequeñ@s

UTILIZA UNA FRASE ENTERA LARGA

Inventa una frase que tenga mayúsculas, números y algún símbolo, como paréntesis, exclamaciones, comillas... por ejemplo: *Llevo viviendo en Madrid 3 años (y 2 meses).*

CIFRA UNA FRASE LARGA EN ALGO MÁS CORTO

Si usar una clave como la anterior te resulta demasiado larga para cada vez que te conectas, puedes ser creativo y reducirla de la siguiente manera: *"LlveM3@(&2m)".* Como ves, hemos utilizado las comillas, las iniciales de cada palabra o el truco de sustituir la "a" por la "@" y la "y" por la "&".



INSTALA UN ANTIVIRUS

Contar con un buen antivirus es otro pilar fundamental para proteger tu seguridad. Sabemos que no siempre es fácil dar con el adecuado si uno no está familiarizado con el tema, por eso te damos unas pistas básicas para que sepas elegir el mejor para tu equipo.

• **Asegúrate de que sea apto para tu ordenador.** Si tienes un equipo algo viejo, con poca memoria RAM, un procesador lento o poco espacio de almacenamiento, asegúrate de que el software que has elegido es óptimo para este tipo de dispositivos. Y si no eres un usuario experto, busca una opción que tenga una buena valoración en la facilidad de uso.

• **Mejor con protección frente a phishing.** No todos los antivirus cuentan con protección antiphishing y los navegadores web no protegen completamente frente a este tipo de engaño. Asegúrate de elegir uno que sí lo ofrezca.

• **Algunos incluyen otras funciones extra.** Muchos fabricantes incluyen en algunas de sus versiones funciones adicionales relacionadas con la seguridad, como pueden ser la VPN (para conectarse de manera privada desde cualquier sitio), el control parental (para monitorizar el uso de dispositivos en menores) o herramientas de optimización del PC (para acelerar el funcionamiento del mismo borrando programas

y ficheros innecesarios del ordenador). Si ves que vas a necesitar alguna de ellas, elige el programa que más te conviene en función de cuantas de estas funciones tenga integradas.

- **¿Un gratuito o de pago? A decir verdad, algunos productos gratuitos ofrecen resultados muy buenos.** Puedes tener un antivirus con altas prestaciones sin pagar un céntimo, a cambio de soportar anuncios y ventanas emergentes que te sugerirán continuamente que te pases a la versión de pago.

- **Otra opción es *Windows Defender*,** el antivirus que viene instalado por defecto en los equipos de este sistema operativo. Si bien nuestros estudios han evidenciado que Microsoft ha mejorado la calidad de su producto en los últimos años, sigue careciendo de protección antiphishing, ralentiza el PC y da muchos falsos positivos, detectando como potencialmente infecciosos archivos limpios o bloquea el acceso a páginas web que realmente no tienen ningún problema.

- **Ten cuidado ¡los hay falsos!** Hay programas que se muestran como antivirus y que en realidad son todo lo contrario, que solo buscan obtener un lucro por el pago de un programa que no funciona o incluso puede ser un virus de verdad. Normalmente se muestran como anuncios de páginas webs que te instan a instalar urgentemente un antivirus porque tu ordenador está infectado. Desconfía de esos avisos, solo un antivirus que realmente esté instalado en tu ordenador puede saber si tienes virus o no. Te recomendamos que recurras a las marcas conocidas y de prestigio pues cualquier antivirus tiene acceso a todos tus archivos y tus historiales de navegación, así que más vale fiarte del fabricante.

- **Siempre actualizado.** Una vez hayas descargado el antivirus nuevo, no te olvides de actualizarlo. Es fundamental actualizarlo siempre que sea necesario.

¿QUIERES ELEGIR EL MEJOR ANTIVIRUS?

Comparamos las características, marcas, compatibilidad con el sistema operativo, funcionamiento y precios de los mejores modelos del mercado. En OCU hemos analizado los antivirus para Windows más habituales del mercadopara que sepas qué programa instalar en tu ordenador, porque no todos son iguales y los reclamos publicitarios son engañosos. Consulta los resultados en nuestro comparador para elegir el que mejor se adapta a tus necesitades.

www.ocu.org/tecnologia/antivirus/comparador

PROTÉGETE DEL PHISHING

El phishing es una técnica de engaño que utilizan los piratas informáticos para robar nuestros datos a través de la página web falsa de alguna institución oficial, de nuestro banco o de cualquier empresa o tienda que consideraríamos de confianza.

El ataque de phishing suele llegar a través de un mensaje o correo electrónico, por lo que te sugerimos que prestes atención a las siguientes señales:

- **Comprueba que el nombre del remitente es conocido y que la dirección de correo electrónico es legítima.** Para ello, asegúrate de que el dominio (texto que se encuentra a la derecha de la arroba "@") se corresponde con la empresa de la que dice provenir.

- **Desconfía cuando se use un lenguaje con errores de ortografía o redacción.** Estos ciberdelincuentes suelen usar traductores automáticos.

- **Pasa el ratón por encima de cualquier enlace o link que contenga el email.** Normalmente aparecerá en una pequeña ventanita la dirección URL "real" a la que dirige ese link. Si no coincide con la que aparece en el email o crees que no se

corresponde con la del sitio que representa, probablemente se trate de phishing.

- **Si el contenido del mensaje te parece sospechoso probablemente lo sea (o bien phishing o bien un virus):** premios de sorteos en los que no participaste, ofertas de trabajo para las que no aplicaste, multas que no te constan... Revisa estos correos dos veces antes de actuar.

El phishing es una amenaza que afecta a todos los dispositivos por igual, ya sea una tableta, un ordenador o un móvil, y sea cual sea el sistema operativo. Aunque el sentido común es la mejor herramienta que tienes para evitar picar el anzuelo, usar un buen navegador y un antivirus, como ya hemos visto antes, ayuda a bloquear muchas de las amenazas.

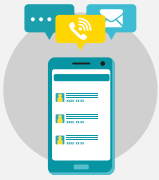
En un reciente análisis de OCU, intentamos acceder a 800 páginas de phishing con los navegadores web más comunes entre los usuarios, pudimos comprobar que los mejores, como Mozilla Firefox o Microsoft Edge en Windows fueron capaces de bloquear más del 80% de las amenazas. Sin embargo, Google Chrome, que es el navegador más usado por los españoles, solo bloqueó el 28% de las páginas fraudulentas en el sistema operativo Windows y el 25% en el sistema operativo Mac.

¿CREES QUE TE HAN HACKEADO LA CUENTA?

Si pese a todas las precauciones crees que has podido caer en la trampa y has dado datos personales en alguna página fraudulenta o sospechas de que alguien te ha hackeado tu cuenta, debes hacer lo siguiente:

- **Cambia de nuevo la contraseña del sitio.** Tienes dos formas de hacerlo: utilizando la opción de "he olvidado mi contraseña" o bien buscando entre tus correos alguno del servicio hackeado (podría estar en la carpeta de elementos eliminados) que diga que has cambiado la contraseña y deshaciendo el cambio desde ese correo.

- **Busca como denunciarlo.** Mira dentro de los ajustes del servicio que te han hackeado; en "ayuda" o "seguridad" deberías poder reportar este robo.



- **Avisa a tus contactos de que te han robado la cuenta de la red social.** El hacker podría haberse comunicado con tus conocidos.

- **Valora los riesgos.** Piensa si usabas el mismo usuario y contraseña (o muy parecida) en otros sitios y cámbialas también.

- **Recurre al servicio nacional de la oficina del internauta.** Entra en www.incibe.es/linea-de-ayuda-en-ciberseguridad y pide ayuda, es un servicio gratuito y confidencial.

¡BIENVENIDO A OCU!

Una comunidad de consumidores decididos
a ser actores del cambio.

Al convertirte en **Amigo de OCU** puedes
disfrutar de una información sin letra pequeña,
de los consejos de expertos independientes y
podrás dialogar con otros consumidores.

www.ocu.org/amigo

Textos: OCU Ediciones, S.A.
C/Albarracín, 21 • 28037 Madrid
tienda.ocu.org