CONCEJOS

3 claves imprescindibles para tu seguridad en Internet

Por Netvez · 01 de abril de 2019 · 12 min de lectura

> *¿Te has parado a pensar alguna vez en que la seguridad en Internet es un tema similar a la salud? Es una cuestión importante, pero no solemos reparar en ella hasta que tenemos un problema. Y normalmente también nos cuesta aplicar medidas de prevención para evitar sustos, aunque sepamos que son neces*

¿Te has parado a pensar alguna vez en que **la seguridad en Internet** es un tema similar a la salud? Es una cuestión importante, pero no solemos reparar en ella hasta que tenemos un problema.

Y normalmente también nos cuesta aplicar medidas de prevención para evitar sustos, aunque sepamos que son necesarias.

Nuestra vida online abarca cada vez más ámbitos. Ya no solo nos comunicamos o compramos por Internet, **cada vez gestionamos más asuntos en sitios web y aplicaciones**, y tenemos más dispositivos conectados a la red.

Gestiones bancarias, citas médicas, dispositivos inteligentes para controlar la música, la limpieza o las luces de tu casa.

El futuro que veíamos en las películas de ciencia ficción ya es nuestro presente y detrás de su cara amable e innovadora se esconden numerosos riesgos para los usuarios.

Cada vez pasamos más tiempo conectados y por lo tanto dejando más y más rastro de nuestra actividad.

Si le añadimos que el robo de datos personales, se encuentra entre los principales objetivos de los cibercriminales y es un negocio cada vez más lucrativo, no hay que esperar a que nos ocurra un incidente grave para **¡tomar acción desde ya!**

3 claves para mantener tu seguridad en Internet

Continuamente se publican noticias relacionadas con brechas de seguridad en empresas, redes sociales e incluso instituciones. Y las consecuencias de estas problemáticas suelen incluir claves de acceso comprometidas e información privada expuesta de forma pública.

En otras palabras, **tus datos privados pasan a estar a la vista de cualquiera**. Los hackers no descansan y lo mejor que puedes hacer es ponerles las cosas difíciles.

¿Tu contraseña es 12345 o tu fecha de cumpleaños?

Para empezar, analiza los datos de acceso que sueles utilizar para tus cuentas y servicios. Repasa tus nombres de usuario y las *password* que has asignado a cada uno de ellos.

¿Cómo de complejas son tus contraseñas? ¿Cuántas veces eliges la misma para diferentes sitios?

La fortaleza de las combinaciones que uses como contraseña es importante, y también lo es que uses combinaciones diferentes para cada sitio.

Dos horas y media

Esto es lo que tardaría un atacante en obtener una contraseña tipo de 8 caracteres. De hecho, puede ponerse mientras a ver una película en Netflix y para cuando acabe ya tiene acceso a tu cuenta.

La prueba la han hecho los desarrolladores de **Hashcat**, una herramienta de código abierto pensada para la recuperación de cuentas y contraseñas.

Pero el problema no está solo en qué datos de acceso eliges, sino también en cómo los almacenas. No sirve de nada usar una contraseña digna de formar parte de un jeroglífico si la guardas de forma insegura y resulta sencillo hacerse con ella

Una libreta o un archivo de texto en tu ordenador, son dos malas ideas.

Ah y por cierto, no guardes las contraseñas en el navegador, existen programas nada complicados que permiten extraer las contraseñas almacenadas en nuestros navegadores. Software nada complejo y de fácil acceso como es el caso de **IEPV**.

Evita conectarte a redes no seguras

Todos lo hemos hecho. Vemos el cartel «wifi gratis» y nos conectamos para no aumentar el consumo de datos y por tanto de la factura del móvil.

El problema es precisamente ese, que todos podemos hacerlo, tanto los que nos conectamos para echar un vistazo a Instagram o hacer una compra rápida, como los que se conectan para ver qué hacen los demás.

No son necesarios demasiados conocimientos para monitorizar la actividad de los dispositivos conectados a una red compartida. Y haciéndolo podrías ver todo lo que hacen y los datos que envían y reciben esos usuarios, incluidos números de tarjeta de crédito, usuarios, contraseñas... ¡TODO!

Ataques «man in the middle»

Los ataques **“man in the middle”** se encuentran entre los más populares cuando hablamos de wifis públicas. En este caso un atacante crea una falsa red inalámbrica.

De esta forma el hacker puede interceptar direcciones web, nombres de usuario, contraseñas y toda la información que viaja entre el dispositivo que se conecta a Internet y la red Wi-Fi infectada.

Y no pienses que requiere de un sistema sofisticado, un desarrollador de Firefox lanzó **Firesheep**, una extensión que permitía “secuestrar” sesiones HTTP (conexiones de red, sesiones de usuario, contraseñas, etc.) prácticamente pulsando un botón.

Servidores maliciosos

Otro ataque “clásico” cuando hablamos de WiFis públicas, es el uso de servidores maliciosos. En este caso, el atacante suele escoger una red WiFi pública (por ejemplo la de un restaurante) que no tenga contraseña y la clona con un nombre muy similar para utilizarla como señuelo.

A partir de aquí el hacker puede optar por el ataque “man in the middle” que hemos visto antes o decidir por ejemplo, gracias a una herramienta open-source como FruityWifi, alterar las direcciones IP de los servidores DNS de la víctima para que apunten a servidores maliciosos.

La solución para evitar este tipo de riesgos pasa por no conectarse a wifis públicas o hacerlo siempre a través de una VPN.

Una segunda cerradura para proteger tus accesos

Añadir un segundo factor (2FA) vinculado a tu teléfono móvil para verificar tu identidad, es un seguro adicional del que no deberías prescindir.

El único método que de verdad te da seguridad en Internet hoy en día es la doble autenticación, debes tenerla activa en cuantos servicios te lo permitan.

El sistema de doble identificación evita que si te roban el usuario y contraseña no puedan acceder a ese determinado sitio si además no tienen tu móvil.

¿Recuerdas el reciente hackeo de las cuentas de correo de muchos políticos alemanes? Pues lo evitaron aquellos que usaban un 2FA. □□

La seguridad en Internet es una responsabilidad compartida

En Webempresa, **la seguridad ha sido siempre uno de los pilares de nuestro trabajo**. Es un ámbito al que dedicamos muchos recursos en términos de monitorización y análisis, desarrollo tecnológico, actualización, etc.

Lo hacemos así porque nos tomamos muy en serio el compromiso que adquirimos con nuestros clientes.

No solo debemos ocuparnos de que la velocidad web y el soporte sean los mejores, sino también de que los proyectos que alojamos estén a salvo, haciendo **copias de seguridad** diarias y protegiendo las webs de ataques e intentos de acceso malintencionados.Sin embargo, se trata de una **responsabilidad compartida**.

Hay una parte que podemos gestionar nosotros de forma directa, pero hay otra sobre la que no tenemos capacidad de acción, que es la que corresponde al usuario, es decir, la que te corresponde a ti.

Podemos poner cientos de medidas de seguridad en nuestros servidores, pero **no podemos evitar que uses una contraseña fácil de adivinar** para acceder a tu WordPress o a tu correo.

Por contraseña fácil de adivinar me refiero a 123456 o a tu fecha de cumpleaños, por ejemplo.

Tampoco podemos evitar que **te conectes a una red wifi no segura** en la que alguien pueda ver cómo navegas y los datos que envías por Internet.

Y aunque cada día se publican nuevos artículos sobre seguridad con consejos sobre cómo elegir una buena contraseña o cómo navegar de forma segura, la mayoría de los usuarios siguen con dinámicas muy vulnerables en su actividad online.

> *¿Imagina que dejas la llave de tu casa bajo una maceta junto a la puerta, y tus vecinos saben que la guardas ahí porque te han visto utilizarla.*
>
> *Seguramente pensarás que nadie en su sano juicio debería hacer eso, puesto que algún vecino podría entrar en tu casa cuando se le antojase.*

Eso es precisamente lo que pensamos nosotros cuando vemos casos reales, cada día, de accesos no autorizados o de pérdida de datos de acceso. Las contraseñas son como esa llave que cualquiera podría utilizar o robarte directamente.

Durante años **hemos insistido en la importancia de mantener unas medidas de seguridad básicas**. Hemos aconsejado a nuestros clientes, hemos publicado numerosos artículos sobre seguridad y hemos implementado nuevas medidas de protección en nuestros sistemas.

Pero siempre habíamos sentido que necesitábamos ir más allá, dar un paso más para ofrecer algo más que un consejo.

Queríamos ofrecer una solución. Y como no encontrábamos una solución, la hemos creado, y se llama CiberProtector □□

¿Qué es CiberProtector?

CiberProtector es una herramienta desarrollada por nuestro equipo para hacer que todos podamos dormir más tranquilos □□

Nuestro objetivo es que te resulte muy sencillo **aplicar las medidas de seguridad necesarias para proteger tu vida en Internet** (tu hosting, tus datos, tus transacciones y compras, etc.).

Para conseguir esta protección, CiberProtector incluye 4 servicios diferentes, pero complementarios: un gestor de contraseñas, una conexión VPN, un segundo factor de autenticación y un check de seguridad para tu ordenador y tus dispositivos móviles.

- **Gestor de contraseñas**: para crear, guardar, usar y compartir tus contraseñas de acceso de forma segura. También podrás almacenar documentos e información secreta (códigos PIN, datos bancarios, etc.) y acceder a ellos sin riesgo desde cualquier dispositivo.
- **Conexión VPN**: para garantizar que tu conexión a Internet sea segura. Los datos que envíes o recibas en tus dispositivos se encriptarán y se volverán indescifrables para posibles intrusos, aunque te conectes desde redes wifi públicas o poco seguras.
- **Segundo factor de autenticación**: es el método más fiable para evitar que personas no autorizadas que hayan conseguido tus datos de acceso entren en tus cuentas.

- **Seguridad para tus equipos**: para mantener las medidas básicas de seguridad en tu ordenador y en tus dispositivos móviles.

¿Para qué sirve el gestor de contraseñas?

Piensa en cómo estás gestionando tus contraseñas actualmente.

¿Para cuántos sitios de Internet tienes datos de acceso? Si tienes un servicio contratado con nosotros, solo en Webempresa ya tienes unos cuantos: el acceso al área de cliente, a cPanel, a tus cuentas de correo…

Y es probable que uses contraseñas muy débiles (tu fecha de nacimiento, el cumpleaños o incluso 12345) y que las repitas en diferentes sitios para no tener que acordarte de muchas combinaciones distintas.

También es posible que tengas que usar de vez en cuando el famoso '¿Has olvidado tu contraseña?' para sitios en los que no entras muy a menudo, porque no recuerdas los datos de acceso.

CiberProtector resuelve estos problemas con el gestor de contraseñas. Podrás crear contraseñas fuertes (y por tanto más difíciles de adivinar o conseguir) y tener una diferente para cada sitio web, porque no tendrás que recordarlas todas

CiberProtector las almacenará de forma segura (encriptadas) y te las facilitará en cualquier momento desde un plugin en tu navegador o una APP en tu móvil. Tu solo tendrás que recordar una contraseña: tu contraseña maestra de CiberProtector.

Todos tus datos se almacenarán en la nube de CiberProtector, y evitarás tenerlos guardados en el navegador (que es algo muy inseguro) o anotados en libretas o archivos de texto o excel, a la vista de cualquiera.

¿Para qué sirve la conexión VPN?

Cuando te conectas, por ejemplo, a un red wifi pública de una cafetería o un aeropuerto, corres el riesgo de haya "espías" viendo lo que haces: la información que consultas, los datos

que envías, etc. Esto también puede pasarte con la conexión wifi de tu casa si no tienes las medidas de seguridad básicas.

No te hablo de un riesgo remoto pensando en la posibilidad de que tu vecino sea un hacker. Cualquier persona con unos conocimientos básicos podría conectarse a tu dispositivo a través de la wifi si no tomas precauciones.

Una VPN es como una red de seguridad para tu conexión a Internet.

Al conectarte a través de la VPN se crea una especie de túnel seguro para ti, y esto hace que esos posibles espías no puedan ver nada de lo que haces porque toda la información se envía y se recibe encriptada. Todos los datos que envíes o recibas al navegar se volverán indescifrables para posibles intrusos.

Tendrás una conexión segura de alta velocidad para trabajar tanto con tu navegador como con tus aplicaciones; y te servirá para todos tus dispositivos (ordenador, móviles y tablets).

¿Para qué sirve el segundo factor de autenticación?

Para explicarte cómo puede ayudarte tener un **segundo factor de autenticación (2FA)**, te pondré un ejemplo práctico. Imagina que trabajas en una oficina con más personas, y que por casualidad un compañero ve cómo accedes a tu correo electrónico y cuáles son tus datos de acceso.

Tan solo con apuntarse esos datos podría entrar en tu correo sin tu permiso. El segundo factor de autenticación sirve precisamente para evitar esto.

Configurando un 2FA tendrás una aplicación en tu teléfono que te dará un código numérico para completar la verificación en el momento de acceder. Estos códigos son únicos y cambian cada 30 segundos, por lo que aunque alguien se quede con tus datos de acceso no podrá ver tus cuentas sin tu permiso porque no dispondrá del segundo factor necesario para acceder.

¿Para qué sirve el sistema de seguridad para dispositivos?

Tu ordenador y los dispositivos móviles que usas para conectarte a Internet deben mantener unas medidas básicas para no ser vulnerables. Lo habitual en estos casos es pensar en un antivirus, pero hay otros factores adicionales que hay que tener en cuenta.

El servicio de seguridad analiza el estado de esas medidas en tus equipos para decirte cuáles están aplicadas correctamente y cuáles debes activar o configurar.

En resumen, te indica si la configuración de tu equipo, tablet o móvil es correcta a nivel de seguridad o debes modificar algún parámetro.

Fuente: Webempresa