VISITA
NUESTRA
EDICIÓN
DIGITAL

BUSCANDO PARCHES PARA EL OJO DE GRAN HERMANO

Consejos de seguridad digital

TEXTO **JAVIER ORTEGA** | ILUSTRACIÓN **THINKSTOCK**

Aunque hoy la mayoría asocia el concepto *Big brother* a un fenómeno televisivo, la realidad digital en la que estamos inmersos bien podría remitirnos a la intuición profética del ojo que todo lo ve concebido por George Orwell en su novela *1984*. Vivimos en una especie de casa de cristal. Cualquier cosa que hacemos en internet deja huella. Aunque creamos que nuestras comunicaciones son seguras, el simple hecho de estar conectados hace que mucha más gente de la que creemos tenga acceso a nuestra información.

En la era de la "democratización digital" el porcentaje de ciudadanos con conexión a internet se incrementa a diario. La generalización del uso de internet ha traído innumerables ventajas pero también lleva asociados algunos inconvenientes. El mayor riesgo es el acceso impune a nuestra información por parte de terceros. Evitar que estos invitados no deseados se cuelen en nuestra vida depende en gran medida de cada uno de nosotros.

No hay métodos infalibles pero se puede empezar por subir la guardia y desterrar la sensación de confianza que tienen los que piensan que estas cosas siempre les pasan a otros. La clave no es tener miedo a usar los recursos digitales a nuestro alcance, sino crecer como ciudadanos digitales responsables y tomar conciencia de cuáles son las normas básicas para el uso seguro de Internet. Esta actitud es la que deben adoptar también las empresas a la hora de afrontar los riesgos que acechan y trabajar para mejorar la experiencia de sus clientes. Para Guillermo Llorente, subdirector general de Seguridad y Medio Ambiente de MAPFRE, "no se puede vivir al margen de esta realidad, que está aquí para quedarse. No tenemos que preocuparnos, sino ocuparnos".

Opciones a nuestro alcance

PC, portátil, teléfono móvil, tableta, smart TV, relojes inteligentes... Nuestras opciones de conexión crecen sin parar y con ellas se multiplican los lugares en los que se almacena parte de nuestra información privada como la agenda de contactos, contraseñas de servicios bancarios, correos electrónicos, fotografías y vídeos, etc. Conviene, en primer lugar, tener claras las opciones de seguridad que nos ofrece cada dispositivo al que nos conectamos y, en aquellos casos en los que sea posible, protegerlos con una solución de seguridad pensada particularmente para ellos, como un antivirus u otras aplicaciones específicas. También es importante tener siempre actualizado el software o sistema operativo base (Windows, MacOS, iOS, Android...) de cada aparato, ya que en las versiones más recientes se contemplan las

últimas lagunas de seguridad detectadas. No hacerlo puede tener consecuencias. En España, por ejemplo, uno de cada cuatro casos de asistencia informática que resuelve el seguro está relacionado con problemas de virus y con la instalación de antivirus.

Con un simple vistazo a tu navegador puedes comprobar si existen complementos que no usas o, simplemente, no recuerdas haber instalado. De darse el caso, debes deshabilitarlos. Hay veces que, al descargar algún programa y pulsar el botón de aceptar, sin darnos cuenta, estamos autorizando la instalación de otras utilidades que muchas veces recopilan nuestros datos de navegación o, en el peor de los casos, pueden ser vías para introducir virus o *software* malicioso (*malware*). Otra recomendación básica, y de la que solo nos solemos acordar cuando ya es tarde, es la de hacer con frecuencia copias de seguridad de nuestro dispositivo. Llegado el caso, si se realiza periódicamente esta práctica puede minimizar considerablemente la pérdida de datos e información importante.

Peligros en red

Aunque el ordenador es donde parece más obvia la necesidad de controlar la seguridad, estas precauciones pueden trasladarse a otro tipo de aparatos que forman parte de nuestro ecosistema doméstico y han incorporado últimamente internet a su funcionamiento, como las smart TV o las videoconsolas.

La configuración de opciones de seguridad no acababa en nuestros terminales. Cada app, la mayoría de las webs y, por supuesto, todas las redes sociales (se acceda a ellas de una u otra manera) tienen sus propios ajustes de privacidad (en el caso de las app, este espacio suele identificarse con el icono de una rueda dentada). Por lo general, accedemos a este espacio la primera vez que tomamos contacto con un sitio o aplicación pero luego cae en el olvido. No es mala costumbre revisar este rincón de vez en cuando. Además, las políticas de privacidad de los sitios web cambian constantemente y, aunque están obligados a avisarnos, es importante revisarlas.

PARA HABLAR DE UNA **SEGURIDAD ALTA** SE RECOMIENDA USAR EN ELLA POR LO MENOS **12 CARACTERES QUE INCLUYAN MAYÚSCULAS, MINÚSCULAS, SÍMBOLOS Y NÚMEROS.**

PRECAUCIÓN Y SENTIDO COMÚN

Otro aspecto fundamental a la hora de protegerse tiene que ver con el uso de contraseña. Para hablar de una seguridad alta se recomienda usar en ella por lo menos 12 caracteres que incluyan mayúsculas, minúsculas, símbolos y números. No hay que usar una misma combinación en más de una aplicación o dispositivo porque si se da un caso de vulnerabilidad en algún servicio y se filtran las claves (sucedió, por ejemplo, con Adobe) los piratas tendrían las cosas más fáciles.

Descargar software o ficheros de audio y vídeo sin licencia, además de ilegal, es una de las formas más habituales que usan los ciberdelincuentes para acceder a nuestros dispositivos. La mejor manera de evitarlo es no ejercer de piratas. Al final, todo se resume en seguir unas pautas básicas que son igualmente válidas para el mundo offline: ante todo, precaución y sentido común.

ALGUNAS **CLAVES BÁSICAS**

1/

Utiliza contraseñas alfanuméricas en tus cuentas y evita que las claves se basen en información personal (DNI, número de teléfono, fecha de nacimiento, nombres de familiares, etc.) o patrones muy sencillos (12345).

2/

No uses la misma contraseña en más de un lugar y renuévalas periódicamente.

3/

Evita navegar en redes Wi-Fi abiertas, y si lo haces no accedas a cuentas personales de email, banco, redes sociales, etc.

4/

El router que tenemos en casa es la principal puerta de acceso a tu red doméstica y a todos los dispositivos conectados a ella, especialmente con el acceso Wi-Fi. Asegúrate de que el nivel de seguridad de acceso a la Wi-Fi está en WPA2 y que la contraseña de acceso es robusta.

5/

Modifica la contraseña y el nombre de usuario que viene por defecto con el router. Hay aplicaciones especialmente diseñadas para adivinar los patrones seguidos por las compañías telefónicas para las claves de acceso que tienen asignadas.

6/

Instala antivirus o aplicaciones de seguridad pensadas para cada tipo de dispositivo.

7/

Navegando, nunca abras links o ficheros adjuntos sospechosos, aunque puedan procedan de alguien conocido y bajo ninguna circunstancia si no conocemos a quién los remite.

8/

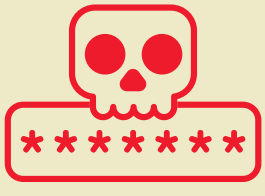
En las compras online, verifica que operas en webs conocidas y seguras antes de realizar cualquier tipo de pago (deben usar el protocolo https:// y generalmente aparece un candado en la barra de dirección).

9/

No instales programas si desconoces el fabricante y descárgalos siempre de la página oficial del mismo. Si son de pago y los encuentras gratis en otras páginas será por algo.

10/

Aumenta la seguridad de tus tarjetas de crédito para el uso en Internet. Hoy en día los bancos ofrecen este servicio de forma gratuita, introduciendo medidas de seguridad adicionales como envío de SMS o preguntas de verificación que evitan a terceros hacer uso en internet de nuestras tarjetas aunque dispongan de todos los datos.



¿SABÍAS QUE?

SE TARDA **10 MINUTOS**

EN HACKEAR UNA CONTRASEÑA DE **6 CARACTERES MINÚSCULAS**

SE TARDA **3 AÑOS**

EN HACKEAR UNA CONTRASEÑA DE **8 CARACTERES CON ALGUNAS LETRAS MAYÚSCULAS**

SE TARDA **44.530 AÑOS**

EN HACKEAR UNA CONTRASEÑA DE **9 CARACTERES CON NÚMEROS Y SÍMBOLOS**