Publicado en el 25/11/2015

Los virus informáticos infectan al 46% de usuarios

Estos son los principales resultados de la encuesta sobre seguridad en Internet que OCU ha realizado a 549 españoles mayores de edad:

Lo que nos da miedo

Las empresas y sus intenciones: son muchas y están dispuestas a pagar por tener acceso a tus datos personales. Esa información (email, teléfono, aficiones...) vale dinero porque luego se usa para intentar venderte productos. Nueve de cada diez encuestados cree que hemos perdido el control y al 70% no le gusta nada esta tendencia. Recuerda, tus datos son tuyos: firma para que se enteren en el Ministerio de Justicia.

La violación de la intimidad: tus emails, tu estado de salud, tus hábitos sexuales, fotos privadas.... todo puede acabar en manos de extraños. A la mayoría le preocupa y un 54% ha reaccionado teniendo más cuidado con lo que comparte.

Las fuerzas del Estado: el 70% expresa desasosiego porque las agencias gubernamentales puedan pinchar comunicaciones de manera masiva.

Lo que debería darnos miedo

Somos mucho más conscientes de los peligros que hace una década, pero aún hay mucho que avanzar:

el 10% no tiene ningún antivirus en su ordenador.

un 5% no cree que sea arriesgado abrir los archivos adjuntos del mail que te envía un desconocido.

el 20% de los encuestados usa la misma contraseña en varias cuentas online.

un 29% de los que navegan con WiFi no ha configurado los parámetros de su conexión.

el 77% no hace copias de seguridad con regularidad.

Lo que de verdad nos pasa

Aunque la preocupación entre los usuarios es grande, son relativamente pocos quienes han tenido problemas con la seguridad en Internet:

10 maneras de perder el miedo

La protección total es imposible, pero minimizar riesgos es bastante sencillo:

1. Instala un antivirus: y tómate el tiempo de configurarlo. Si quieres más garantías, instala también un firewall.
2. No pases de las actualizaciones: tienes que trabajar con la última versión disponible del antivirus, del sistema operativo y de los principales programas.
3. Haz copias de seguridad periódicamente
4. Navega con brújula: es decir, no hagas clic en todos los pop-ups que saltan a tu encuentro, no descargues software de webs no oficiales, no vayas a páginas de poca confianza y jamás entres en la web de tu banco desde un email que te ha llegado.
5. Cuidado con los ordenadores ajenos: si el equipo no es el tuyo, no hagas operaciones bancarias y

desmarca siempre la opción de "guardar contraseña".

6. No compartas tus contraseñas: no se las digas a nadie. Elige una diferente para cada cuenta: mejor si no usas palabras del diccionario y si no son fácilmente deducibles basándose en tu fecha de nacimiento, nombre, ciudad... Ni se te ocurra guardarlas en un documento de texto.

7. No compartas toda tu intimidad: antes de publicar en una red social sé consciente de que el público potencial es la humanidad entera. En Twitter es exactamente así. En Facebook, si has configurado bien la privacidad, lo más probable es que no vaya a ser así... pero nunca se sabe.

8. Tu móvil también es vulnerable: los antivirus para smartphones aún tienen mucho que mejorar, pero puedes optar por ser prudente. No descargues apps de tiendas no-oficiales, utiliza patrones o contraseñas de bloqueo de pantalla, instala una app de control remoto que te permita borrar todos los datos personales si pierdes o te roban el teléfono...

9. Cuidado con el WiFi: si es una red pública (un bar, un hotel, una biblioteca...), ten en cuenta que los datos que envías podrían quedar registrados.

10. No digas constantemente dónde estás: la geolocalización es tremendamente útil, pero que todo Internet pueda saber en cualquier momento dónde te encuentras entraña riesgos.

Datos de contacto:

Nota de prensa publicada en:

Categorías: E-Commerce Ciberseguridad