ABC (EDICION NACIONAL)
MADRID
08/09/12
Prensa: Diaria
Tirada: 326.584 Ejemplares
Difusión: 249.539 Ejemplares
Cód: 61417909
Página: 44
Sección: SOCIEDAD Valor: 21.142,00 € Área (cm2): 707,9 Ocupación: 93,76 % Documento: 1/2 Autor: ANDREA C. FERNÁNDEZ S. Núm. Lectores: 670000

Intimidad bajo mínimos en la

▸ Los expertos alertan de los riesgos de compartir de forma compulsiva la vida privada a través de las redes sociales y la mensajería instantánea

ANDREA C. FERNÁNDEZ S.
MADRID

La filtración y publicación de un vídeo erótico de la concejala de Los Yébenes ha puesto sobre el tapete informativo a internet, las redes sociales y el concepto actual de la privacidad. Grabar un vídeo o hacer fotografías subidas de tono no es un delito o una perversión cuando se limita a la intimidad. El problema llega cuando esta información es publicada en la World Wide Web y millones de personas acceden a ella. Es un riesgo, que por más antivirus que tenga un PC, se corre cuando se está en el plano de redes sociales o la mensajería instantánea.

«Todo lo que pongas en internet se va a replicar. Una vez que saques algo de tu ordenador, esta información deja de ser tuya y empiezas a estar en riesgo», explica Mario García, director general de la empresa Check Point, especialista en seguridad para internet. García hace el símil con el envío de cartas. «Siempre que hay un sistema de intermediarios, tu mensaje puede estar en peligro. Imagina que envías una carta con dinero. Si tu no la entregas personalmente al destinatario, existe la probabilidad de que el mensajero se quede con el dinero», señala.

Para García, el problema se agrava cuando entran en juego las redes sociales —Facebook, Twitter, Flicker o Instagram—, ya que, considera, que las personas no terminan de entender los peligros que encierra este sistema diseñado para compartir. «Las redes sociales son como un tablón de anuncios donde en principio dejas solo entrar a tus amigos más cercanos. Si le das permiso a una persona desconocida, simplemente se convierte en alguien de afuera que te puede robar lo que hayas publicado en ese tablón», considera García. Para este especialista en seguridad, cada usuario, antes de compartir un contenido, debe hacerse una pregunta clave: «¿Publicaría esto en la cartelera de la comunidad de vecinos o en el tablón del colegio? La mayoría de las personas nunca haría eso en la vida física», relata.

Manuel Ransán, del Instituto Nacional de Tecnologías de la Comunicación (Inteco), sigue en esta línea. Ransán ya advertía en declaraciones a ABC el pasado mayo que para evitar ser víctimas de filtraciones y publicaciones de documentos privados, lo más idóneo es no realizar en la web «cosas que no harías» fuera de ella. Es decir, llevar la vida «digital o virtual», tal cual se maneja la vida física.

De vuelta al pueblo

Detrás de los fallos de seguridad o acciones imprudentes realizadas en la web, existe otro tema de fondo; el concepto de privacidad. Según el Diccionario de la Real Academia Española, privacidad es el «ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión». Sin embargo, Enrique Dans, profesor y especialista en Sistemas de Información, considera que esta concepción ya no es la misma de la de hace una década.

«El concepto de privacidad ha cambiado. Estamos ante la primera generación que está rodeada siempre de conectividad», explica Dans. «El disfrute de algo ya no termina cuando acaba, sino cuando compartes las fotos o el vídeo de lo que pasó. En los via-

DECÁLOGO PARA PROTEGERSE DE LOS PIRATAS

Blindar con antivirus a los ordenadores

La Oficina de Seguridad del Internauta recomienda proteger el ordenador con un antivirus y actualizarlo periódicamente. Mientras más se tarde en actualizar, mayor será el peligro de virus.

No meter claves en los PC de lugares públicos

Evite utilizar los ordenadores públicos de hoteles, cafeterías, para acceder a servicios que requieran contraseña. En estos dispositivos no se conoce su nivel de seguridad y protección.

No confiar en anuncios maravillosos

CheckPoint señala que no se debe ser ingenuo y pinchar en anuncios sospechosos. Si le llama la atención el anunció, diríjase a la web original que coloca el anuncio y evitará contraer un virus.

Cautela con las redes Wifi abiertas o públicas

A menos que sea necesario, no utilice estas redes, y menos para manejar información importante. Allí los datos son más susceptibles de ser interceptados y captados por hackers.

Reforzar la contraseña del Wifi en casa

Los expertos dicen que un hacker común puede descifrar la clave original de tu Wifi casera fácilmente. Para evitar que alguien usurpe tu red o tenga acceso a sus datos, cambie la contraseña genérica por una complicada.

Cuidar la privacidad en redes sociales

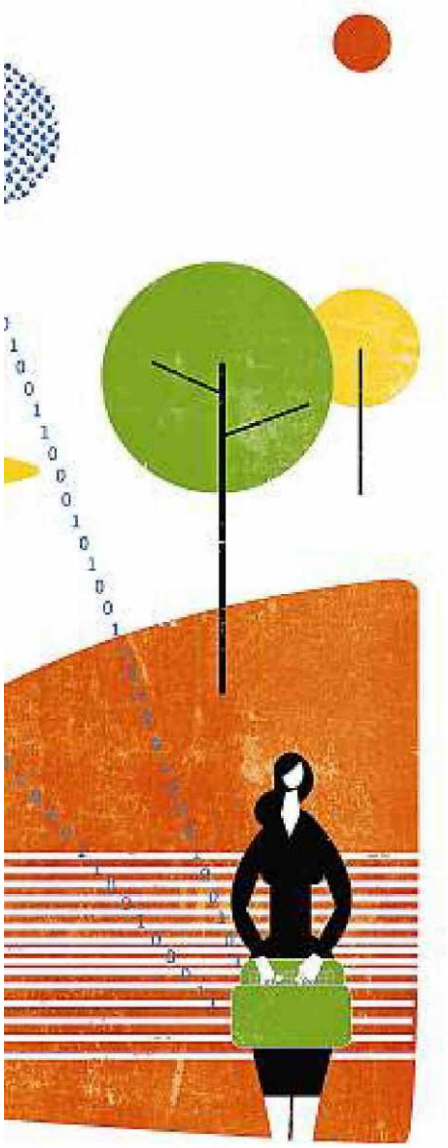
Evite aceptar a desconocidos en Facebook y otras redes sociales o colocar fotos de tu casa o geolocalización. Esta información podría ser usada por delincuentes y perjudicar a su familia.

Descargar aplicaciones certificadas

La información que se comparte o almacena en el móvil también está en riesgo si se descargan «apps» inseguras. Adquiera sus

ABC (EDICION NACIONAL)
MADRID
08/09/12
Prensa: Diaria
Tirada: 326.584 Ejemplares
Difusión: 249.539 Ejemplares
Cód: 61417909
Página: 45
Sección: SOCIEDAD Valor: 10.962,00 € Área (cm2): 367,0 Ocupación: 48,61 % Documento: 2/2 Autor: ANDREA C. FERNÁNDEZ S. Núm. Lectores: 670000

era de internet



IVÁN MATA

jes de vacaciones, o fiestas, cuando no se tiene la conexión de datos y no se puede compartir la información al instante, la experiencia te parece incompleta», señala este especialista.

Por algo ya Facebook tiene 900 millones de usuarios, Twitter ha alcanzado los 500 millones o Whatsapp en marzo de este año tenía ya 10 millones de usuarios solamente en España. Marshall McLuhan lo adelantaba con su teoría de la aldea global décadas atrás. «La aldea global es un mundo en el que tienes mucha preocupación por los asuntos de los demás y en la que estás más involucrado con la vida de otras personas.(...) La aldea global es tan grande como el planeta Tierra, pero al mismo tiempo tan pequeña como el tamaño de la oficina de correos de un pequeño pueblo».

Esta vuelta al pueblo es lo que destaca también Enrique Dans, que cita a Mark Zuckerberg, creador de Facebook, quien establece que el concepto que se conocía de privacidad se dio de manera accidental. «La privacidad fue un accidente histórico. Antes, cuando se vivía en los pueblos, se sabía todo sobre la vida de las personas. Lo realmente privado eran cosas muy íntimas. Con el paso del tiempo, las ciudades fueron creciendo y las personas perdimos la capacidad de almacenar tanta información de tanta gente, no teníamos el ancho de banda mental suficiente. Ahora con las redes sociales hemos podido recuperar ese ancho de banda y volvemos al pueblo, a conocer todo acerca de todos con solo entrar en Facebook», apunta el especialista.

El peligro no es solo contra la privacidad. En 2011, unos 413 millones de personas se vieron afectadas por un ataque cibernético. Desde Check Point alertan que aunque una persona no sea el objetivo del ataque, se convierte en parte de una red de crimen. «Los hackers pueden manipular tu PC, y sin que sepas nada, empiezas a envíar spams y virus. A través del ordenador del trabajo pueden contaminar a toda una empresa», concluye.

«apps» desde las tiendas oficiales como App Store o GooglePlay.

Usar el bluetooth en momentos precisos

Evite mantener encendido el bluetooth de su móvil a todas horas. Le pueden ubicar, enviar documentos, virus y dañar su dispositivo. Use esta red inalámbrica en momentos precisos.

Ignorar correos basura o de desconocidos

Tenga cuidado con las campañas fraudulentas que llegan a través del correo basura y remitentes desconocidos. Estos le pueden direccionar a sitios fraudulentos.

Complicar las contraseñas

Tras una quiebra de seguridad en Twitter, se demostró que 55.000 usuarios tenían como clave «1234». Sea más ambicioso y evite contraseñas fáciles. Intente tener una distinta para cada correo electrónico, cuentas bancarias y otras páginas.