



Seguridad también en vacaciones

En verano conviene adoptar precauciones cuando la conexión se realiza dentro de redes inalámbricas o en lugares de acceso público

Por simple afición o por pura necesidad, son muchos los usuarios que ni siquiera en vacaciones se desconectan de Internet: allá donde estén quieren poder gestionar su correo electrónico, escribir en su página web o en un foro especializado, chatear o, sencillamente navegar por la Red. Entre estos usuarios que no pueden o no quieren prescindir de Internet, pueden distinguirse dos tipos de 'veraneantes': los que se llevan consigo ordenador portátil, PDA y todo lo necesario para conectarse a Internet por sus propios medios, y quienes confían en encontrar en su lugar de destino un cibercafé, un locutorio o un ordenador conectado a la Red en el hotel o camping en que se alojan. Unos y otros deben tener en cuenta siempre que la seguridad debe acompañar al acceso a la Red también durante los viajes. La conexión desde un lugar público aumenta las posibilidades de que los intrusos tengan acceso a nuestros datos. La seguridad exige, en estos casos, extremar las precauciones y añadir prácticas que no son tan necesarias en el hogar.

Aplicar el sentido común

Más que a los 'hackers' (mejor llamados 'crackers') que emplean sofisticadas técnicas para introducirse en nuestro ordenador, hay que temer prácticas tan clásicas y elementales como el **figoneo por encima del hombro**. Cuando tecleamos una clave de acceso en un lugar público hemos de comprobar que ojos extraños no vigilen nuestra pantalla o teclado y evitaremos desatender el ordenador si en la pantalla se muestra información confidencial. **Las contraseñas**, conviene recordarlo siempre, deben ser seguras: combinaciones de letras y números de más de seis caracte-

teres que no se puedan asociar a su propietario (el nombre del perro o el cumpleaños de la pareja no son buenas contraseñas). **El intento de captura de nombres de usuario y contraseñas es un delito** y está experimentando un importante aumento, traducido en robos de dinero y suplantación de identidades. Para que la seguridad sea del 100% con un ordenador público, lo más eficaz es no introducir informaciones confidenciales (número de tarjeta de crédito, clave de acceso a servicios bancarios). El PC podría tener instalado software espía que registra las teclas pulsadas. Como no tendremos a mano un programa que detecte y elimine estos *espías*, al salir del ordenador minimicemos el riesgo borrando toda nuestras "huellas", la información sensible que hemos tecleado.

Cómo borrar las huellas

Antes de usar cualquier servicio online, vigilemos que no esté activada **la opción 'guardar contraseña'** o 'inicio automático de sesión', habitual en correo-web (como los de Yahoo! o Hotmail) y programas de mensajería instantánea. Y, respondamos "no" cuando el navegador pregunta si queremos que guarde la contraseña. En la navegación las precauciones son las mismas que en casa: cuidado con los archivos adjuntos a los mensajes y con los descargados de sitios dudosos. **Cuando se sale de una página que requiere registro** cerremos la sesión; y cuando abandonamos el ordenador, cerremos el navegador eliminando antes cualquier rastro que hayamos dejado: con las preferencias del navegador borramos los archivos temporales de Internet (registran todas las páginas visitadas), las *cookies* (puede haber información personal) y el Historial.



En las redes inalámbricas

Las cada vez más ubicuas redes inalámbricas son una bendición para quien viaja con un portátil equipado con tarjeta WiFi (inalámbrica). En aeropuertos, hoteles e incluso en algunos restaurantes y cafeterías, es posible conectarse a la Red por el aire, en muchos casos de forma gratuita. En el acceso a una red pública con el ordenador propio lo que hemos de proteger son los archivos del disco duro, en especial los que contienen información valiosa o confidencial.

El ordenador nos dirá si se trata de una red inalámbrica segura (cifrada o protegida por contraseña, que habrá que conocer) o no, pero en cualquier caso habremos de tener instalado un programa cortafuegos (*firewall*), que evite accesos no deseados al equipo. Si es imprescindible introducir claves o números de tarjeta en una red pública, comprobemos que se emplean páginas seguras: empiezan por *https://* y muestran un candado cerrado en la parte inferior del navegador. ◀

Cuidar el portátil (y su contenido)

Los ordenadores portátiles son un objeto muy 'goloso' para los amigos de lo ajeno: sólo en EEUU, más de medio millón de ordenadores 'cambian de propietario' cada año. Cuando se viaja con un portátil, habremos de vigilar tanto el hardware (el portátil mismo) como la información que almacena. Para lo primero, basta seguir unas reglas tan obvias como habitualmente olvidadas:

- '**Camuflé**' el portátil. Evite transportarlo en un maletín llamativo (mejor una mochila o una bolsa).
- No lo **abandone**. Ni al pasar un control de seguridad, ni en el coche, ni en el hotel. Tampoco en la silla de al lado cuando toma un café.
- Guárdelo en **lugar seguro**. En los aviones, mejor bajo el asiento de delante que en el portaequipajes.

Para proteger lo que llevamos en el portátil habremos de ser precavidos con la conexión en sitios públicos, tanto por la seguridad de la red como por los fisgones a la caza de datos personales. Si extraviamos el portátil, si se estropea o si nos lo roban, podemos reducir el perjuicio que nos causa esta contingencia. Veámoslo:

- Protejamos el acceso al ordenador mediante una contraseña segura y cifremos las carpetas y archivos confidenciales.
- Guardemos una copia de seguridad de los archivos importantes en un servidor de Internet o un llavero USB (o reproductor de MP3), desde los que se podrá recuperar la información dondequiera que estemos. El bajo precio de las grabadoras de DVD facilita el volcado a este soporte del contenido íntegro de nuestro disco duro de manera regular.
- Instalemos un programa que siga la pista del equipo en caso de que se "extravíe", como zTrace o Computrace. Actúan como un radiofaro que indicará -de modo imperceptible para el ladrón- la posición del equipo cada vez que éste se conecta a Internet.
- Sopesemos la opción de asegurar el portátil.

Navegar a la carta



Seguridad en marcha

www.microsoft.com/spain/seguridad/usuarios/onthego/default.mspx

Especial de Microsoft sobre seguridad en portátiles, Pocket PC, dispositivos SmartPhone y otros equipos para conectarse en los viajes.



Cibercafés www.world66.com

Una guía para el turista escrita por los viajeros, con atención especial a los cibercafés repartidos por el mundo. También se pueden localizar en www.cybercafes.com y, en español, en [ociototal \(www.ociototal.com/recopila2/r_internet/cibercafe.html\)](http://ociototal.com/recopila2/r_internet/cibercafe.html).



'Hotspots'

<http://hotspots.netstumbler.com>

Para encontrar puntos de acceso a Internet inalámbricos, conocidos como *hotspots* (a los que acceder mediante la tarjeta Wifi del equipo) en todo el mundo.