

Consumer Reports WebWatch
Proyecto para prevenir el crimen en el ciberespacio
Hoja informativa #10: Protéjase contra los estafadores o ladrones de
identidad en el mundo inalámbrico

Ésta es la décima hoja informativa de la campaña “Ver antes de hacer clic” del proyecto WebWatch de *Consumer Reports*, financiado por la Oficina del Procurador General del estado de Nueva York para ayudar a los consumidores a evitar problemas en línea.

Puede que usted use una computadora portátil en su hogar o negocio. Quizás aún haya establecido su propia red inalámbrica en su casa con routers y repetidores de señales para alcanzar a todos los cuartos de su casa. ¿Sabe que el uso de Wi-Fi y redes caseras crea cierto tipo de riesgos de seguridad y privacidad? Aquí le diremos cómo protegerse contra estafadores de identidad, ladrones que le roban la señal inalámbrica de la red de su casa o piratas informáticos que quieren atacar a su máquina en la relativa tranquilidad del sitio donde se vende café en el aeropuerto.

Acuérdese de que los lugares con red inalámbrica para Wi-Fi son los sitios públicos donde la gente se conecta al Internet. Usando software fácilmente accesible, otros pueden ver los sitios Web que usted está visitando, ver su información de inscripción en sitios no protegidos (para el chat, por ejemplo), y posiblemente ver el contenido de los documentos en su máquina.

¿Qué debe de hacer entonces? Primero, siga las mismas reglas básicas de seguridad en la computación que ha leído en nuestras hojas informativas y en el sitio de *Consumer Reports WebWatch*. Use un programa activo contra los virus (uno que instale programas continuamente para defenderlo contra los últimos desafíos); instale un limpiador de *spyware* para remover software dañino a su computadora; active su cortafuegos y baje los últimos programas de seguridad del fabricante de su sistema. Use la codificación para mezclar y proteger sus comunicaciones. Si puede elegir, use el Wi-Fi Protected Access (WPA), el cual es más poderoso que el Wired Equivalent Privacy (WEP), a pesar de que pudiera requerir equipo más nuevo. Si tiene acceso a una red virtual privada (VPN, por sus siglas en inglés), aprovéchese de su seguridad, pero si es proporcionada por su empleador, considere para qué motivo la usará.

Si el servicio de Wi-Fi requiere que usted pague para usarlo, asegúrese de leer todos los términos y condiciones, y preste atención a la información sobre seguridad y privacidad. Finalmente, piense si quiere hacer sus transacciones bancarias y de tarjetas de crédito desde un lugar más seguro y menos público.

Estos asuntos y sus soluciones son similares al usar la red de su casa. Apague la transmisión identificadora en su router inalámbrico, para que no envíe una señal a cualquier máquina en la vecindad anunciando su presencia. Apague su red inalámbrica cuando sepa que no la va a usar. Haga todas sus claves de acceso más difíciles de identificar, y reajuste las claves de acceso proporcionadas por el fabricante. Además, no deje papeles con sus claves de acceso cerca de su computadora, ni notas en la pared arriba de su monitor. Estos son los primeros lugares que un ladrón buscará si logra a su casa.