Fuente OSI

Protégete al usar WiFi públicas

Conectarse a redes WiFi desconocidas siempre entraña riesgos.

Riesgos

Cuando nos conectamos a una red WiFi pública desconocemos quién es el administrador o qué medidas de seguridad utiliza para impedir acciones malintencionadas de otros usuarios conectados.

- **Robo de datos transmitidos.** Si la conexión la realizamos sin contraseña, lo que conocemos como red "abierta", los datos que transmitimos pueden ser leídos por cualquiera, tanto el administrador como otros usuarios conectados a la red. La información está expuesta a cualquiera que sepa cómo leerla, y para ello no es necesario tener unos conocimientos técnicos muy elevados.

  Si el sistema nos pide una contraseña y aparece un candado, como "red protegida", la información se transmite de forma cifrada. No obstante, esto está condicionado por el sistema de seguridad utilizado y la contraseña escogida. De menor a mayor seguridad, los sistemas son WEP, WPA y WPA2.
  Nunca debemos conectarnos a una red WEP ya que se ha demostrado que es vulnerable y que su seguridad equivale a una red abierta (sin contraseña).

- **Robo de datos almacenados en nuestro equipo.** Al formar parte de una red pública en la que existen otros usuarios conectados, nuestro dispositivo está expuesto y visible a los demás usuarios presentes en la misma.

  Por tanto somos susceptibles de recibir cualquier tipo de ataque desde uno de estos equipos conectados.

- **Infección de los dispositivos.** Al conectarnos a una WiFi ajena, un usuario malintencionado conectado a la misma red podría tratar de infectar nuestro equipo con algún tipo de virus.

  Es importante mantener siempre nuestro equipo actualizado con las últimas actualizaciones de seguridad para el sistema operativo y para las aplicaciones que tengamos instaladas.

- **Equipos intermediarios malintencionados.** Un usuario malintencionado conectado a la red podría configurar su equipo para hacer de intermediario de la comunicación entre nosotros y el servicio (por ejemplo, Facebook) modificando o eliminando la información intercambiada, que pasaría a través del ciberdelincuente.

- **El hacker "inocente".** En un momento dado,podemos sentir la tentación de conectarnos a una red ajena abierta o protegida utilizando herramientas de*hacking* WiFi. Sin embargo, esta práctica constituye un uso ilícito de servicios de terceros que puede tener consecuencias legales. Además, puede darse el caso de que esa red WiFi no presente

contraseña o sea especialmente fácil de hackear precisamente para atraer víctimas a ella y así robar los datos al pícaro usuario.

Recomendaciones de seguridad

Nunca debemos utilizar redes WiFi no confiables para acceder a servicios donde se intercambie información sensible: información bancaria, recursos corporativos, correo electrónico o acceso a las redes sociales.

Debemos evitar el uso de cualquier servicio en el que la información transferida tenga un componente importante de privacidad.

Nunca intercambiar información privada en redes no confiables.

Aunque podemos utilizar las redes públicas para otras acciones, como leer noticias en periódicos online o mirar la previsión del tiempo, no olvidemos que la mayor parte de los dispositivos mantienen un proceso de sincronización continua, por lo que el riesgo continúa existiendo.

Para protegernos de estos riesgos en redes donde los demás usuarios son desconocidos, contamos con una serie de medidas de seguridad que debemos aplicar:

- **Cortafuegos**. Es muy importante tener instalado y habilitado un cortafuegos que no permita las conexiones entrantes a nuestro equipo por parte de otros usuarios de la red. Muchos sistemas operativos actuales permiten escoger el modo de funcionamiento del cortafuegos cada vez que nos conectamos a una nueva red WiFi.
- En Windows, en “Centro de redes y recursos compartidos” encontramos dos configuraciones. ‘Pública’ es la que debemos seleccionar en las redes ajenas, y ‘Privada’ aquella a utilizar en redes de total confianza, como la de nuestra casa o la del trabajo.

- **Sistema antivirus**. Algunas aplicaciones antivirus pueden no solo identificar y detener software malintencionado destinado a nuestro equipo, sino también detectar y bloquear intentos de ataque a nuestro terminal.

- **Parches de seguridad**. Las aplicaciones y los servicios de nuestros dispositivos pueden contener fallos de seguridad que un atacante utilizará para ganar acceso a nuestro equipo.

  Las actualizaciones facilitadas periódicamente por los fabricantes de software deben ser instaladas en cuanto estén disponibles, preferiblemente de manera automática.

- **Desactivar la sincronización**. Muchos de nuestros dispositivos realizan tareas en segundo plano sin la participación directa del usuario: sincronizaciones de agendas, calendario, descarga de correo electrónico, realización automática de copias de seguridad.

  Se recomienda deshabilitar estos servicios cuando nos encontremos conectados a una red no segura. Ésta opción de habilitar o deshabilitar la sincronización en segundo plano

la encontraremos generalmente en los ajustes generales de nuestro dispositivo copias de seguridad.

- **Desactivar el sistema WiFi**. Cuando nos encontremos fuera del alcance de nuestras redes WiFi de confianza debemos deshabilitar la opción de conectarse a este tipo de redes. Se aconseja porque un atacante puede suplantar una red WiFi de nuestra lista de favoritos, forzándonos a que nos conectemos a ella de forma automática y transparente para nosotros.

- **Limpiar la lista de puntos de acceso memorizados**. Conviene revisar la lista de puntos de acceso memorizados para eliminar aquellos esporádicos y dejar únicamente los realmente confiables.

  La mayoría de nuestros dispositivos almacenan un listado de las redes a las cuales nos hemos conectado previamente, almacenando incluso las credenciales de acceso. Cada cierto intervalo de tiempo nuestra WiFi intenta conectarse de forma automática a cada una de las redes almacenadas, y es posible que nos encontremos formando parte de una red inalámbrica involuntariamente.

  Esto es debido a que para realizar su asociación con el punto de acceso tan solo se comprueba el nombre de la red (SSID) y el sistema de seguridad. Por ejemplo, si en el aeropuerto de Bilbao nos conectamos a una red WiFi abierta llamada “Aeropuerto” y en el terminal de pasajeros de Valencia existe una red abierta con el mismo nombre, nos veremos formando parte de esa red de forma automática sin desearlo.

Consejos finales

Las conexiones WiFi son una importante tecnología hoy en día, sin embargo, hay ciertas recomendaciones que debemos recordar:

- Las redes públicas pueden ponernos en peligro. Tanto el administrador como alguno de los usuarios conectados pueden utilizar técnicas para robarnos información.
- Si vamos a conectarnos, es preferible **acceder a una red con seguridad WPA o WPA2.** Las redes abiertas y con seguridad WEP son totalmente inseguras.
- Si vamos a usar una red pública, **deshabilitar cualquier proceso de sincronización de nuestro equipo**.
- Tras la conexión, **eliminar los datos de la red memorizados por nuestro equipo**.
- **Mantener siempre el equipo actualizado, con el antivirus instalado correctamente** y si es posible, hacer uso de un cortafuegos.
- **No iniciar sesión (usuario/contraseña) en ningún servicio** mientras estemos conectados a una red pública.
- **No realizar trámites a través de estas redes**: compras online, bancarios, etc.
- **Confirmar que se visitan sitios que comiencen por HTTPS** para que la información viaje cifrada y no puedan interceptar la que intercambiamos.