

INTERNET PÚBLICO (WIFI): CONSEJOS DE SEGURIDAD

Autor: David Hobson
MD de Sistema de Seguridad Global (GSS)
Boletín Commercial Crime Internacional
ed. Andy Holder, February 2009
volume 26, No 8, pag 10-11.

Los accesos a Internet a través de un servidor público están creciendo y continuarán haciéndolo a medida que más y más puntos de acceso estén disponibles. Encontramos que McDonalds ofrece acceso gratuito a Internet e incluso Boris Johnson propone que Londres se convierta en una ciudad WiFi, con conexión a Internet WiFi gratuita. ¡Siguiendo los pasos de Norwich!

Esta libertad de banda ancha viene con un elemento de riesgo una vez que se asocian a un punto de acceso que está en la misma red que conecta a los demás, es decir, al enchufar a todos en un sólo segmento de red. Un simple descubrimiento de red mostrará quién más está conectado... y sin escrúpulos, desde allí, un usuario puede intentar acceder a su máquina. Un troyano automáticamente puede ser escaneado en el fondo y tratar de infectar a otras máquinas. Además existe la posibilidad de ataque directo y los datos probablemente van a ser "texto no cifrado".

¿Cuáles son los problemas cuando se utilizan puntos de acceso público?

1.- Los datos de texto, por su propia naturaleza, en un punto de acceso no tendrán ningún cifrado de seguridad. Están allí para que tantas personas como sea posible puedan conectarse fácilmente; para ofrecer una seguridad compartida la clave es impracticable y el mayor número de personas tienen un menor valor de la clave. ¿Qué significa esto? Si envía un correo electrónico, alguien en la red será capaz de ver y leer los datos. Es un poco como una tarjeta postal que entrega una oficina de correos, todos en la oficina de correos pueden leerla, así que realmente no debe escribir nada confidencial sobre ella; al decir "hola, estoy pasando un maravilloso tiempo, ojala estuvieras aquí", no es precisamente un secreto. ¡Es posible que no quiera poner toda su información de tarjeta de crédito allí!

2.- La mayoría de tráfico Web es, por su propia naturaleza, el texto claro. La mayoría de los sitios Web cambiará el seguro cifrado HTTPS de tráfico, cuando se realicen las transacciones comerciales.

El correo Web normalmente es claro... ¿cómo puede saber si usted lo ha cambiado? ¡Busque el pequeño candado en su navegador!

3.- Si está utilizando el correo electrónico de la empresa, le recomendamos usar una VPN (red privada virtual) entre usted y la empresa del servidor de correo, esto debe ser proporcionado por la empresa. Normalmente esta es una superposición de seguridad en el tráfico. Esto normalmente trata de cifrar los datos y asegurarse de no eliminarlos al leerlo.

4.- Tu PC necesita tener instalado un firewall y debes mantenerlo encendido. Windows brinda un firewall básico. ¡Utilízelo! Esto detiene el acceso no autorizado a su PC.

5.- Muchas empresas agregan un firewall personal adicional. Lo más inteligente será el actual cambio de políticas basadas en la ubicación, lo cual controlara el flujo de información dentro y fuera de la PC de acuerdo con su política.

6.- Asegúrese de que el software de su anti virus este activado y ¡póngase a trabajar! Esto lo defenderá contra los virus desconocidos y el ataque de los troyanos.

7.- Desactivar la creación de redes ad-hoc WiFi cuenta con dos métodos de trabajo, ad-hoc e infraestructura. Infraestructura es cuando la PC se conecta a un punto de acceso y a continuación, en una red cableada. Ad-hoc es cuando dos computadoras se comunican entre sí directamente, sin un punto de acceso; usted realmente debería garantizar que no se puede conectar nadie directamente a su red, ¡a menos que exista una razón específica!

8.- Surf desde el hombro. Siempre debe ser consciente de lo que usted está viendo, procure no sentarse dando la espalda a una multitud o la ventana, brindando una invitación no deseada para ver su contraseña o leer sus documentos.

9.- Pensando acerca de la cantidad de tiempo que está conectado, como medida de precaución, prepare mensajes fuera de línea y conecte sólo para enviar y recibir. Esto reducirá la ventana de oportunidad para capturar los datos de alguien.

10.- Por último, cuando se accede a una red pública, debe ser consciente de un posible secuestro. Cuando se trata de una red falsa de acceso, ésta registrará todo el tráfico de su sistema, este tipo de ataque se utiliza principalmente en cafés Internet ya que el acceso está abierto. Siempre trate de asegurarse de que se está conectando a una auténtica red de acceso.

Para mayor información acerca de los temas abordados: www.gss.co.uk