Hoy en día no podemos imaginar un mundo sin acceso inalámbrico. La conectividad que ofrece no tiene precio - permite a los empleados trabajar desde cualquier lugar, aumentando la productividad, la movilidad y la comodidad. Con estas ventajas, sin embargo, viene un riesgo de seguridad, aunque se puede manejar fácilmente tomando las siguientes precauciones:

1. Cambiar contraseñas - Las contraseñas predeterminadas deben cambiarse para todos los equipos. Cree una contraseña segura con 8 o más caracteres utilizando números, letras mayúsculas y minúsculas, así como caracteres no alfanuméricos. Todo el hardware viene con contraseñas preestablecidas, pero muchas personas no se toman el tiempo para cambiarlas. Esto hace que sea fácil para los hackers entrar en los dispositivos corporativos como contraseñas predeterminadas se pueden encontrar fácilmente en Internet.

2. Elegir equipos de clase empresarial - El equipo hecho específicamente para uso comercial ofrece una mayor seguridad. Busque a una marca bien conocida y el uso de WPA2 para la seguridad inalámbrica.

3. Separar los datos corporativos de los dispositivos personales - Muchos enrutadores wifi permiten múltiples redes inalámbricas. La creación de redes separadas para datos corporativos, dispositivos personales e invitados hace más difícil el acceso o la corrupción de los equipos y datos de su empresa, por parte de usuarios no corporativos.

4. Mantenga todo el software actualizado - Los vendedores de hardware lanzan periódicamente actualizaciones de firmware que proporcionan soluciones de seguridad para sus dispositivos cuando se encuentra una falla o agujero de seguridad. Ignorar las actualizaciones de software ofrece a los intrusos una manera fácil de acceder a su equipo.

5. Asegure los dispositivos - Mantenga el equipo corporativo fuera del alcance de otros o bajo cerradura. Esto ayuda a evitar que el interruptor de encendido o el botón de reinicio sean golpeados por error. Colocar puntos de acceso a cierta altura no sólo mantiene el equipo fuera del alcance de los extraños, sino que también ayuda a distribuir mejor la señal.

6. Cree una política inalámbrica: establezca reglas básicas para el uso de su red inalámbrica corporativa. Nunca es demasiado pronto para crear e implementar una política de acceso inalámbrico para promover las mejores prácticas.

La seguridad inalámbrica es vital y sólo una herramienta para mantener su entorno corporativo seguro. Háganos saber que le gustaría aprender más sobre el uso de la tecnología para ayudar a que su negocio tenga éxito. Si tiene alguna pregunta o comentario, favor de comunicarse con nosotros en info@misits.com o en twitter @jmlucien.