



RECOMENDACIONES PARA PROTEGERSE DE HACKERS

Internet se ha convertido en una herramienta imprescindible en la operación de los negocios pequeños y medianos: la utilizamos para hacer transferencias electrónicas, revisar el estado del inventario, compartir datos confidenciales con nuestros clientes o proveedores, y manejar las campañas en redes sociales. Sin embargo, pocas veces tenemos en cuenta los peligros de que esa información confidencial pueda ser robada.

Los ataques cibernéticos son una realidad que no podemos ignorar, y cuyas modalidades cambian año con año. La buena noticia es que podemos prevenirlos y evitarlos con prácticas sencillas y las herramientas adecuadas.

Aquí te decimos cuáles son las siete más importantes, e incluimos algunas recomendaciones para que aumentes al máximo el nivel de seguridad de las comunicaciones y redes de contacto de tu negocio

- 1. Instalar un antivirus.**
 - a. Estos programas son básicos, y protegen tu equipo en tiempo real de código malicioso y cualquier pieza de software que pueda afectar el sistema operativo. Los mayores peligros de estos tipos de ataque son principalmente dos: eliminar archivos importantes y hacer que la computadora se vuelva más lenta.
Recomendación: cuando adquieras un anti-virus, asegúrate de que incluya una actualización automática.
- 2. Usa un firewall.**
 - a. Se trata de una capa adicional de protección, que crea una barrera entre la computadora y el exterior cada vez que te conectas a Internet. ¿Cómo? Bloqueando accesos no autorizados a un equipo y enviando avisos de alerta.
- 3. Suma un paquete anti-spyware.**
 - a. También conocidos como "troyanos", los ataques espía pueden recolectar en segundos datos confidenciales de la empresa, como passwords de acceso a cuentas bancarias. El problema es que son difíciles de detectar y de remover del equipo, por lo que es clave contar con un programa que bloquee estas amenazas en tiempo real.
 - b. Recomendación: la mayoría de los programas anti-virus más conocidos incluyen esta herramienta, así que asegúrate de hacer la compra correcta.
- 4. Mantén todos los programas actualizados.**
 - a. Los sistemas operativos, los softwares (como los de edición de texto o cálculo) y las aplicaciones tienen que estar al día. De lo contrario, estarás abriendo pequeñas ventanas para que los códigos maliciosos ingresen en el equipo sin ser detectados.
 - b. Los sistemas operativos, los softwares (como los de edición de texto o cálculo) y las aplicaciones tienen que estar al día. De lo contrario, estarás abriendo pequeñas ventanas para que los códigos maliciosos ingresen en el equipo sin ser detectados.
 - c. Recomendación: fija un día por semana en tu calendario para revisar los avisos automáticos de actualización de tu computadora.
- 5. No abras los mensajes spam.**
 - a. Esto incluye los links incluidos en el email y los archivos adjuntos. En los últimos años, los piratas cibernéticos se han sofisticado y han encontrado maneras más creativas de engañar a los usuarios, así que se muy cuidadoso a la hora de revisar esta carpeta.
 - b. Recomendación: ignora especialmente los correos sospechosos que lleguen de tu banco, tu contador u otro proveedor, un cliente o un amigo
- 6. Actualiza tus contraseñas.**
 - a. Es la forma más efectiva de prevenir la invasión de tu computadora y su sistema operativo. Ten en cuenta además que cuanto más seguro es un password, le harás más difícil el trabajo a los hackers. Usa claves complejas, que tengan al menos ocho caracteres y que no contengan datos obvios como tu fecha de nacimiento o el número de la calle de la empresa.
 - b. Recomendación: para registrar y poder recordar tus contraseñas en forma segura, usa apps como Sticky Password o Keeper Gestor.
- 7. Apaga la computadora.**
 - a. Si permanece prendida todo el tiempo, se volverá más visible para los hackers y aumentarán las posibilidades de un ataque. En cambio, cuando está apagada se corta la conexión a Internet y se cierra todo acceso a un código malicioso.
 - b. Recomendación: cierra el equipo al final de la jornada laboral, pero también durante esos períodos largos en los que estarás fuera de la oficina por presentaciones o comidas. Otro beneficio adicional es el ahorro de energía

Cualquier duda, comunicarse a Sierra.