HughesNet®

6 consejos para mantener seguro tu negocio en línea

Comprar desde la comodidad de una computadora, hacer operaciones bancarias, pedir el super, son sólo algunas de las cosas que diariamente hacemos como usuarios de **Internet** y es un pequeño ejemplo de cómo ha evolucionado el **comercio electrónico** y nuestra vida los últimos años.

Y sí, la **red** se convirtió en una herramienta esencial para el crecimiento y éxito de un negocio, sobre todo durante y a partir de la pandemia por COVID 19.

Sin embargo, como siempre hay peros en la vida, del otro lado de la moneda encontramos fenómenos como los **ataques cibernéticos,** que aumentan cada día, y que pueden comenzar como algo pequeño y evolucionar rápidamente en una seria amenaza para cualquier negocio que cuente con una estrategia digital.

En términos generales, y por citar un ejemplo, podrían obtener tu contraseña, entrar a uno de tus sistemas de pago o cobro, o a tu información financiera y hacer mal uso de ella.

Si estás usando una o varias herramientas en línea para tu negocio y lograr mayor cercanía con tus clientes, es importante que te asegures de que todas tus transacciones de comercio electrónico estén protegidas para evitar el acceso no autorizado o el uso fraudulento de los datos y recursos de tu empresa.

¿Cómo protejo mi negocio digital

1. Olvídate de la contraseña **"1234".** Utiliza contraseñas largas y complejas que incluyan letras, números y símbolos (pero que puedas recordar fácilmente). Además, evita usar la misma para múltiples cuentas y cámbialas regularmente.
2. Blinda tu computadora contra los virus. Existen programas antivirus que pueden proteger tu equipo. Asegúrate de mantenerlo actualizado y que un experto lo revise regularmente.
3. **¿Wi-Fi gratis?** Mejor no los uses. Comprueba que tu conexión a Internet sea segura al usar una conexión Wi-Fi, da preferencia a redes protegidas con contraseña y evita conectarte a redes públicas si vas a realizar operaciones.
4. Haz que internet sea seguro para tu negocio. Utiliza un navegador seguro que te proteja contra sitios web maliciosos y ataques de phishing* (abajo te explicamos de qué se trata). Algunos buenos ejemplos de esto son Chrome, Firefox, Opera, Tor Browser, Edge y Safari. Básicamente, los más comerciales.
5. Evita "hablar de más". No compartas información personal, por ejemplo, tu **número de seguridad social,** cuenta bancaria o contraseñas con desconocidos en línea (ni en ningún lado).
6. Los bancos cuidan tus datos. Usa una tarjeta de crédito con protección contra fraudes y notifica inmediatamente a tu banco si detectas alguna actividad sospechosa. No contestes mensajes, no des información por teléfono y comunícate directamente con tu banco.

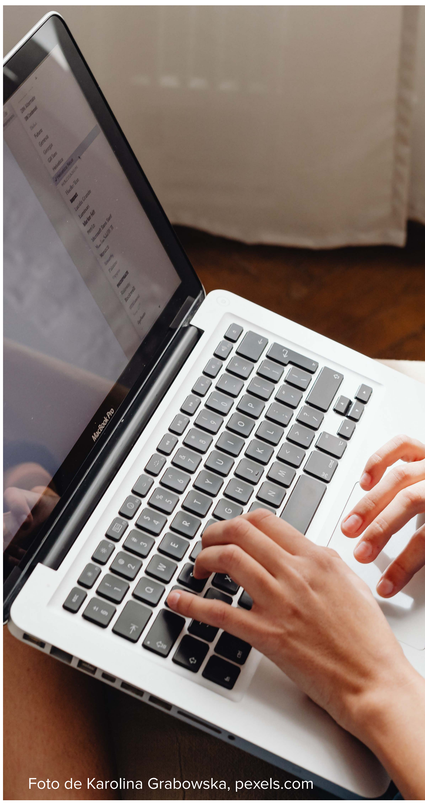

Foto de Karolina Grabowska, pexels.com

Cuida también los dispositivos

Asegúrate de que todos tu **dispositivos** conectados a la red estén protegidos. Utiliza contraseñas difíciles de adivinar y actualiza regularmente tus equipos y sus antivirus. Anticípate para que no te caiga un virus informático. Asesórate con alguien que sepa de computación y pide que instale lo necesario para proteger tus equipos de programas maliciosos y ataques en línea.

Actualmente, la seguridad de **Internet** es una gran preocupación para todo el mundo, no importa si son usuarios tradicionales o de **Internet satelital;** sin embargo, para quienes viven en áreas remotas, donde no hay acceso a las conexiones cableadas tradicionales, es vital.

*El phishing o suplantación de identidad, es una técnica fraudulenta utilizada para obtener información confidencial. Los atacantes crean correos electrónicos, mensajes de texto o sitios web falsos para engañar a las víctimas.