Publicado en Ciudad de México el 09/07/2018

# [¿Cómo evitar riesgos al reservar vacaciones en internet?](http://www.notasdeprensa.es)

## Avast, líder global en productos de seguridad digital para consumidores y empresas, comparte 5 consejos para evitar riesgos al hacer reservaciones en línea

 Las vacaciones de verano ya están aquí, y representan el momento ideal para salir con amigos o familiares. Aquellas personas que aun no han realizado sus reservaciones, probablemente recurrirán a Internet para encontrar la felicidad del verano. Sin embargo, el usuario de Internet con la mente en las vacaciones, se vuelve un objetivo ideal para los ciberdelincuentes. Internet brinda la comodidad de conseguir transporte o alojamiento para las vacaciones, así como la capacidad de comparar ofertas en el momento y lugar de preferencia. Sin embargo, los hackers están constantemente atentos a las malas prácticas y la falta de conciencia del consumidor con respecto a la ciberseguridad, cualquier vulnerabilidad se convierte en una oportunidad para ellos. Reservar es sinónimo de compartir información personal y sensible en línea, como los datos bancarios. Es por ello que Avast, líder global en productos de seguridad digital para consumidores y empresas, recomienda a los usuarios adoptar algunos hábitos simples en cuanto a la reservación en línea para no caer en trampas establecidas por los ciberdelincuentes durante este período específico del año. A continuación 5 consejos básicos: Tener cuidado con los correos electrónicos de phishing. Un hacker utiliza los principales eventos en el calendario y puede enviar falsas y atractivas ofertas a futuros visitantes. Esta es la razón por la que cualquier correo electrónico que no parezca legítimo debe verse con recelo. Si este es el caso, es mejor no hacer clic en los enlaces o archivos adjuntos, ya que si resultan ser maliciosos, un malware potencial se instalará en el dispositivo del usuario y permitirá a los hackers robar información como credenciales de inicio de sesión o números de tarjetas de crédito. De igual manera, los usuarios de Internet también pueden ser redirigidos a un sitio que imite un sitio oficial y ser invitados a `restablecer su contraseña´, o proporcionar datos personales para `corregir´ un error de cuenta falsa. En caso de duda, abrir una página nueva y ponerse en contacto con la compañía en cuestión para saber si el correo electrónico recibido realmente proviene de su servicio. Esto evitará el robo de datos, y si hay un intento real de fraude, el sitio web / compañía imitado puede tomar las medidas necesarias para advertir a todos sus contactos. Crear credenciales únicas. Cada cuenta en línea debe tener un nombre de usuario y contraseña únicos. Por lo tanto, si un cibercriminal hackea un sitio web, no podrá acceder a otras cuentas del usuario. Además, no hay ningún secreto, las mejores contraseñas se componen de una variedad de símbolos, es decir que deben incluir más de 8 caracteres en total y deben incluir letras mayúsculas, números y caracteres especiales. Frente a los múltiples sitios web y aplicaciones, la creación de contraseñas únicas puede ser muy restrictiva para el usuario, que tenderá a elegir la misma en todas las cuentas. Para ayudar a los usuarios, existen herramientas de administración de contraseñas que permiten obtener una contraseña infalible y generada automáticamente para todas sus cuentas en línea.​ Verificar la presencia de `https´ y el candado verde. En el momento del pago, si los sitios web no incluyen `https´ y el candado verde en la barra de direcciones, los consumidores no deben finalizar la compra. De hecho, eso significa que el sitio web no proporciona cifrado ni se beneficia de un certificado de autenticación emitido por una autoridad confiable. Significa que no protege proactivamente los datos confidenciales del usuario. Adoptar autenticación de 2-factores. Esta adopción permite configurar varios niveles de protección, lo que dificulta el acceso de una persona no autorizada a la información asegurada. Por ejemplo, el usuario recibirá un código único en su teléfono móvil con cada pago y lo completará en el sitio para poder finalizar la transacción. Esto significa que si un cibercriminal logra obtener la contraseña de un consumidor, no podrá ir más allá porque no tendrá el segundo factor requerido. Utilizar métodos de pago seguros. Idealmente, cualquier transacción financiera en línea se debe hacer utilizando una tarjeta de crédito con protección contra el fraude. Hoy en día, la mayoría de las tarjetas de crédito le permiten informar una compra fraudulenta dentro de los 30 días posteriores a su hallazgo en el extracto bancario. Alternativamente, es posible utilizar servicios de pago en línea como PayPal que evitan ingresar detalles bancarios. "Las fuentes y herramientas en línea para la planificación de viajes son infinitas, al igual que lo son las posibilidades de llevar a cabo un ataque. A pesar de que los usuarios de internet saben que la ciberseguridad es importante, continúan sufriendo el síndrome de and #39;solo les sucede a los demás and #39; y no toman las medidas necesarias. Es por ello que la conciencia continúa y la educación sobre las prácticas más simples es esencial. Al final, se convertirán en hábitos y permitirán organizar sus vacaciones tranquilamente, pero también para disfrutar de Internet de forma segura durante todo el año, más allá del período de verano". Visitar: www.avast.com

**Datos de contacto:**

Flor Carreno

Agencia de Relaciones Públicas

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/como-evitar-riesgos-al-reservar-vacaciones-en](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Viaje E-Commerce Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)