Publicado en América Latina el 22/06/2023

# [DigiCert brinda 5 consejos para que las vacaciones estén libres de piratas informáticos](http://www.notasdeprensa.es)

## Ante la temporada de vacaciones y verano de mitad de año, es primordial que los usuarios tomen las medidas necesarias para evitar ser victimas de estafas durante sus viajes. Tomar en cuenta recomendaciones básicas como proteger los dispositivos personales y no confiar en las redes abiertas pueden garantizar un viaje seguro y placentero

 Después de un largo período de pandemia, los operadores turísticos están ansiosos por mejorar los ingresos con la proximidad de la temporada alta de vacaciones y verano. Según la estimación del Consejo Mundial de Viajes y Turismo (WTTC) en su Informe Anual de Impacto Económico, este año la contribución del sector turismo al PIB de América Latina será de 319 mil 500 millones de dólares, 1,2% por encima de 2019. En 2022, el sector de viajes y turismo aportó el 7,6% al PIB de América Latina, equivalente a 302.600 millones de dólares, un crecimiento del 34% respecto al año anterior. Asimismo, para fines de 2023 se proyecta que los niveles de empleo en la región alcancen los 17,07 millones de puestos de trabajo ocupados por el sector turístico, lo que también superaría en 0,1% la cifra de 2019. "Antes, cuando te ibas de vacaciones, solo te preocupaba cerrar con llave la puerta de tu casa. Pero ahora debes preocuparte por "bloquear" cualquier cosa que se conecte a Internet para que no roben datos personales", dijo Dean Coclin, director sénior de desarrollo empresarial de Digicert. "Lo último que necesitas es enterarse de una violación de datos. Es primordial desde proteger los dispositivos personales hasta evitar las amenazas cibernéticas mientras se viaja, hay muchos pasos que se pueden tomar para garantizar un viaje seguro y placentero", agregó el ejecutivo. Estos son algunos consejos de DigiCert para viajar de forma segura durante las próximas vacaciones y mantener los datos del mundo real a salvo de los ciberdelincuentes, tanto en casa como en el extranjero. Entonces, ya sea que el usuario viaje regularmente por negocios o esté buscando unas vacaciones de verano, aquí 5 consejos para viajar de manera segura: 1. No dejarse engañar por sitios web falsos y ofertas tentadoras que son demasiado buenas para ser verdadAl reservar viajes y alojamiento en línea, es importante evitar sitios web fraudulentos y estafas de phishing. ¿Qué pueden hacer los usuarios para reconocer los sitios fraudulentos? Tres palabras: examinar, examinar y examinar. También es importante tener cuidado al navegar, ya sea en sitios web, redes sociales o aplicaciones. Se recomienda no abrir ni descargar archivos de sitios web desconocidos o sospechosos ni hacer clic en enlaces enviados en redes sociales o aplicaciones de mensajería, debido al aumento de intentos de phishing. El phishing es una de las prácticas más comunes en la ingeniería social, con un costo estimado de $ 2 mil millones al año. Este tipo de ataque ha ganado aún más popularidad desde la pandemia. En un ataque de phishing, un usuario recibe un correo electrónico que parece provenir de una fuente confiable, pero en realidad es fraudulento y se usa para robar información personal. Tratar todos los correos electrónicos de ofertas demasiado buenas para ser verdad con sospecha. Evitar hacer clic en enlaces de correo electrónico sospechosos o descargar documentos desconocidos, y solo usar fuentes confiables para conocer las oportunidades de venta y compra. Y nunca revelar información personal o financiera por correo electrónico ni responder a solicitudes de esa información. 2. No olvidar dejar los dispositivos muy bien protegidosAntes de salir a la carretera, hay algunas medidas de seguridad importantes que los usuarios deben tomar para asegurar cualquier dispositivo que se lleve durante el viaje, como computadoras portátiles, teléfonos y tabletas. Es clave comenzar usando contraseñas seguras y autenticación de dos factores. Un administrador de contraseñas también puede ayudar a establecer y administrar contraseñas seguras, y puede informar qué tan seguras son las contraseñas, si se está utilizando duplicados y si las contraseñas han estado involucradas en una violación. "También considere usar una red privada virtual (VPN) cuando acceda a redes Wi-Fi públicas, ya que las VPN encriptan sus datos y algunas de ellas verifican el certificado digital, que redirigirá a un sitio web real si el que accedió es falso. Las VPN son también es útil cuando se viaja, ya que acceder a sitios web y aplicaciones prohibidos en algunos países requerirá una VPN. Finalmente, mantener el software y los sistemas operativos actualizados puede ayudar a evitar vulnerabilidades que pueden ser aprovechadas por los ciberdelincuentes ", explicó Dean Coclin. 3. Sí, la casa inteligente también necesita protecciónMatter es el primer intento de reunir a los nombres más importantes en el hogar inteligente para desarrollar un estándar de la industria para la interoperabilidad segura y confiable de los dispositivos conectados. Con Matter, los consumidores ahora pueden controlar todos los dispositivos de confianza en el hogar, independientemente de la marca, mientras eligen los productos individuales de su elección. Además de eso, Matter aumenta la seguridad del hogar inteligente porque los fabricantes que venden dispositivos confiables de Matter deben cumplir con ciertos requisitos, incluida la recepción de certificados de atestación de dispositivos. "Entonces, si el usuario está fuera de casa, puede administrar todos sus dispositivos domésticos inteligentes confiables de Matter a través de Siri, o a través de las aplicaciones Alexa o Google Home, y no solo sus dispositivos Apple, Amazon o Google. Hay cientos de empresas involucradas en Matter y DigiCert ha jugado un papel clave en el desarrollo de los aspectos relacionados con la seguridad del estándar, patrocinado por Connectivity Standards Alliance (CSA)", dijo Dean Coclin. No importa en qué lugar del mundo se encuentre el usuario, puede controlar la iluminación, las cerraduras de las puertas, la calefacción y el aire acondicionado, la seguridad del hogar, los parlantes inteligentes y más, todo desde el controlador que se elija, y sin aplicaciones separadas para todo. Al asegurar los dispositivos domésticos inteligentes con Matter, los propietarios pueden proteger sus hogares de las amenazas cibernéticas mientras están fuera y ser más inteligentes que sus hogares inteligentes. 4. Vigilar los documentosDurante el viaje es importante proteger las pertenencias físicas como pasaportes, billeteras y teléfonos. Así mismo se debe proteger la computadora portátil de trabajo y cualquier información confidencial para evitar el robo de datos o identidad. Cuando los usuarios se conectan a Wi-Fi en hoteles, aeropuertos, cafés y más, puede ser vulnerable a los ataques, por lo tanto es mejor evitar usar el wifi del hotel cuando se acceda a sitios que soliciten  datos personales, especialmente del  banco. Se debe tener cuidado al conectarse a redes Wi-Fi públicas y no confiar en las redes abiertas. El uso de una VPN a redes Wi-Fi públicas puede encriptar el tráfico de Internet y evitar que los ciberdelincuentes roben información personal.  5. Las medidas de protección continúan después de regresar a casaAl regresar a casa de un viaje, es primordial controlar las cuentas personales y los informes de crédito en busca de actividades sospechosas o cargos no autorizados. Proteger la información personal cambiando las contraseñas y monitoreando los extractos de las tarjetas de crédito. Finalmente, reportar cualquier actividad sospechosa o cargos no autorizados a las instituciones financieras y agencias de informes crediticios. "En conclusión, si bien viajar puede ser emocionante y rejuvenecedor, lo último que necesita en sus vacaciones es enterarse de que un ciberdelincuente ha robado su identidad o sus datos confidenciales. Pero hay pasos que puede tomar para minimizar el riesgo de que sus datos sean robados", concluyó Dean.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-brinda-5-consejos-para-que-las](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Software Ciberseguridad



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