[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en México el 23/06/2022

# [Viajes de mitad de año: cuidados esenciales para no caer en manos de estafadores digitales](http://www.notasdeprensa.es)

## Ante la alta demanda de viajes, los estafadores aprovechan el momento para aplicar estafas de robo de datos y pérdida de dinero. Es por ello que DigiCert ha enumerado las principales precauciones que se deben tomar en esta época del año, para garantizar la seguridad digital

Después de un período turbulento, los calendarios escolares volvieron a la normalidad y también las vacaciones escolares de mitad de año. Después de casi dos años de restricciones, las familias están emocionadas de viajar. Para América Latina, los destinos de playa son los que lideran la demanda en viajes. Según reportes de plataformas de viajes como Booking y Kayak; México lidera la recepción de turismo en América Latina. República Dominicana, Panamá, Chile y Colombia; son los otros espacios deseados por los viajeros. En Brasil, el estudio "Pulse Expectation 2022", realizado por Hibou con más de 1.800 personas, muestra que cerca del 43% de los encuestados tiene la intención de viajar en 2022. Los destinos más populares son las playas desiertas (51%) seguidos de las haciendas (32%) y los campo/hoteles (31%). Precisamente porque hay tanta gente buscando información sobre viajes y desplazamientos por diferentes partes del mundo, los estafadores aprovechan el momento para aplicar estafas de robo de datos y pérdida de dinero. Para que los usuarios no caigan en una de estas trampas, DigiCert ha enumerado las principales precauciones que se deben tomar en esta época del año para garantizar la seguridad digital. 1. Buscar la confianza Es primordial comenzar en un sitio web confiable, en lugar de comprar cualquier boleto o tarifa de hotel con un motor de búsqueda. Los resultados de la búsqueda pueden manipularse para desviarlo, especialmente cuando se pasan por alto las primeras páginas de enlaces. ¿Qué pueden hacer los usuarios para reconocer sitios web fraudulentos? Tres palabras: examinar, examinar y examinar. Si bien en el pasado estaba bien buscar el candado, ahora se debe examinar el candado. Pasar el cursor sobre el candado para ver qué CA (autoridad de Certificación) ha emitido el certificado. “Si es un certificado de DigiCert, los usuarios pueden estar seguros de que el sitio web ha sido verificado, de acuerdo con los estándares de la industria y que, en el caso de un certificado OV o EV, la identidad del propietario del sitio web ha sido investigada para mayor protección”, afirma Dean Coclin, Director de Desarrollo de Negocios Sr. en DigiCert. Revisar de cerca la barra de direcciones y leer la dirección cuidadosamente. Hacer clic en el candado para revelar información adicional sobre el sitio. Si se está utilizando un certificado EV, el nombre de la empresa se identificará inmediatamente después de hacer clic en el candado. 2. Atención al navegar 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 sospechosos o desconocidos, ni hacer clic en ningún enlace enviado en redes sociales o aplicaciones de mensajería. Otro consejo es mantener el dispositivo con un antivirus actualizado. Con la llegada de una web que está encriptada en más del 90 % y con navegadores que muestran un candado sólido para todos los sitios https, independientemente del tipo de certificado, es una falacia simplemente "buscar el candado", ya que esto es insuficiente para proteger a los usuarios de sitios fraudulentos. Los usuarios deben ser diligentes en la búsqueda de pistas sobre la identidad del sitio. Con los certificados EV, debe hacer clic en el candado para ver el nombre legal de la empresa. Esto proporciona una excelente visibilidad de que el sitio ha sido autenticado. "Los certificados OV y EV requieren un poco de esfuerzo para obtenerlos. Primero, la entidad solicitante debe ser una organización válida y la CA debe consultar los registros públicos para autenticarlos. Debido a que esto implica trabajo manual, hay un costo asociado con la obtención del certificado. Estos normalmente no son obstáculos para las organizaciones legítimas, pero para los ciberdelincuentes suponen una fricción importante, que puede evitarse obteniendo un certificado DV. Por lo tanto, DV se ha convertido en el certificado elegido por los piratas informáticos y los delincuentes”, agrega Dean Coclin. 3. Cuidado con los correos electrónicos Probablemente los usuarios hayan escuchado o recibido correos electrónicos con un logotipo muy similar al de una famosa aerolínea, o cadena hotelera con un archivo adjunto o un enlace a un descuento tentador. Cuando se descarga el archivo, se solicita al usuario una instalación que hace que la computadora se infecte con malware. Estos son solo algunos trucos que los piratas informáticos están usando para ingresar a las computadoras en todo el mundo. Una de las prácticas más frecuentes en ingeniería social es el phishing. Este tipo de ataque ganó más popularidad durante la pandemia de coronavirus. El usuario recibe un correo electrónico que parece provenir de fuentes confiables, pero en realidad es información fraudulenta utilizada para influir o robar información personal. La guía principal en estos casos es: tratar todos los correos electrónicos con ofertas demasiado buenas para ser verdad con sospecha. Evite hacer clic en enlaces de correo electrónico sospechosos o descargar documentos desconocidos y use solo fuentes confiables para informarse sobre oportunidades de ventas y compras. Y nunca revele información personal o financiera por correo electrónico, ni responda a solicitudes de esa información. Es importante eliminar siempre los mensajes sospechosos antes de abrirlos si el remitente es desconocido. En lugar de hacer clic en el enlace de un correo electrónico, hay que abrir una nueva página del navegador e ingresar la dirección/localizador uniforme de recursos (URL) del sitio que va a visitar. Mientras está conectado, debe comparar el nombre del sitio web en la barra de direcciones en la que normalmente confía y buscar anomalías. 4. Consultar extractos bancarios con frecuencia Conectarse en línea regularmente durante el día libre y ver los estados de cuenta electrónicos de la tarjeta de crédito, tarjeta de débito y cuentas corrientes. Asegurarse de no ver ningún cargo fraudulento, incluso si se origina en sitios como PayPal. 5. Usar la tecnología para protección Los piratas informáticos están evolucionando sus niveles de piratería, sofisticación de estafa y la están utilizando contra los usuarios. Para evitar ataques, actualice siempre el software y el navegador con las últimas versiones de Microsoft Edge, Mozilla Firefox y navegadores de otros proveedores que vienen equipados con filtros antiphishing. Las tecnologías existentes como PKI, que proporciona cifrado y garantía de identidad criptográfica en cada flujo de datos y verifica a todos los usuarios de la red, pueden desempeñar un papel clave en la protección de hogares, empresas y redes conectadas. Los ataques de correo electrónico son comunes para el phishing y la ingeniería social, y las empresas también pueden ayudar a proteger a los usuarios y otras personas que confían en sus sistemas de correo electrónico mediante el uso de certificados digitales para garantizar la identidad, la autenticación y el cifrado del cliente. Una plataforma PKI sólida puede ayudar a garantizar que los correos electrónicos estén firmados por partes autorizadas dentro de la organización, ya que muchos ataques se basan en la ingeniería social para falsificar un correo electrónico de una fuente supuestamente confiable para ganar la confianza del destinatario y luego robar su identidad o credenciales.

**Datos de contacto:**

DigiCert PR Latam

573125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/viajes-de-mitad-de-ano-cuidados-esenciales\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad Dispositivos móviles

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

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