Publicado en Latinoamérica el 27/12/2022

# [8 Tips para una Navidad con compras seguras en línea](http://www.notasdeprensa.es)

## DigiCert brinda algunos consejos a los usuarios para no caer en estafas en época decembrina

 Diciembre es la época más esperada del año, al menos para aquellos que no están siendo atacados por ciberdelincuentes. La Encuesta sobre el estado de la confianza digital de DigiCert 2022 afirma que más de la mitad (57 %) de los consumidores encuestados han sufrido ataques de ciberseguridad. Los principales ataques incluyen piratería de cuentas, exposición de contraseñas y robo de cuentas bancarias o de crédito. Menos de la mitad de los consumidores encuestados dijeron que su confianza digital en las organizaciones con las que tratan es mayor que en el pasado, y el 54 % dice que hay margen de mejora. A pesar del temible escenario, existen formas sencillas de asegurar las compras en línea para mantenerse seguro. DigiCert brinda a los usuarios algunos consejos para realizar compras seguras en línea esta Navidad: 1. No hacer clic en enlaces desconocidosLa forma más común en que los ciberdelincuentes pueden estafar en esta temporada navideña, es mediante el envío de correos electrónicos de phishing con enlaces que pretenden llevar a los usuarios a un lugar ilícito. Si bien puede ser tentador ver la interesante oferta que han enviado, es mejor prevenir que curar. "Los usuarios deben copiar manualmente el enlace e inspeccionarse antes de pegarlo en un navegador web, para que pueda ver si el enlace lo dirige al sitio del minorista. El mismo consejo se aplica para hacer clic en los enlaces a través de los resultados de búsqueda. Asegúrese de saber a dónde lo lleva el enlace antes de hacer clic, o incluso mejor, escriba la URL del sitio web del minorista en la barra de direcciones siempre que sea posible" afirma Dean Coclin, director Senior de desarrollo comercial en DigiCert. 2. Comprobar que el sitio sea seguroProbablemente los usuarios hayan oído hablar de buscar el candado para confirmar que un sitio web es seguro. Sin embargo, cada navegador muestra estos sitios autorizados de manera diferente, lo que puede generar cierta confusión. Las URL de los sitios que comienzan con HTTPS:// acompañados del icono del candado tienen TLS/SSL (seguridad de la capa de transporte/capa de sockets seguros), y los consumidores deben hacer clic en el candado para revisar la información del certificado y confirmar que el sitio usa el cifrado TLS antes de ingresar la Información de tarjeta de crédito.  Asimismo, revisar si el sitio web parece ser legítimo. "Si ve una página de términos y condiciones, reseñas, buena ortografía y gramática, un sello de sitio seguro y seguidores en las redes sociales, todos esos son indicadores de que se puede confiar en el sitio web" agrega Coclin. 3. No utilizar Wi-Fi públicoEl Wi-Fi público gratuito es común y, a menudo, ni siquiera requiere una contraseña, lo que facilita que los ciberdelincuentes accedan a los archivos e información personal de los usuarios. Muchas de estas conexiones están desprotegidas, por lo que es mejor usar una conexión Wi-Fi personal, un punto de acceso personal o una red privada virtual (VPN) al acceder a cualquier tipo de información privada en línea, como una cuenta bancaria o ingresar información de tarjeta de crédito para compras. 4. No compartir demasiada informaciónCuando llegue el momento de registrarse para obtener un descuento o iniciar sesión para comprar, se le pedirá al usuario información estándar. Los minoristas nunca necesitarán información personal, como un número de seguro social o fecha de nacimiento, para completar una compra, así que es importante proporcionar la menor información necesaria. "Si un contacto se comunica con con respecto a una compra por mensaje de texto o correo electrónico, no haga clic en el enlace ni se apresure a proporcionar información adicional hasta que pueda confirmar que la persona o empresa realmente es quien dice ser" agrega Dean Coclin. 5. Actualizar el softwareLos ciberdelincuentes pueden explotar las debilidades cuando no se mantiene el software actualizado. Por lo tanto, es primordial que el navegador esté completamente actualizado, además de evitar software o complementos sospechosos. También mantener las computadoras, teléfonos y tabletas actualizados. Actualizar regularmente los programas antivirus para protegerse contra elementos como el malware troyano. 6. Administrar y proteger las contraseñasMuchos minoristas requieren crear una cuenta para completar las compras en línea.  Si el pago de invitados es una opción, es óptimo usar esa opción. Para cuentas con contraseñas, se deben crear contraseñas seguras, utilizar la autenticación de múltiples factores cuando esté disponible y no repetir las contraseñas. Un administrador de contraseñas que cifra las contraseñas es una excelente opción para ayudar a guardar las contraseñas que podría olvidar sin comprometer la seguridad. 7. Estar atentos a las actualizaciones de pedidosMientras el usuario espera su nuevo dispositivo doméstico inteligente en el correo, se debe ser diligente: verificar las actualizaciones de seguimiento y asegurarse de que el paquete realmente llegue. Guardar los detalles de confirmación del pedido y estar listo para contactar al comerciante si es necesario. Además, vigilar los estados de cuenta bancarios en busca de cargos fraudulentos para asegurarse de que no facturen algo que el usuario no ha comprado. 8. Usar el sentido comúnSi un sitio parece incompleto, o no se puede encontrar ninguna otra evidencia de su presencia en línea, no se debe confiar en él. Estos consejos pueden evitar ser víctima de una estafa cibernética, pero en última instancia, se necesita sentido común, vigilancia y alfabetización digital para salvarse de los peligros en línea. "Si bien puede parecer arriesgado comprar en línea en esta temporada navideña, recuerde que estos simples pasos lo ayudarán a proteger sus datos personales. No hay motivo para no disfrutar de la comodidad y la accesibilidad de realizar compras en línea: ¡alegría para el mundo digital" concluye Dean Coclin.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/8-tips-para-una-navidad-con-compras-seguras-en](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad Dispositivos móviles



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