Publicado en Ciudad de México el 16/08/2017

#  [Ocho consejos para proteger tus compras online de regreso a clases](http://www.notasdeprensa.es)

## Esta temporada será especialmente atractiva para los ciberdelincuentes: en este momento, mediante el phishing por correo electrónico (que contiene adjuntos o direcciones de internet infectados con malware), por el que se busca engañar a los usuarios, capturar su información bancaria y así robar su dinero, advierte Jan Zika, director de Web Threat de Avast

 Las compras online se van ganando, cada vez más, la confianza de los mexicanos. De acuerdo con el INEGI se ha visto un incremento de 9.7% en 2015 a 15.9% en 2016. Mientras se descubre  como se comportan las compras online este 2017, Avast, el líder global en productos de seguridad digital para usuarios y empresas, comparte 8 consejos para proteger las compras online, sobre todo ahora que el regreso a clases está próximo. `Sucede todo el tiempo, pero se intensifica en las fechas en que los consumidores están más motivados y, en general, más ansiosos o apurados para hacer sus compras, como por ejemplo compras de regreso a clases, Buen Fin y Navidad´, agrega Zika. El experto de Avast explica que las tácticas empleadas por los ciberdelincuentes para atraer y engañar a sus víctimas suelen ser las mismas: ofrecen premios, rebajas y promociones, que les llegan por correo electrónico o por mensaje en las redes sociales. Otra variante es el envío de enlaces o adjuntos que muestran anuncios de tiendas reconocidas, en los que se indica que el usuario puede pasar a buscar alguna mercadería valiosa o a recoger cierta cantidad de dinero en efectivo. Sin embargo, esto es apenas el señuelo para distraer al usuario: al abrir el documento o el enlace, se infecta con malware que puede recolectar información personal o las credenciales de acceso bancario. Estos señuelos también pueden llegarle al consumidor por medio de publicidades con enlaces que buscan llevarlo a sitios peligrosos en la web. Para mantener a los ciberdelincuentes a distancia, Jan Zika brinda estos ocho consejos: 1) Utilice una tarjeta de crédito. Las tarjetas de crédito no solo le ayudarán a llevar un registro de sus compras; lo más importante es que podrá comunicarse con la empresa emisora si nota que hay gastos sospechosos. La mayoría de las empresas de tarjetas de crédito se pondrán en contacto con el comercio y anularán esos gastos. 2) Active una autenticación de dos factores donde sea posible. Esta forma de autenticación requiere que ingrese un segundo código junto con el nombre de usuario y la contraseña cuando inicia la sesión en alguna de sus cuentas. Por lo general, este código se envía al teléfono o correo electrónico asociado a la cuenta, o puede generarse en un dispositivo móvil por medio de una aplicación, tal como la app Authenticator de Google. Si usted no es quien está intentando ingresar a su cuenta, la autenticación de dos factores puede servir como sistema de alerta cuando alguien más trate de acceder a alguna de sus cuentas e ingresa un código erróneo. 3) Busque el candado verde. Cerciórese de que haya un candado verde, símbolo del HTTPS, junto a la dirección del sitio web en la barra de direcciones. HTTPS es un protocolo que encripta sus datos cuando se envían a través de la red. Si está en una página de pago y no ve el candado HTTPS, ¡no ingrese sus datos personales ni sus datos bancarios! 4) Actualice el software. Asegúrese de que todo el software en sus dispositivos esté actualizado. Los ciberdelincuentes aprovechan las vulnerabilidades que encuentran en el software desactualizado y, al hacerlo, pueden infectar el dispositivo para luego robar su información financiera mientras usted hace compras por internet. 5) No se aparte de los sitios conocidos y confiables. Trate de hacer sus compras en línea en comercios conocidos. Hay muchas maneras en las que los ciberdelincuentes buscan atraer a los clientes para que compren en sitios web falsos. Algunos tratan de desviar la conversación de sitios de comercio electrónico como Amazon, por ejemplo, de modo que Amazon ya no sea responsable y puedan robarle sin sufrir las consecuencias. Algunas tiendas falsas tratan de captar clientes ofreciéndoles productos a precios ridículamente bajos y tienen comentarios demasiado positivos en la página. Si una oferta o un sitio desconocido parece demasiado bueno para ser cierto, tal vez deba pensar dos veces antes de llenar el carro de compras y vaciar su billetera. 6) Escriba las URL usted mismo. Muchos correos con phishing incluyen enlaces a sitios maliciosos que se ven igual que los verdaderos y es difícil reconocer que son falsos. Siempre es más seguro escribir la URL directamente en el navegador y, como regla general, evitar pulsar los enlaces o abrir archivos adjuntos que se incluyen en correos electrónicos promocionales. 7) Instale un antivirus en todos sus dispositivos. Un antivirus, como Avast, podrá detectar ataques de phishing y bloquear sitios maliciosos en su PC y dispositivos móviles, antes de que causen daño. 8) Use un navegador seguro, como Avast SafeZone. El navegador Avast Safezone, incluido con el antivirus Avast, trae un "Modo de banca" que aísla sitios bancarios y de pagos en un espacio protegido. www.avast.com es el líder global en productos de seguridad digital, protege a más de 400 millones de personas online. Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y del escenario de amenazas de Internet de las Cosas en constante evolución. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas en el mundo, utilizando tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para Móvil, PC o Mac están mejor clasificados y certificados por V-100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de las principales firmas globales de capital privado CVC Capital Partners y Summit Partners. Más información en  http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017\_Nal.pdf y http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016\_0.pdf

**Datos de contacto:**

Flor Carreño

Marketing Q S

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/ocho-consejos-para-proteger-tus-compras-online](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Sociedad E-Commerce Ciberseguridad



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