S21sec: malware, phishing y redes públicas, entre los grandes riesgos del ecommerce

Los expertos de S21sec, empresa especializada en servicios y tecnología de ciberseguridad, advierten que, ante el actual panorama de ciberamenazas crecientes y el gran movimiento en comercio electrónico que se espera para Navidad y Cyber Monday, los riesgos en internet se multiplican y los usuarios deben mantener la guardia más alta que nunca.

Alexis Alonso, responsable de medios de pago de S21sec, recuerda que "los usuarios están recibiendo en estas fechas ofertas online de todo tipo y el nivel de información al que están expuestos es sencillamente abrumador. Esto **facilita el trabajo al cibercriminal, que usará la vulnerabilidad de los compradores para ofrecer ofertas no legítimas que simulen las que sí lo son**, apoyarse en webs fraudulentas y perpetrar ciberataques recabando los datos financieros del consumidor".

De hecho, según datos de la AMIPCI según el Estudio de Comercio Electrónico en México 2017 de la AMIPCI y ComScore, las compras en línea cerca de Navidad aumentan en 65%, y 28% en Cyber Monday. Con todo esto, los expertos de **S21sec** destacan las cinco principales ciberamenazas que en esta época podrán tener mayor incidencia:

-Ataques de **phishing**: Los usuarios sufrirán un **incremento exponencial de los mails y mensajes que reciben con ofertas de todo tipo**. Se recomienda que "lo mejor para aprovechar las ofertas de la época es acudir siempre a sitios oficiales de las tiendas digitales, y no a través de links que lleguen por correo electrónico".

-Páginas web fraudulentas: La realidad es que los mexicanos cada vez realizamos más compras a través de la web durante fechas como El B**uen Fin, Black Friday, Navidad y Cyber Monday** (los segmentos más destacados son ropa y accesorios, descargas digitales y boletos para eventos). "Si es un sitio web donde nunca hemos comprado anteriormente, nuestra recomendación es observar muy bien todos los elementos, sin pasar por alto ningún detalle: nombre de la URL, direcciones de contacto, sellos de confianza online, conexión segura materializada por un candado al lado del nombre de la URL, etc. Todo nos tiene que encajar, si no será mejor renunciar a realizar la compra online", destaca Alexis Alonso.

-Tecnologías inalámbricas de pago: Recuerda el informe que **cuando una WiFi es libre (sin**

contraseña), tendremos que evitar realizar cualquier tipo de compra o transacción bancaria, ya que podría haber equipos en modo escucha que intercepten las comunicaciones: podrían ver lo que estamos haciendo y robar nuestros datos y credenciales. En cuanto a la creciente tendencias del Internet de las Cosas, dice el informe que "las medidas de seguridad de todos estos elementos (ya sean smartphones, wearables, etc.) deben pasar siempre por la descarga y uso de aplicaciones oficiales desde un marketplace de confianza".

–**Malware móvil**: El celular se ha convertido en un elemento cada vez más importante a la hora de cerrar decisiones de compra y tendrá un papel fundamental durante la época que inicia con Cyber Monday. "Es esencial que los usuarios sepan que la forma más fácil de que entre un malware en nuestro sistema es precisamente mediante una descarga. Por tanto, la primera recomendación para los usuarios es no instalar aplicaciones ajenas a tiendas oficiales".

-Compartir dispositivos: Los expertos advierten que hay que extremar las precauciones a la hora de compartir dispositivos**, ya sea el smartphone, tablet, notebook, en una misma familia o incluso entre conocidos o amigos de nuestros hijos.** Es muy importante utilizar contraseñas seguras y no dejar que los menores jueguen con los dispositivos sin nuestra supervisión. Pueden conectarse a una WiFi sin nuestro conocimiento o descargar aplicaciones poco seguras o de contenido no legítimo.