Consejos para afrontar el CyberDay Chile de forma segura

Los próximos **30 y 31 de mayo** tendrá lugar en Chile el evento de compras online **CyberDay Chile**, que permite a los consumidores acceder a importantes descuentos en tiendas de comercio electrónico.

De cara a este año 2016 en la Cámara de Comercio de Santiago (CCS) apuntan que **tomarán parte 90 empresas** y se lograrán superar las cifras obtenidas el año pasado, cuando se ingresaron 83 millones de dólares en compras y se registraron 390 mil transacciones.

La gran cantidad de operaciones que se realizarán en esos días serán el **blanco perfecto** para que los cibercriminales aprovechen para **robar dinero a los internautas** que participen en las compras.

Roberto Martinez, analista de seguridad para Kaspersky Lab, destaca que durante el CyberDay Chile "**los ciberdelincuentes están atentos a los movimientos de los usuarios**, esperando engañarlos con descuentos, rebajas y promociones maliciosas y así poder infectar sus computadoras y dispositivos móviles con malware para el robo de sus credenciales y finalmente, su dinero".

Desde Kaspersky Lab han aprovechado que se acerca un nuevo CyberDay Chile para mostrar **seis consejos que ayudarán** a los usuarios a **evitar ser víctima de un robo**:

-1. **Conéctese a redes Wi-Fi conocidas y evite las conexiones públicas**. Si el uso de una red Wi-Fi pública es inevitable, utilicé una conexión VPN para cifrar todo el tráfico entre su dispositivo y los sitios Web en Internet.

-2. **Asegúrese de que las URL comiencen con "https: / /" y revise la validez del certificado** dándole clic al ícono del candado ubicado en la barra de la dirección. Esto significa que el sitio cifra la información y que los datos quedan prácticamente inutilizables para cualquier hacker que logre interceptar la transmisión.

-3. **No comparta sus contraseñas ni use la misma para dos o más sitios de Internet**. Asimismo, utilice una que combine letras, números y símbolos especiales como "@#!, a fin de reducir las posibilidades de que un hacker adivine su clave. Para saber qué tan segura es su contraseña haga clic aquí: https://kas.pr/46jd

-4. **Utilice una sola tarjeta de crédito para todas sus compras en líne**a y monitoree las transacciones. Si es posible, habilite con el banco las notificaciones automáticas de SMS por cada transacción realizada.

-5. Cuídese del phishing o suplantación de identidad evitando ingresar información sensible financiera en ventanas pop-up o emails sospechosos o de desconocidos. Si ve que antes del .com, .net, .cl u otros antecede un dominio diferente al original, es phishing.

-6. Finalmente, **mantenga instalado un software de seguridad robusto** como Kaspersky Total Security multidispositivos, que realice escaneos y chequeos rutinarios e incluya herramientas como SafeMoney para asegurar que todas sus transacciones financieras estén protegidas sin importar el dispositivo que utilice.