Deloitte.

Cyber Notes

Compras navideñas

¿Cómo librarse de los cyber delincuentes al acecho de sus tarjetas de crédito y/o débito?

Se acerca una de las fechas más celebradas y los hábitos de consumo con motivo de la temporada decembrina son relevantes para el comercio. Conforme a lo anterior durante esta época navideña las compras por internet aumentan considerablemente, pero ¿conoce usted que en este momento los cyber delincuentes están tratando de robar la información de su tarjeta de crédito o débito para ellos comprar a nombre suyo sin que usted se dé cuenta? Para evitar ser una víctima de este caso, hay que tener cautela y usar esta forma de pago de forma segura para realizar sus compras en línea.

En estas fechas los cyber delincuentes y estafadores utilizan técnicas muy sencillas para crear sitios web falsos, y de esta forma engañar al comprador ofreciendo productos falsificados para robar los datos de su tarjeta de crédito o no entregar el producto que supuestamente compró.

La trampa puede estar en aquellos sitios web que ofrecen el regalo perfecto con un precio evidentemente mucho más barato que todas las demás páginas de compras en línea.

Para identificar un sitio web falso de compras debe realizar la siguiente revisión antes de poner los datos de su tarjeta de crédito para comprar:

- Lo primero que hay que verificar es que el sitio en el que va a efectuar la compra es correcto y seguro. Ingrese a páginas que inicien en su dirección con “https://”

- El sitio web es una copia exacta de otro sitio igual al que está acostumbrado a usar o que utilizó días atrás. Para comprobarlo se tiene que verificar que la dirección es la correcta. Si ve un nombre escrito de manera diferente, como en estos casos www.amazom.com, www.ebey.com, aborte la compra.

- En el sitio web falso o de trampa, en la mayoría de los casos no se incluye números de teléfono para poder llamar a consultar por alguno de los artículos que se ofrecen o para recibir asistencia para realizar la compra, algunos sitios falsos incluyen direcciones físicas de contacto que son falsas o que no existen.

- Si tiene sospechas de un sitio, utilice su buscador favorito y busque referencias, en el resultado de la búsqueda valida los datos del sitio en duda y los resultados de los demás sitios que se mencionan, identifique si existen comentarios negativos de otros compradores o información negativa del sitio.

- La mayoría de estos ataques provienen de otras zonas horarias o geográficas distantes, es importante que revise la ortografía o gramática, errores muy considerables y fáciles de notar son señales de un posible sitio falso.

Tener presente también mantener en la medida de lo posible software antivirus reconocido para protección y seguridad en la navegación por internet, al mismo tiempo recuerde que cada vez que visite un comercio y vaya a pagar con su plástico (tarjeta de crédito y/o débito), no la pierda de vista, existe un alto número de casos en los cuales los estafadores logran copiar sus datos personales y toda información que esta posee al dorso de la misma (incluso hasta los números telefónicos que en algunos países o comercios solicitan se deje anotado). Hay casos en los cuales se logra determinar el patrón de comportamiento comercial de la víctima para realizar transacciones "típicas" (como son compras de supermercado, restaurantes de frecuencia, establecimientos comerciales) y evitar ser detectado. Esta información le sirve a un estafador o incluso a un Hacker para clonar la tarjeta y utilizar técnicas de manipulación de personas para hacer compras a su nombre. Hay entidades financieras que para prevenir este tipo de casos ofrecen a los tarjetahabientes programas de prevención en los cuales para cada compra que se efectúa con el plástico se envía un mensaje de notificación al celular, en estos escenarios se recomienda que visite al emisor de su plástico para que consulte sobre dichos planes de prevención y robo.

Es importante que tenga presente los puntos anteriores a la hora de ingresar los datos de su tarjeta de crédito en un sitio web, le ayudará a realizar sus compras de manera segura y no ser una víctima de fraudes o estafas cibernéticas en esta Navidad.

Existen una diversidad de formas de estafas, con el uso de herramientas de mensajería (como lo es la popular aplicación WhatsApp) han circulado desde hace meses estafas con el logo de marcas como Starbucks y Zara ofreciendo dinero o cupones de descuento para cumplir una encuesta, este tipo de estafa es conocida como "Hoax" y que consiste en engañar a los usuarios suplantando la personalidad de marcas famosas, se recomienda no participar en este tipo de encuestas o sorteos online y en caso de ejecutarlo consultar siempre con la compañía suplantada para corroborar la veracidad de los mismos. La mejor recomendación siempre es no introducir nunca datos personales ni el número de móvil en promociones online.

Emilio Sandoval
Director de Enterprise Risk
Services / Consulting Deloitte