LOCKTON®

Boletín
DAÑOS y FIANZAS

Febrero ·2015·

VIOLACIÓN DE LA SEGURIDAD
DEL CORREO ELECTRÓNICO DE EPSILON.

En un caso de violación de seguridad, el comercializador en línea Epsilon fue víctima de un hacker que obtuvo acceso a los nombres y las direcciones de correo electrónico de los clientes de numerosas compañías e instituciones conocidas de los EE. UU.

Afortunadamente, el fraude de tarjetas no es lo que constituyó la preocupación principal, sin embargo, si lo fue la suplantación de identidad (phishing) y el correo masivo. Un delincuente que ahora sabe que usted compra a un determinado comerciante minorista puede dirigirle un correo electrónico de suplantación de identidad muy convincente. El correo electrónico puede parecer más creíble dado que usted conoce al supuesto remitente y este podría hacer referencia a su nombre completo. Este tipo de correo de suplantación de identidad muy directo se denomina "suplantación de identidad con objetivo específico" (spear phishing).

Los consumidores deben estar atentos a las estafas de suplantación de identidad con objetivo específico. Si recibe una solicitud por correo electrónico en la que se solicita información financiera personal, sea extremadamente cuidadoso y suponga que es fraudulento.

Este incidente se aprovecho para recordar a los clientes que Visa nunca pide ni solicita datos financieros personales por correo electrónico ni por teléfono.

Fuente: VISA Security Sense

LOCKTON CUENTA CON EL PRODUCTO QUE TE PUEDE AYUDAR A MITIGAR EL COSTO DERIVADO DE POSIBLES DEMANDAS DE CLIENTES POR SER VICTIMA DE HACKERS, ADEMAS DE RIESGOS CIBERNETICOS, CONTACTANOS Y TE PODREMOS OFRECER UN INDICATIVO.

CONTACTO:
Araceli Acosta
Tel. 5980.4361
aacosta@mx.lockton.com