Cómo detectar una suplantación de identidad

Un fraude de phishing o suplantación de identidad por correo electrónico es un mensaje de correo electrónico fraudulento que trata de engañar al lector para que proporcione información valiosa personal o de pagos. La suplantación de identidad también puede incluir enlaces o elementos emergentes que, si se les hace clic, pudiésen instalar software nocivo en su computadora.

Para obtener más información sobre los fraudes más novedosos y los consejos de prevención más inteligentes, visite **www.VisaSecuritySense.com**.

Esté atento a estos indicios en su portal de entrada:

¡Mire, pero no haga clic! Si se desplaza el mouse por encima del enlace inserto, se puede ver la dirección de una página web sospechosa y no de un sitio web de Visa. Mientras que el campo "De:" del mensaje de correo electrónico indica que este mensaje proviene de una dirección web "usa.Visa.com", este enlace (como se muestra a continuación) conduce a un dominio extraño que finaliza con ".be".

http://verified.visa.com.aam.data.default.landing.aam.partner.default.resize-yes.cyclepassion-borgloon.be/
Click to follow link

Los cinco mejores consejos para evitar los fraudes de phishing por correo electrónico

1. Considere sospechosos todos los mensajes de correo electrónico que le soliciten información personal o de pagos.
2. Nunca haga clic en los enlaces de los mensajes de correo electrónico no solicitados que reciba.
3. Verifique que cualquier consulta por correo electrónico que solicite información personal o de pago sea legitima. Para ello, busque por separado el número de teléfono de la compañía y llame para verificar la solicitud.
4. Esté atento a los errores tipográficos y gramaticales. Son señales de advertencia de que el mensaje de correo electrónico puede ser fraudulento.
5. Use bloqueadores de correo basura y mantenga su software antivirus actualizado.

La línea "De:" parece ser de una dirección válida de correo electrónico de Visa, pero eso no garantiza que el mensaje sea legítimo. Los estafadores pueden hacer que un mensaje de correo electrónico parezca provenir de alguien o de algún lugar que no es la fuente real, una táctica conocida como "spoofing" (falsificación de IP).

La línea del asunto usa lenguaje amenazador o inquietante para obligar al destinatario a actuar de inmediato. Crear carácter de urgencia o provocar miedo es una táctica común del phishing.

Este mensaje es de Alta prioridad.

De: Visa.com [mailto:service@usa.visa.com] Enviado: Viernes 10 de febrero de 2012, 1:40 a. m.

Para: destinatarios desconocidos

Asunto: Su Tarjeta de Crédito ha sido Suspendida

VISA

Estimado cliente:

Su Tarjeta de Crédito ha sido Suspendida, ya que se detectó un error en la información de su Tarjeta de Crédito. El motivo del error no está corroborado, pero por cuestiones de seguridad hemos suspendido temporalmente su Tarjeta de Crédito.

Necesitamos que actualice su información para poder seguir usando esta Tarjeta de Crédito.

Para Levantar esta Suspensión:

Haga clic aquí

y siga los Pasos para volver a activar su Tarjeta de Crédito.

NOTA: Si ésto no se resuelve dentro de 72 horas, nos veremos obligados a suspender su Tarjeta de Crédito Permanentemente, ya que puede ser usada en forma fraudulenta. El propósito de esta verificación es garantizar que la cuenta de su Tarjeta de Crédito no se haya usado en forma fraudulenta.

Gracias,

Servicio de Atención al Cliente.

Verá que falta personalización, saludo o tratamiento formal, a diferencia de lo que esperaría de la mayoría de las empresas legítimas.

Lea el mensaje detenidamente. A pesar de que el lenguaje parece coherente, hay varias palabras escritas con mayúscula que no deberían estarlo (p. ej., "Tarjeta de Crédito"). Los errores tipográficos y gramaticales deberían ser una clara señal de advertencia de que es probable que el mensaje de correo electrónico sea fraudulento.

Esta suplantación de identidad nuevamente usa un lenguaje amenazador que insta al destinatario a actuar de inmediato. Si recibe un mensaje de correo electrónico semejante, busque por separado la línea de servicio para clientes de la compañía y, en primer lugar, llame para consultar sobre el supuesto problema con la cuenta.

La falta de detalles de cierre, entre ellos cómo comunicarse con la compañía si se requiere más información, también sugiere de manera contundente que se trata de una suplantación de identidad. Una empresa legítima brindaría un número de teléfono de contacto para los clientes, especialmente para un asunto importante como la suspensión de una cuenta.

Nota: Este es sólo un ejemplo de un fraude de phishing, pero existen incontables variaciones que pueden presentar diferentes señales de advertencia.