

**MODALIDAD DE FRAUDE
POR MEDIO DE CORREO ELECTRÓNICO**

La División Seguridad de la Información, comunica a los usuarios que desde el 18 de abril, está circulando un nuevo correo electrónico fraudulento a nombre del Banco de la Nación, donde indica que su cuenta ha sido temporalmente suspendida y donde se le pide ingresar a un link fraudulento para su activación, tal como se muestra a continuación:

De: Banco de la Nacion [mailto:info@h15.com] Enviado el: domingo, 18 de abril de 2010 11:57 p.m. Para: [REDACTED] Asunto: Estimado Cliente	18/04/2010
---	-------------------

ESTIMADO CLIENTE

Debido a reiterados intentos incorrectos para acceder a su cuenta desde nuestra sucursal virtual <http://www.bn.com.pe/index2.shtml>, su cuenta del [Banco de la Nacion](#) ha sido temporalmente suspendida, Por motivos de seguridad.

Hemos implementado los procedimientos electrónicos y administrativos para proteger y ayudar a prevenir el acceso no autorizado, evitar la pérdida, mal uso, alteración y hurto de los datos personales.

En [Banco de la Nacion](#) nos preocupamos por su seguridad, por este motivo recibirá esta notificación de forma automática cada vez que sea necesario.

Para evitar bloqueos y suspensión de los servicios ofrecidos en nuestra sucursal virtual, acceda a su cuenta de manera rápida y segura haciendo click sobre el siguiente enlace que lo llevara directo a nuestra Web. Si el acceso es exitoso nuestro sistema eliminara la suspension de manera inmediata y usted podrá seguir disfrutando de todos nuestros servicios de banca por internet.

<http://www.bn.com.pe/index2.shtml>

Todos los Derechos Reservados 1998-2010 Banco de la Nacion Para cualquier duda o consulta comuniquese con nosotros Desde Lima: 311-6000 Desde Provincias: 0-801-1-6000 Desde Extranjero: (511)311-6000 Copyright © 2010

Figura N°1: “Ejemplo de correo electrónico fraudulento”

Al respecto, comunicamos que dicho correo electrónico es **FALSO**. El Banco de la Nación nunca solicita a través de su página Web, correo electrónico o por algún otro medio sus datos personales confidenciales (número de tarjeta, claves, CVV2, DNI, Fecha de nacimiento, otros).

Por lo tanto, se sugiere que **ELIMINE** estos tipos de correo electrónico y reporte inmediatamente a Mesa de Consultas (anexo: 11491), a fin de realizar el bloqueo de éstas páginas fraudulentas.