

Recuerde:

El Banco de la Nación informa que NUNCA solicita la actualización de los datos personales, claves de información bancaria de sus clientes a través de su página Web, correo electrónico, teléfono u otro medio alternativo.

Estamos para ayudarlo

Para bloquear su tarjeta por pérdida, robo o retención en el cajero:

A nivel nacional desde un teléfono público o fijo a la línea gratuita: **0800-10700**.

Para Lima y Provincias: **01-440-5305**
01-442-4470

atención **24** horas
365 días del año

Horario de atención:

Sedes Multired: Lunes a viernes de 8:30 a 17:30 hrs.

Red de Agencias: Lunes a viernes de 8:00 a 17:30 hrs.
Sábados de 9:00 a 13:00 hrs.

Visite nuestra página en Internet: www.bn.com.pe

Esta información se proporciona con arreglo a la Ley N° 28587 y al Reglamento de Transparencia y Disposiciones aplicables a la Contratación con Usuarios del Sistema Financiero, aprobado mediante Resolución SBS N° 1765-2005.

 Banco de la Nación

Prevenir el fraude
es tarea de todos



Tips de seguridad en tus transacciones por Internet

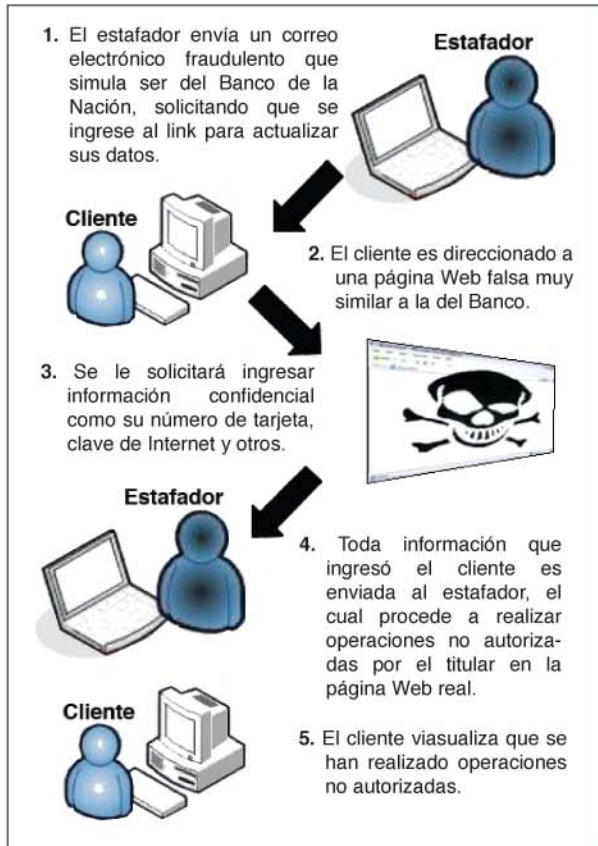
 Banco de la Nación

Prevenir el fraude es responsabilidad de todos

¿QUE ES EL PHISHING?

El phishing en el ámbito bancario es un delito que se comete mediante el uso de la ingeniería social. Se caracteriza por intentar adquirir información confidencial de los clientes como su número de tarjeta, clave de Internet, CVV2, DNI, fecha de nacimiento y otros, para realizar operaciones no autorizadas por el titular tales como transferencias de fondos, pagos, giros, etc.

¿COMO OPERA EL PHISHING?



¿QUÉ APARIENCIA TIENE UN CORREO ELECTRÓNICO FRAUDULENTO?

- Los estafadores crean correos electrónicos fraudulentos más sofisticados, incluyendo logotipos y otras imágenes institucionales.
- Los correos fraudulentos pueden contener mensajes aludiendo situaciones urgentes, utilizando frases como: “Actualice sus datos”, “Alerta de fraude”, “Verifique sus datos”, “Por motivos de seguridad”, “Problemas de carácter técnico”, entre otros.
- Estos mensajes normalmente no son personalizados.
- Están relacionados a las cuentas de ahorros del usuario.
- Solicitan ingresar información confidencial.

Al colocar el mouse en el link que parece dirigir a la página Web real (1), hace referencia al link de una página Web falsa (2).



RECOMENDACIONES PARA EVITAR SER VÍCTIMAS DE PHISHING

- Cuando ingrese a Multired Virtual, usted deberá visualizar que la dirección Web comienza con “httpS://”, donde la “S” indica que la transmisión de información es “segura” y está accediendo a la verdadera página del Banco. Verifique que en el navegador aparezca un candado cerrado, que indica que la página Web cuenta con un Certificado Digital.



- Para visitar el Portal del Banco de la Nación, digite en la barra de direcciones de su navegador: <http://www.bn.com.pe>
- Nunca acceda a la página oficial del Banco a través de links que provienen de correos electrónicos.
- No acceda a la página Web del Banco desde lugares públicos (cabinas de Internet, cibercafé, etc.).
- Evite descargar archivos, música o programas de páginas web o correos de los que no tenga referencias de veracidad.
- Sospeche de correos que lo inviten a ver videos o imágenes de personajes públicos del espectáculo, de la política nacional o internacional, debido a que pueden infectar su PC con virus que roben su información personal.