

## Brinde protección adicional a sus transacciones bancarias por BN Internet Banking

El Banco Nacional NO tiene como política, solicitar a sus clientes información confidencial, como claves de acceso a Internet o los números de tarjetas de crédito o débito, a través de correo electrónico. Si recibe un correo solicitando esta información, le recomendamos borrarlo de inmediato y NO ingresar a los sitios (links) referenciados.

Este hecho constituye una nueva modalidad delictiva denominada "phishing", el cual hace referencia a páginas web falsas que imitan las páginas reales del Banco. **Esta modalidad tiene como fin último engañar y estafar a los usuarios de Internet Banking.**

[Recuerde que la seguridad en el manejo de sus claves, es su responsabilidad, por eso:](#)

- Evite acceder hipervínculos o ejecutar archivos adjuntos en mensajes de correo electrónico.
- No proporcione información personal o referente a sus claves de acceso cuando es solicitada por medio de correo electrónico.
- Nunca ingrese información en un sitio sin haber verificado que el ambiente es seguro, esto se puede reconocer buscando "https://" en la barra de dirección, junto con un candado en la parte inferior derecha de su Explorer.
- Realice sus transacciones únicamente en sitios seguros y si utiliza un Café Internet, asegúrese que cuenta con los requerimientos de seguridad necesarios, de lo contrario no proceda a realizar sus transacciones desde ahí. Les recordamos que el Banco Nacional tiene a su disposición en las Agencias y Sucursales equipos con la seguridad adecuada para el uso de BN Internet Banking Personal.
- Utilice siempre las opciones tecnológicas para la generación de claves aleatorias (OTP) que le brinda el Banco Nacional. Para ello, puede encontrar la información en nuestro sitio web y en nuestras agencias y sucursales.
- Mantenga actualizado su sistema operativo (aplique los parches y recomendaciones del proveedor), el software antivirus, el antispyware y active las funcionalidades de seguridad de su sistema operativo.
- Reporte a cualquiera de nuestras oficinas o a la cuenta de correo bnseg@bncr.fi.cr todo correo sospechoso. Recuerde que en el Banco Nacional estamos más cerca de usted.
- Elimine correos sospechosos o que no conoce su procedencia.
- Sospeche de direcciones numéricas o vínculos desconocidos que se presenten visualmente parecidos a su Banco Nacional.

Para realizar sus transacciones ingrese únicamente a [www.bncr.fi.cr](http://www.bncr.fi.cr) y [www.bnonline.fi.cr](http://www.bnonline.fi.cr).