

FRAUD ALERT

Dear Customer:

It is important to identify and combat a new type of Internet scam known as "*phishing*". The term is a play on the word "fishing," and that's exactly what Internet thieves are doing--fishing for confidential financial information, such as account numbers and passwords. With enough information, a con artist can run up bills on another person's credit card or, in the worst case, even steal that person's identity.

In a common type of phishing scam, individuals receive e-mails that appear to come from their financial institution. The e-mail may look authentic, right down to the use of the institution's logo and marketing slogans. The e-mails often describe a situation that requires immediate attention and then warn that the account will be terminated unless the e-mail recipients verify their account information immediately by clicking on a provided link.

The link will take the e-mail recipient to a screen that asks for account information. While it may appear to be a page sponsored by a legitimate financial institution, the information will actually go to the con artist who sent the e-mail.

The federal financial regulatory agencies want consumers to know that they should never respond to such requests. No legitimate financial institution will ever ask its customers to verify their account information online.

It is also advisable:

- Never click on the link provided in an e-mail if there is reason to believe it is fraudulent. The link may contain a virus.
- Do not be intimidated by e-mails that warn of dire consequences for not following their instructions.
- If there is a question about whether the e-mail is legitimate, go to the company's site by typing in a site address that you know to be legitimate.
- If you fall victim to a phishing scam, act immediately to protect yourself by alerting your financial institution, placing fraud alerts on your credit files and monitoring your account statements closely. If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:
 - Immediately contact your financial institution.
 - Contact the three major credit bureaus and request that a fraud alert be placed on your credit report. The credit bureaus and phone numbers are: Equifax, 1-800-525-6285; Experian, 1-800-397-3742; and TransUnion, 1-800-680-7289.
 - File a complaint with the Federal Trade Commission, FTC at www.consumer.gov/idtheft, or by calling 1-877-438-4338.

AVISO DE FRAUDE

Estimado Cliente:

Es importante identificar y combatir un nuevo tipo de fraude a través del Internet conocido como "*phishing*". Este término viene de la palabra "fishing" (pescando), y es exactamente lo que están haciendo los estafadores por Internet, pescando información financiera confidencial de una persona, como son sus números de cuenta y claves. Con suficiente información, un estafador puede hacer crecer rápidamente cuentas de pagos en la tarjeta de crédito de una persona, o en el peor de los casos, robar la identidad de un individuo.

En una forma común de fraude, las personas reciben correos electrónicos que parecen venir de su institución financiera. El correo electrónico puede parecer auténtico, con logotipo y lemas de mercadeo de la institución. Los correos electrónicos a menudo describen una situación que requiere inmediata acción y luego alertan que la cuenta será cerrada, a menos que quienes estén recibiendo el mensaje verifiquen inmediatamente la información de sus cuentas haciendo "click" en el enlace proporcionado.

El enlace llevará el correo electrónico de quien recibe el mensaje a una pantalla que le pedirá información de la cuenta, y aunque pueda lucir como una página patrocinada por una institución financiera legítima, en realidad la información irá al portal del estafador que envió el correo electrónico.

Las agencias reguladoras federales financieras desean que los consumidores conozcan que nunca deberían responder a tales solicitudes.

Ninguna institución financiera legítima le pedirá a sus clientes verificar información de sus cuentas a través del Internet.

También es aconsejable:

- Nunca hacer "click" al enlace proporcionado, dentro de un correo electrónico, si hay razón para creer que es fraudulento. El enlace puede contener virus.
- No se deje intimidar por correos electrónicos que alertan de lamentables consecuencias por no seguir sus instrucciones.
- Si cree que el correo electrónico no es legítimo, visite el portal de la empresa usando la dirección de Internet que usted sabe es legítima.
- Si Ud. es víctima de fraude por Internet, para su protección, debe actuar rápidamente notificando a su institución financiera, colocando alertas de fraude en sus archivos de crédito y monitoreando sus estados de cuenta constantemente. Si cree que ha proporcionado información financiera confidencial a través de este tipo de fraude, Ud. debe:
 - Informar inmediatamente a su institución financiera.
 - Contactar a las tres agencias nacionales de crédito y solicitar se coloque una alerta de fraude en su reporte de crédito. Los nombres y teléfonos de estas agencias son: Equifax 1-800-525-6285; Experian 1-800-397-3742; y TransUnion 1-800-680-7289.
 - Presentar queja formal con la Comisión Federal de Comercio, FTC a través de la página de Internet www.consumer.gov/idtheft o llamando al número 1-877-438-4338.

Member FDIC

1390 Brickell Avenue, Miami, FL 33131-3324 • P.O. Box 012620, Miami, FL 33101-2620 • Telex 6736848 • ABA: 066011350
Tel.: (305) 539-7500 • Fax: (305) 539-7600 • Direct Call® (305) 539-7574 – From Ecuador 1-800-722-4342
Email: pacific@pnb.com • Web Site: www.pnb.com