

DELITOS. BANCO DE LA NACIÓN ADVIERTE QUE NO REMITE NINGÚN E-MAIL

Mucho cuidado con los correos electrónicos fraudulentos

Estafadores utilizan la técnica del "phishing" para captar víctimas a través del internet. Un correo misterioso es el inicio de todo.

Consuelo Alonzo C.

El "oficio" de Frank Anthony Salvatore Junior Yerena Flores, alias 'Charapa', era robar dinero clonando las páginas webs de conocidos bancos. Para lograrlo se encargaba de enviar correos electrónicos masivos simulando provenir de una entidad financiera determinada y pedía actualizar datos o claves con solo "un clic".

Su modus operandi era adjuntar un link a la misiva y a través de él se descargaba automáticamente un virus informático que roba todo tipo de información. Y, claro, a la vez aparecía una página muy similar a la del banco para generar confianza en el usuario-víctima.

Ahora, si bien él fue capturado la semana pasada, según la Policía Nacional sus cómplices aún libres continúan con sus fechorías.

Tal vez por eso en los últimos días correos fraudulentos del Banco de la Nación comenzaron a llegar a clientes de esa y otras entidades, e incluso a usuarios que no lo eran.

Sobre los mismos, Jorge Gómez, gerente de Comunicación Corporativa del Banco de la Nación, remarcó que dicha entidad no envía ningún tipo de correo electrónico



CHRISTIANSALAZAR.LA REPUBLICA

ALERTAS. Dude siempre cuando le llegue un correo de una entidad bancaria.

●●● LA CLAVE

MODALIDAD. A este tipo de robos a través de internet se le denomina "phishing" pues tratan de "pescar" a una víctima a la que le lanza un anzuelo, vía correo masivo, y su objetivo es conseguir los datos personales para realizar transacciones fraudulentas.

a sus clientes bajo ningún concepto. "Alertamos que no le den clic a ningún enlace. Por ahí se cuelan los virus troyanos y todas las páginas a las que crees que entraste son falsas", sostuvo.

Es más, indicó que cuando ingresen a la página web del banco comprueben siempre que es <http://>

www.bn.com.pe. Y en caso de entrar a la Multired Virtual, es <https://zonasegura1.bn.com.pe/BNWeb/Inicio>. Si es que percibe alguna situación extraña o tiene alguna consulta, puede llamar al 0800-10-700 o al 440-5305.

Sospeche siempre

Otra de las recomendaciones dadas por Gómez es sospechar siempre de correos electrónicos con solicitudes de información personal (nombre de usuario, password o clave de acceso, número de tarjeta bancaria, fecha de caducidad, etc). En otras ocasiones los estafadores emplean argumentos como problemas técnicos, detección de un posible fraude, políticas de seguridad, promoción de nuevos productos, entre otros.