Superintendencia de Bancos y de Otras Instituciones Financieras

Alerta: Recomendaciones para evitar ser víctima de fraude

Estimados Clientes o Usuario de Servicios Financieros:
La Superintendencia recomienda las siguientes medidas ante el auge de los eventos de fraude en cuentas bancarias y tarjetas de crédito.

No revelar a terceros, información de ningún tipo, tales como nombre de usuario y contraseña de acceso a banca en línea, códigos token, nombre completo, número de cédula de identidad, lista de tus contactos telefónicos, pin de cajeros automáticos o números de cuentas bancarias o tarjetas de crédito/débito.
Los bancos no solicitan este tipo de información, ni realizan verificación de cuentas mediante llamadas, mensajes de texto, WhatsApp o correo electrónico.

Si recibes una llamada solicitando información de tus cuentas bancarias o tarjetas de crédito/débito, indicando que proviene de una entidad bancaria, desconfía y llama inmediatamente a los números telefónicos oficiales de dicha entidad.
El Banco no te contactará para solicitar información sobre tus cuentas bancarias y tarjetas de crédito/débito, de manera telefónica.

No descargues aplicaciones desconocidas.

Nunca ingreses tus credenciales en un sitio web que no confíes.
Escribe la dirección del sitio web (URL) de forma manual y verifica que la página web a la que accedes tenga el símbolo de un candado.

No abras archivos o accedas a enlaces que estén dentro de un correo enviado por un remitente desconocido.

No prestes tu cuenta para que otros depositen o transfieran dinero que no te pertenece.
En su mayoría, los defraudadores te ofrecen comisiones para retirar dinero a través de tus cuentas.

No creas en premios o sorteos en los que no participas, principalmente si debes pagar para reclamar el premio.

Superintendencia de Bancos y de Otras Instituciones Financieras

No selecciones "recordar contraseña" en ningún dispositivo. Utiliza contraseñas distintas para cada sitio o producto y asegúrate de que las mismas estén compuestas de letras, símbolos y números.

Recuerda siempre cerrar sesión en las aplicaciones de banca en línea y correo; asimismo, finaliza la sesión cada vez que utilizas cajeros automáticos.

Ten siempre actualizado el sistema operativo y el antivirus de tus dispositivos móviles y fijos.

Verifica la seguridad de las redes Wifi públicas en las que te conectas.

No confíes en ventas de productos a un costo "sospechosamente" bajo. Verifica en las páginas y cuentas oficiales de los comercios las promociones de los productos.

Sospecha si te hablan con acento extraño o palabras rebuscadas.

No te dejes sorprender ante comunicaciones que utilicen el nombre de la Superintendencia y que ofrecen beneficios económicos.

La Superintendencia no promueve, no participa no organiza ni realiza concursos, premios o rifas, en ningún momento y bajo ninguna circunstancia.

Si crees que has sido víctima de fraude, repórtalo inmediatamente a tu banco, solicita el bloqueo de tus cuentas y tarjetas de crédito/débito y cambia tus credenciales de acceso.