Prevenga situaciones riesgosas, no se exponga usted ni su información

En Banco Improsa nos preocupamos por su seguridad, es por ello que a continuación le brindamos consejos y recomendaciones que le ayudaran a prevenir situaciones que expongan su información personal o bien sus recursos.

Estamos a su disposición por medio de nuestra Unidad de Servicio al Cliente, para apoyarle en sus consultas respecto a las mejores prácticas para el manejo de sus datos, cuentas y dinero.

Importancia manejar nuestra información de manera segura

Las contantes transacciones financieras y comerciales que realizamos día a día con rutinas que llevamos sin contratiempos al hacer nuestras diligencias provocan que en muchas ocasiones, debido a un exceso de confianza, no tomemos medidas de seguridad adecuadas para prevenirnos de ser víctimas de un fraude. Es por ello que a continuación les exponemos sobre los principales riesgos relacionados al manejo de su dinero y recomendaciones para prevenirlos.

Riesgos en el manejo de su información personal

Phishing

Es un tipo de fraude originado al recibir un correo electrónico que lo invita a hacer clic en un enlace que envía al usuario a una página falsa la cual le solicita su información personal por diversas razones:

- Participación en sorteos
- Acreditación de premios
- Amenaza de cancelar cuentas al no ingresar sus datos

Recuerde, Banco Improsa nunca le solicitara su información personal por medios no seguros como links correos o acceso

Pharming

El Pharming es un fraude similar al Phishing, pues se trata de extraer sus datos de ingreso a la Banca electrónica Improbank, sin embargo su funcionamiento es distinto, pues no se le invita a ingresar a un link por medio de un correo, si no que al ingresar a www.improbank.com lo redirige a una página falsa.

Recomendaciones de seguridad contra Phishing y Pharming

- Desconfié de correos que aparentan ser de Banco Improsa, pero que le solicitan ingresar a un link de una página que aparenta ser de Improbank para completar sus datos (usuarios, contraseña)
- Verifique siempre la validez de la página web del Banco comprobando que el dominio inicia con https
- Valide que el dominio sea https://www.improbank.com y no un subdominio, por ejemplo http://blogs.totalpda.co.uk/wp-includes/images/improsa.htm
- Verifique en Improbank la existencia del certificado digital, a través del candado cerrado
- Improbank solo le solicitara dos coordenadas de su Improclave, no le va solicitar que las digite todas
- Reporte al Banco cualquier correo sospechoso que reciba
- Si cree que a través del engaño ha digitado su información personal en un sitio web falso repórtelo inmediatamente a la Unidad de Servicios al Cliente de Banco Improsa
- Revise periódicamente su estado de cuenta

Riesgo en el uso de tarjetas de crédito y débito

Clonación de tarjetas de débito y/o crédito

La clonación de tarjetas se da al deslizar la tarjeta en un dispositivo, el cual copia los datos de la banda magnética para ser descargados y transmitidos a una tarjeta falsa.

Recomendaciones de seguridad

- Cuando pague con su tarjeta de crédito o débito en un comercio, no la pierda de vista la tarjeta en la medida de lo posible o bien de un tiempo prudencial para que le sea devuelta

- Mantenga bien custodiadas su tarjeta de crédito y débito para evitar que alguien acceda a ellas y haga una copia de la banda magnética
- No revele su PIN
- En los cajeros automáticos verifique que no hayan lectores de banda magnética sobrepuestos y si descubre algo sospechoso reporte al Banco (numero teléfono)
- Verifique constantemente su estado de cuenta y reporte al Banco aquellas compras con su tarjeta de crédito o débito que no reconozca

Riesgo en el uso de chequera

Robo de cheques

Se trata de extraer cheques en blanco o para completarlo con los datos del estafador y cambiarlos posteriormente en cualquier agencia bancaria

Recomendaciones de seguridad

- Al recibir su chequera verifique que los datos de su cuenta sean precisos y que el consecutivo este completo
- Guarde su chequera bajo llave, puede utilizar archivos de seguridad o cajas fuertes para custodiar sus cheques

- Lleve un control del personal con acceso a las oficinas o lugares donde mantiene sus cheques
- Lleve un control estricto de cheques emitidos y concilie sus cuentas periódicamente
- Al emitir cheques:
    a. Utilice bolígrafos con tinta antifraude
    b. Anote en ellos la leyenda:
        i. Únicamente para depósito en la cuenta N° _____
        ii. No negociable
    c. No deje espacios en blanco, anote el símbolo monetario del monto y escriba en letras la cantidad
    d. No utilice la misma firma para emitir cheque que para firmar cotizaciones o comunicados
- Utilice cámaras para registrar a las personas que ingresan al lugar donde se mantienen custodiados sus documentos valores
- Custodie los documentos que contengan aquellas firmas autorizadas para aprobar cheques
- Mantenga actualizada su información de contacto en el Banco para que sea fácil ubicarlo para la verificación de alguna transacción

Cambio de cheques alterados

Se trata solicitar el pago de algún producto o servicio a los clientes por medio de cheques, los cuales posteriormente se le alteran los datos previo a ser cambiados.

Los riesgos en el uso de chequera pueden incluir el robo de cheques, alterar la información de cheques girados o usar mensajeros falsos para extraer cheques de pagos periódicos

Recomendaciones

- Antes de girar un cheque, analice las empresas o personas que lo solicitan, es preferible que se cuente con una relación comercial establecida, caso contrario verifique las referencias comerciales.
- Al emitir cheques utilice bolígrafos con tinta antifraude, cuyas partículas se adhieren a las fibras de papel e impiden que se pueda borrar lo escrito
- Solicite una identificación de aquellas personas a la cuales se les está pagando con cheque y solicite la firma de un documento de recibido conforme
- Mantenga actualizada su información de contacto en el Banco para que sea fácil ubicarlo para la verificación de alguna transacción

Timo del mensajero falso

Se trata de extraer cheques emitidos por concepto de pagos periódicos, utilizando llamadas y mensajeros falsos.

Recomendaciones

- Este alerta si recibe alguna llamada, después de haber recibido un pago a través de un cheque, indicando que hay algún problema y que enviaran a alguien a entregar un cheque bueno
- Verifique por algún medio con alguien de confianza que efectivamente quien le llama es su Cliente
- Si ha caído en el engaño y entrego el cheque bueno rápidamente coordine con su Cliente y el Banco para poner orden de no pago al cheque
- Mantenga actualizada su información de contacto en el Banco para que sea fácil ubicarlo para la verificación de alguna transacción

En caso de consulta sírvase contactar a la Unidad de Servicio al Cliente al 2522-3800 o escribanos a servicioalcliente@improsa.com