Recomendaciones de seguridad y ciberseguridad

V02 Julio 2019

RECOMENDACIONES GENERALES

- Recuerde que sus claves y datos personales son confidenciales. No los comparta con cualquier persona ni a través de medios como internet, correos electrónicos, encuestas, entre otros.
- La Cooperativa nunca solicita información de sus claves por ningún medio. Absténgase de responder correos que solicitan sus claves.
- Cambie sus claves frecuentemente.
- Revise con frecuencia el saldo y movimiento de sus productos.

AHORROS

- Verifique periódicamente el saldo de las cuentas y reportar cualquier anomalía a la Cooperativa.
- Evite informar a terceros sobre las transacciones realizadas o que se vayan a realizar.
- Al recibir chequeras o libretas de ahorros, verifique que estén completos y la numeración sea consecutiva.
- Siempre destruya comprobantes y extractos antes de depositarlos en la basura.
- Mantenga actualizados los datos de contacto donde se recibirán notificaciones de transacciones.
- Reclame siempre el comprobante de la operación efectuada en su cuenta y verifique su contenido.
- Procure conocer el estado actual de su cuenta de ahorro (Activa o Inactiva)

CFA EXPRESS

- Al asignar su clave personal utilice números que no sean obvios, ejemplo; 1234 ó 0000.
- Para el retiro a través de un Autorizado, CFA entregará el código de autorización a través de un mensaje de texto enviado al celular del titular del CFA express.
- Para retiros de autorizados recuerde que el código de retiro es informado a su número celular registrado, solo debe informar el código de autorización de retiro al autorizado de la operación.
- Recuerde notificar a CFA novedades en el número de celular registrado y realizar la actualización respectiva.
- Evite aperturar el producto con un número de celular cuyo uso sea compartido con terceras personas.

CRÉDITOS

- Entregue la documentación para solicitud de crédito únicamente a personal de CFA que se encuentra identificado y carnetizado en las oficinas o personas autorizadas para atender en sitio.

- En caso de que el crédito solicitado no haya sido aprobado o que no se realice el desembolso, reclame los documentos que entregó a la Cooperativa antes de los 30 días, después de este tiempo serán destruidos.
- En caso de verificación de referencias vía telefónica, sólo brinde información en caso de que efectivamente este solicitando un crédito con la Cooperativa; cerciórese que la información solicitada por nuestro personal sea la misma que usted brindó en la solicitud.

TARJETA DÉBITO

- Cambiar la clave de la tarjeta periódicamente.
- Las claves de sus tarjetas son personales intransferibles, memorícelas, no las escriba y no las comparta; por ningún motivo un empleado de CFA debe solicitárselas.
- Siempre firme la tarjeta en su reverso.
- Reporte inmediatamente a la Cooperativa tras la pérdida de la tarjeta.
- No preste la tarjeta ni permita que otras personas la usen en nombre del titular.
- Al recibir la tarjeta, verificar que sea personalizada con el nombre del titular.
- Mantener la tarjeta en un lugar seguro.
- Realice cambios de su clave al menos una vez al mes, utilice números que no sean obvios, ejemplo; 1234 ó 0000.
- Al sospechar o detectar que ha sido víctima de un fraude, bloquee su cuenta inmediatamente por el servicio de consulta telefónica 01800421827 y/o acuda a la oficina más cercana de CFA solicite una nueva tarjeta y cambie sus claves.
- Actualice permanentemente sus datos personales a través de los diferentes medios dispuestos por CFA.
- Autorice y registre su número de celular y/o correo electrónico para el servicio de alertas automáticas vía mensaje de texto o correo electrónico cada vez que realice una transacción.
- Si desea mayor control de sus operaciones puede personalizar el valor y número que podrá realizar con la tarjeta debito por cajero automático y/o datafono.

CAJEROS ELECTRONICOS

- No realice transacciones cuando observe objetos extraños (cámaras, material pegante, clips) en datafonos y cajeros automáticos, ni acepte ayuda de extraños que le ofrezcan colaboración para realizar sus transacciones, así sean empleados de CFA, personal de mantenimiento del cajero o de transporte de valores.
- Proteja su clave con sus manos y cuerpo al digitarlas, no permita que la vean cuando la esté digitando en un cajero, oficina o establecimiento público.
- Siempre que sea posible, ingresar al cajero automático y asegurar la puerta para que no ingresen otras personas mientras se realiza la transacción.
- En caso que el cajero retenga la tarjeta o no dispense el dinero, comunicarse inmediatamente con la Cooperativa a la línea de Audiorespuesta Jocefa, Área Metropolitana 232 00 11 o en el resto del país al 01 8000 421 827 o con

Visionamos a los siguientes números de contacto: Área Metropolitana – 354 23 24. Antioquia - 01 8000 400 550. Resto del país - 01 8000 521 124 o dirigirse a la oficina más cercana de CFA para realizar la reclamación.

- No permita el ingreso de terceros al cajero automático, si observa personas sospechosas cerca del cajero automático, no realice sus operaciones.
- Presionar el botón Anular o Cancelar para finalizar la transacción si por alguna razón debe abandonarse el cajero automático.
- Espere que el cajero automático indique que la transacción ha finalizado ante de retirarse del mismo.
- No arroje a la cesta de basura los recibos de operaciones de cajeros automáticos; guárdelos destrúyalos, al retirarse del cajero recuerde oprimir la tecla “cancelar” transacción.
- Recuerde que si se usa el sistema de chip, la tarjeta debe permanecer en la unidad lectora hasta finalizar la transacción, en caso contrario la tarjeta nunca debe ser retenida por el dispositivo.

PUNTOS DE PAGO (POS)

- No permita que durante el pago se ingrese la tarjeta en ranuras o dispositivos diferentes al Pin Pad.
- No pierda de vista su tarjeta, verifique que sea pasada por los datafonos una sola vez y después de realizada la transacción verifique que le hayan devuelto su tarjeta.
- Las tarjetas con tecnología chip no deben ser deslizadas por ranuras o lectoras.
- En caso de identificar alguna manipulación sospechosa con la tarjeta, comunicarse inmediatamente con la Cooperativa a la línea de Audiorespuesta Jocefa, Área Metropolitana 232 00 11 o en el resto del país al 01 8000 421 827 o con Visionamos a los siguientes números de contacto: Área Metropolitana – 354 23 24. Antioquia - 01 8000 400 550. Resto del país - 01 8000 521 124.
- Después de realizada la compra verifique la tarjeta que le devolvieron sea la de su propiedad , conserve la copia de la transacción en un lugar seguro y verifíquelos con sus extractos mensuales e infórmenos sobre cualquier anomalía.
- Recuerde que si se usa el sistema de chip, la tarjeta debe permanecer en la unidad lectora hasta finalizar la transacción, en caso contrario la tarjeta nunca debe ser retenida por el dispositivo.

OFICINA VIRTUAL Y PAGOS PSE

- Ingrese a la Oficina Virtual digitando la página web https://www.cfa.com.co, nunca ingrese a través de buscadores, otros sitios web o enlaces de correos ya que pueden direccionarlo a sitios fraudulentos, si recibe estos mensajes repórtelos inmediatamente. Adicionalmente cuando se encuentre en el sitio web de CFA, diríjase a la opción denominada PSE para realizar el pago de sus obligaciones.
- Memorice su usuario y contraseña y manténgalos en absoluta reserva. No los escriba, comparta ni preste.
- Procure cambiar sus contraseñas periódicamente.

- Nunca suministre datos personales confidenciales (usuarios, contraseñas, números de cuenta, etc) en correos electrónicos.
- Cuando ingrese a Oficina Virtual o Pagos PSE verifique que el sitio web es seguro (La barra de navegación se torna color verde e inicia con HTTPS).
- Realice sus transacciones únicamente en equipos de uso personal, evite el acceso desde equipos de uso público como las salas de internet, sitios universitarios, o lugares donde extraños tengan acceso a los equipos.
- No abandone su computador mientras se encuentra en la Oficina Virtual o Pagos por PSE, cuando finalice sus transacciones no olvide CERRAR SESION.
- Apunte siempre el número de aprobación.
- Revise frecuentemente los movimientos de sus productos financieros.
- Mantenga actualizado su sistema operativo, navegador y software antivirus.
- Evite realizar transacciones mientras se está conectado a través de redes inalámbricas públicas.
- La Cooperativa nunca solicitará información personal o financiera por medio de correo electrónico.
- Evite abrir mensajes de correos electrónicos, sospechosos o de los cuales se desconozcas su origen.
- Ejecute análisis de antivirus sobre dispositivos de almacenamiento (memorias usb, discos usb, cds, etc.) antes de usarlos en la computadora.
- Para Persona Jurídica, en la medida de lo posible contar con una máquina dedicada para realizar transacciones electrónicas, protegida con software antivirus y sistema operativo actualizados, evitando la instalación de aplicaciones y uso de memorias usb.
- Para Persona Jurídica, indicar las direcciones IP desde las cuales se autoriza realizar transacciones en la Oficina Virtual.
- Mantener actualizados los datos de contacto donde se recibirán notificaciones de transacciones.

OFICINAS CFA

- No entregue dinero o información a supuestos empleados que los abordan en área de atención al público o en las afueras de la oficina. CFA solo recibe dinero en efectivo en las áreas de caja de las oficinas. Verifique que nuestros emplea dos porten la escarapela y el uniforme que los identifica como tal.
- No permita que personas extrañas se acerquen a las taquillas en el momento de realizar la operación.
- Si al interior de la oficina detecta que personas sospechosas quieren engañarlo con habilidades, artimañas, simulaciones, o lo están siguiendo o acechando solicite apoyo policial o infórmelo a la dirección de la oficina.
- Evite retirar grandes sumas de dinero en efectivo, retire en cheque, procure utilizar los canales virtuales que CFA tiene disponibles como Oficina Virtual o ACH
- Evite ser víctima del “paquete chileno” desconfié cuando extraños le ofrezcan un dinero que supuestamente se han encontrado, esto lo hacen para quedarse con el suyo.

- Observe con atención su entorno y detecte personas o actitudes sospechosas o extrañas e infórmelas inmediatamente.
- Evite mostrar el dinero que consignará hasta que esté en presencia del cajero.
- Abstenerse de cambiar billetes a personas que los aborden al interior de oficinas de CFA
- La policía Nacional presta el servicio de escolta a clientes que realicen retiros de dinero en efectivo, coordine previamente con las autoridades las condiciones y disponibilidad. Dicho acompañamiento no tiene ningún costo.
- Evite en la medida de lo posible retiros de alto monto en efectivo, procurar en cambio utilizar cheques o realizar transacciones electrónicas.
- En caso de observar comportamientos o situaciones sospechosas al interior de la Oficina, avisar de inmediato a los asesores de la Cooperativa.
- Antes de retirarse de la taquilla debe revisarse el comprobante y que la información esté correcta. De igual forma realizar conteo de dinero en taquilla, evitar realizar dicha actividad en otros lugares donde las demás personas puedan observar.
- Asimismo no responder a personas al interior de la oficina que indaguen acerca de sus productos, claves o monto de las operaciones. El personal de la Cooperativa se encuentra debidamente identificado con carnet, sólo ellos podrán brindar ayuda con los servicios de la entidad.
- El uso de teléfonos celulares al interior de la Oficina, se encuentra prohibido.

TRANSACCIONES LÍNEA AUDIO RESPUESTA JOCEFA

- Digite la clave de acceso a la línea JOCEFA solo cuando el sistema lo solicite y recuerde que esta es personal e intransferible.
- Si al realizar una transacción telefónica detecta ruidos extraños, desista de la operación y cambie sus claves secretas.
- Al momento de finalizar la operación a través del teléfono, borre la última marcación haciendo enseguida otra llamada o marcando otro número.
- Consulte con frecuencia sus saldos y revise sus extractos.
- Preferiblemente realice sus llamadas en privado.
- Asegúrese que nadie observe su clave al digitarla.
- Apunte siempre el número de aprobación.
- Evite usar el audiorespuesta desde teléfonos públicos.
- No considere válidos los mensajes que le solicitan llamar a un supuesto número de la Cooperativa.

CORRESPONSALES CFA

- Los Corresponsales CFA se encuentran debidamente identificados en la fachada o letrero del establecimiento y señalizados al interior de este.
- Verificar que el recibo de la operación tenga el número de aprobación, el valor aplicado, la hora y el nombre de la Cooperativa.
- Si realiza retiro de efectivo, verifique el valor de la transacción antes de retirarse del corresponsal.
- Proteja su privacidad, cubra con sus manos o cuerpo las claves mientras las digita.

- No entregue su clave a ninguna persona, digítela usted mismo y no permita que nadie las vea al teclearlas.
- Siempre reclame y verifique la tirilla de la transacción realizada antes de retirarte del Corresponsal, este será su respaldo en caso de presentar una reclamación.
- El Corresponsal no está autorizado para prestarte servicios financieros por cuenta propia.
- El Corresponsal no está autorizado para realizar ningún tipo de cobro por la transacción realizada.
- Recuerde entregar el dinero únicamente al operador del punto de atención en el Corresponsal, no entregue su dinero a personas en la fila.
- Nunca acepte la ayuda de extraños para realizar sus transacciones en el Corresponsal.

RECOMENDACIONES DE CIBERSEGURIDAD

ACERCA DE CIBERSEGURIDAD

La ciberseguridad se refiere a la protección de la información en el ciberespacio (comprendido por Internet y todos los elementos que interactúan con esa red mundial). De allí nacen otras terminologías como ciber-ataques o ciber-delincuentes, que mantienen el mismo concepto pero referidos al crimen a través del ciberespacio.

A continuación CFA Cooperativa Financiera le informa sobre algunas de las principales técnicas de fraude que los ciber-delincuentes utilizan en contra de los consumidores financieros.

PHISHING

- ¿Qué es?
  Los ciber-delincuentes envían correos electrónicos a las víctimas donde les solicitan que accedan a enlaces o archivos adjuntos de manera urgente, utilizando como excusa diferentes tipos de engaños tales como supuestas multas, citaciones judiciales, premios, bloqueos de cuentas bancarias, etc. Esta técnica de fraude es conocida como “phishing”.

- ¿Cómo detectarlo?
  - Verificar siempre que el remitente del correo sea legítimo.
  - Revisar que el contenido del mensaje no contenga errores ortográficos evidentes.
  - Asegurarse que el saludo del mensaje sea personalizado, no genérico.
  - Validar que el idioma del mensaje sea consistente, que no contenga una mezcla de idiomas.
  - Siempre requiere acciones urgentes o inmediatas por parte de la víctima.
  - Analizar si realmente se tienen vínculos con la supuesta entidad que envía el mensaje

- ¿Cómo protegerse?

Nadie está a salvo de recibir este tipo de mensajes, sin embargo ante sospecha de un correo electrónico fraudulento:

- Evitar abrir enlaces o archivos adjuntos.
- Evitar responder a correos electrónicos sospechosos.

MENSAJES DE TEXTO FRAUDULENTOS

- ¿Qué es?

  Los delincuentes envían mensajes de texto (SMS) a las líneas celulares de las víctimas, invitándolos mediante engaños a:
  - Acceder a enlaces de páginas web
  - Llamar a líneas telefónicas atendidas por los defraudadores.

  En ambos casos el propósito es obtener información personal confidencial o estafar a las víctimas.

  Esta técnica es conocida en la terminología de Internet como “smishing”.

- ¿Cómo detectarlos?

  Son mensajes de texto provenientes de números desconocidos que solicitan a la víctima tomar acciones inmediatas o urgentes, tratándose de promociones, ofertas especiales, premios, alertas para verificar o actualizar datos bancarios.

- ¿Cómo prevenirlo?
  - Evitar abrir enlaces contenidos dentro del mensaje de texto.
  - Evitar responder a los mensajes de texto o llamar a las líneas remitente.

FRAUDE POR TELÉFONO

- ¿Qué es?

  Los delincuentes envían correos electrónicos, mensajes voz o correos electrónicos a sus víctimas, invitándoles a comunicarse a líneas telefónicas que ellos mismos controlan. Cuando el usuario realiza la llamada, un sistema de audio-respuesta captura sus datos confidenciales con los cuales se realiza fraude posteriormente. Esta técnica de fraude se conoce como vishing.

¿Cómo detectarlos?

Las solicitudes que reciben las víctimas insisten en la necesidad de llamar con urgencia a una línea telefónica determinada, acudiendo a excusas engañosas como boqueos de cuentas bancarias, actualizaciones de datos, ofertas, premios, etc.

¿Cómo prevenirlo?

- Evitar abrir enlaces contenidos en mensajes de texto sospechosos.
- Evitar responder a los mensajes de texto o llamar a las líneas remitente.
- Evitar abrir enlaces o marcar a líneas telefónicas contenidos en correos electrónicos sospechosos.