Cartilla de seguridad Para nuestros clientes

Recomendaciones para protegerse de los riesgos generados por la utilización de los **Servicios y Canales Bancarios.**

Versión 1.7
Gerencia integral de riesgos
Bogotá D.C.
Febrero 2024

Contenido

Contenido

Advertencia

Advertencia

Las siguientes recomendaciones son tomadas de autoridades a nivel nacional e internacional. Son únicamente una guía educativa para **protegerte de ciertos riesgos derivados de la utilización de los servicios Bancarios.** Por lo tanto, la información aquí presentada no genera ningún tipo de obligación entre el Banco Popular y sus clientes, ni garantiza que su aplicación desaparezca la posibilidad de ocurrencia de fraudes y/o irregularidades. El Banco Popular tampoco se responsabiliza por las decisiones que se adopten con base en esta información.

1. Seguridad En Cajeros Automáticos

El Banco Popular cuenta a nivel nacional con más de 678 cajeros, como parte de la Red de 2256 Cajeros Automáticos de la Red Aval, los cuales prestan un servicio ágil y sencillo para realizar tus transacciones monetarias.

Queremos brindarte una serie de recomendaciones para el uso de tus tarjetas Débito y Crédito en cajeros automáticos, y que sea más seguro vivir una experiencia agradable al utilizar los servicios del Banco Popular.

De igual modo, le brindaremos información sobre posibles eventos de fraude, a los cuales usted se puede ver expuesto al utilizar este canal de servicio, para ello, es necesario que preste atención a las siguientes modalidades:

1.1 Cambiazo En Cajeros Automáticos

Este es un fraude donde personas externas ofrecen ayuda u orientación al cliente para realizar sus transacciones en el cajero automático; con la excusa de que el cajero se encuentra presentando fallas técnicas al momento de efectuar la transacción. Es aquí en donde estas personas ágilmente logran observar la clave que digitas, posteriormente, llevan a cabo el cambio de tu plástico real por otro de características similares, con ello, una tú y el estafador abandonen el cajero automático, este último, con la tarjeta original y la clave de acceso buscará la forma de retirar el dinero antes de que notes el cambio de tarjeta.

En este caso intervienen generalmente dos personas, quienes se ubican cerca al cajero automático para vigilar a los clientes que ingresan allí.

Para evitar que seas víctima de este tipo de fraudes, ten presente las siguientes recomendaciones:

Modalidades

- Firma tu tarjeta en el espacio destinado para este propósito (reverso del plástico).
- Ten mucha precaución si al momento de realizar la transacción en el cajero automático identificas personas pendientes de tus movimientos.
- Procura hacer uso, en la medida de lo posible, de cajeros automáticos que cuenten con una puerta y permitan bloquear el acceso desde adentro.
- Siempre oculta el teclado al momento de digitar tu clave de acceso
- Si en el cajero automático presentas algún tipo de inconveniente con la transacción que intentas realizar, evita recibir ayuda de personas desconocidas, valida directamente con personal del
- Banco, si lo anterior no es posible, puedes revisar si recibiste notificación de la transacción por SMS o consultar tus movimientos en los canales digitales.
- No permitas que se te acerque un tercero a ayudarte o a indicarte pasos sobre la transacción que pretendes realizar.
- No pierdas de vista tu tarjeta y si requieres estar acompañado para realizar operaciones en cajeros automáticos, procura que sean personas conocidas y de mucha confianza.
- Cuando finalices la transacción, por precaución, revisa que se encuentre marcada y tu firma en el reverso .
- Por ningún motivo prestes tu tarjeta, ni divulgues tu clave.
- Si observas cualquier situación sospechosa en el cajero no realices la transacción.
- Si debes salir rápidamente de un cajero electrónico, presiona la tecla cancelar.
- Nunca aceptes ayuda con teléfonos celulares para que llames a tu banco.

2. Seguridad En Establecimientos Comerciales

Otro escenario para ser víctima de fraudes con tarjeta débito/Crédito es cuando realizas compras en establecimientos comerciales. A continuación, conoceras una modalidad utilizada por los delincuentes en establecimientos comerciales, con el propósito de engañar y estafar a su víctima cuando realiza compras mediante el uso de su tarjeta débito/crédito.

2.1 Cambiazo En Comercios

En este caso, al momento de devolverte la tarjeta es cambiada por otra similar, de otro cliente al que han estafado o una falsa. En el momento en el que digitas tu clave, la memorizan, y junto con la tarjeta que han cambiado, proceden a realizar retiros o avances.

Para evitar ser víctima de este tipo de hurto, ten presente las siguientes recomendaciones:

- Cuando realices compras en establecimientos comerciales con cualquiera de tus tarjetas, infórmale al encargado que tu mismo realizarás el ingreso del medio de manejo al datáfono, para hacer la transacción en la caja.
- No entregues tu medio de manejo, los dueños de los comercios están obligados a permitir que sea el titular del medio de manejo quién haga el ingreso del mismo en el datáfono.
- Nunca permitas que deslicen o acerquen tu tarjeta a dispositivos diferentes a los definidos para el pago (Ej. Datáfonos).
- Siempre verifica el monto de la compra, solicita copia del voucher de la compra...
- Cuando digites tu clave cubre el teclado numérico de tal forma que nadie lo pueda ver.
- Destruye los comprobantes de pago de tus compras, antes de arrojarlos a la basura.
- Revisa siempre tu tareta antes de guardarla a fin de verificar que sea la tuya, la cual te recomendamos firmar y marcar con tu nombre y apellido para que la identifiques con facilidad.
- Si tu tarjeta cuenta con tecnología “contactless”, puedes efectuar todo el proceso del pago de la compra sin tener que entregar el plástico.
- No permitas que se tomen fotos de tus tarjetas, ya que esta información puede ser usada para transacciones en comercios electrónicos.

3. Seguridad En Red De Oficinas Bancarias

Otro escenario utilizado por los delincuentes para la realización de fraudes a los clientes, son las oficinas bancarias. En muchas ocasiones, el alto flujo de clientes en un establecimiento bancario se presta para que los delincuentes hagan uso de artimañas para engañar a los clientes, haciéndose pasar por empleados de la entidad bancaria.

A continuación, conoceras algunas modalidades usadas por los delincuentes para defraudar a un cliente que se encuentra dentro de una oficina bancaria, realizando algún tipo de operación en efectivo.

3.1 Fleteo

Es una práctica muy común, la persona que acaba de retirar una gran suma de dinero de una oficina bancaria, al salir de esta es robada a mano armada por individuos que se desplazan en automóvil o motocicleta.

Por lo general, los delincuentes ubican puntos estratégicos dentro de la oficina bancaria, con el propósito de identificar, observar y marcar a sus víctimas, para que puedan ser abordadas al momento de salir del establecimiento bancario.

Para evitar que seas víctima de esta modalidad de hurto, ten en cuenta las siguientes recomendaciones, analizando muy bien los diferentes momentos que harán parte de las transacciones que realice en una oficina bancaria:

- Valida con la entidad los tipos de transacciones que esta te ofrece, en lo posible evita el manejo de grandes sumas de dinero y que debas desplazarte hasta una oficina bancaria.
- Si necesitas realizar el pago de una obligación con la entidad o un tercero, explora alternativas que no implique el uso de dinero en efectivo (Ej. Cheque de gerencia, transferencias electrónicas, débitos automáticos, entre otros).
- En caso de ser obligatorio realizar su transacción en una oficina bancaria, evita comentar o mencionar el detalle de la operación, a personas que no sean de su entera confianza.
- Estando dentro de una oficina bancaria, revisa su entorno, las personas que lo rodean, evita entablar conversaciones mientras estas esperando a ser atenido por un cajero en la ventanilla.
- Cuando seas llamado por un cajero, procura estar solo en la ventanilla y no permitas que personas extrañas se acerquen a tú lado mientras realizas la transacción en efectivo.
- En caso de realizar un retiro en efectivo, se muy discreto mientras verificas el monto recibido, cuando finalices, guarda el dinero de forma segura.
- En caso de tratarse de una gran suma de dinero la que está retirando por ventanilla, solicita el servicio de escolta de la policía antes de retirarte de la oficina bancaria.
- Para el caso de depósitos en efectivo, entrega el dinero únicamente al cajero de ventanilla.

- No entregues tu dinero a personas que se acercan a ti haciéndose pasar por empleados de la entidad bancaria, quienes le ofrecerán su ayuda para agilizar la atención de su transacción y ahorrarle tiempo de espera; esta es la forma en que le pueden hurtar tu dinero..
- Procura llegar a la entidad con los formatos de consignación, o retiro, debidamente diligenciados, evita realizar esta actividad dentro de la oficina y más aún cuando se encuentre con un alto flujo de clientes.
- Al salir de la oficina bancaria, no abordes vehículos de transporte ubicados al frente de esta, procure tomarlos en un sitio diferente.
- Cambia tu rutina de desplazamiento y así evitarás ser "perfilado" por un delincuente.
- En caso de que percibas que está siendo perseguido, ubiqca prontamente una estación de policía o CAI y cuenta la situación.
- Por último, si terminas siendo víctima de un hurto después de abandonar la oficina bancaria, no expongas tu integridad física ni pongas resistencia, intenta memorizar las características de las personas que te atacaron, para que después los puedas denunciar a las autoridades competentes.
- Siempre piensa en resguardar tú seguridad personal y de las personas que te acompañan.

3.2 Cambio De Títulos Valores Por Efectivo

Otra modalidad de estafa que utilizan los delincuentes, tal vez no muy común, es la de aprovechar la urgencia de un cliente que espera el llamado por un cajero de ventanilla para cambiar su cheque en efectivo; es aquí donde el delincuente le ofrece a su víctima suministrarle el valor en efectivo por el cual le han girado su cheque; pero en realidad se pueden presentar dos situaciones fraudulentas:

- Estafar al cliente con billetes falsos
- Adulterar los datos del cheque para cometer fraudes en contra del girador de este.

Para evitar ser víctima o partícipe de estafa en el cambio de títulos valores, debes tener presente las siguientes recomendaciones:

Verifica si tu cheque tiene restricción de pago "únicamente al primer beneficiario"
Si lo anterior es afirmativo, verifica si tiene algún tipo de cruce para consignar en cuenta de primer beneficiario o si es posible su cobro en ventanilla.
Cuando necesites cambiar un cheque por efectivo, procura hacerlo con tiempo y sin endosos a terceras personas que no tengan relación contigo, puedes verte involucrado en un fraude.
Procura consignar a tu cuenta bancaria los cheques recibidos.
No seas parte de un fraude al entregar un título valor a terceros, con quién no guardas relación.
Ante la imposibilidad de realizar el cobro de un cheque por ventanilla, valida la posibilidad del uso de transferencias entre cuentas bancarias.

3.3 Suplantación De Empleados Del Banco

Es una modalidad de fraude utilizada por los delincuentes, consiste en suplantar un empleado de oficina bancaria y así acercarse a los clientes que llegan con la necesidad de ser atendidos lo antes posible; para ello, primero se fijan en clientes que llegan a realizar transacciones en efectivo, por lo cual, los delincuentes ofrecen a sus víctimas la posibilidad "falsa" de ser atendidos de manera especial y sin tener que realizar largas filas. El cliente confía y termina entregándole el dinero que lleva para realizar su transacción en ventanilla a cambio del comprobante de recibido que es emitido por la entidad; situación que nunca sucederá debido a que una vez el delincuente toma el dinero de su víctima, este busca la forma de salir lo antes posible de la oficina sin que nadie se percate de ello.

Para evitar caer en este tipo de engaños y fraudes, ten en cuenta las siguientes recomendaciones:

Cuando llegues a una oficina bancaria a realizar consignaciones o pagos en efectivo, no pongas al descubierto el dinero correspondiente a la transacción.
Evita contar el dinero dentro de la oficina y a la vista de los demás clientes, es ahí donde pueden estar los delincuentes en espera de sus posibles víctimas para hurtarles el dinero en efectivo.
Procura presentarte en la oficina con los comprobantes diligenciados, ya sea un pago o consignación en efectivo.
Cuenta con tiempo considerable para realizar este tipo de operaciones, ten presente que se puede presentar situaciones relacionadas con alto flujo de clientes o fallas en los sistemas de la oficina, lo cual puede ocasionar algunas demoras para ser atendidos.
Por ningún motivo aceptes propuestas de personas que se identifiquen como empleados de la oficina bancaria y le ofrezcan su ayuda para realizar su transacción sin tener que hacer la fila o pasar por la ventanilla.
No olvides que los únicos autorizados para recibir dinero en efectivo son los cajeros por ventanilla, no caigas en la trampa de personas que prometen ahorrar tiempo..
Ten paciencia y espera el llamado del cajero para ser atendido.
Si evidencias alguna situación anormal o que se presenta alguna situación de las mencionadas anteriormente, avisa inmediatamente al Gerente o asistente administrativo de la oficina, para que tomen las medidas correspondientes.
No solicites ni recibas ayuda de extraños, solicítala únicamente al personal de la entidad.
Al realizar trámites con cierta periodicidad, evita crear rutinas que permitan conocer días, y horarios de tus movimientos bancarios.
Si se presentan demoras injustificadas en la entrega del dinero que hayan obligado al cajero a retirarse del lugar y realizar llamadas telefónicas, se debe informar de inmediato al Gerente de la Oficina del Banco.

4. Tu Seguridad En Los Canales Digitales (Internet)

Dada la evolución que ha tenido el uso de los canales digitales al momento de realizar operaciones bancarias, así mismo, los delincuentes han desarrollado técnicas para estafar a más clientes y con menor grado de exposición, ellos han encontrado en el ciberespacio una gran fuente de ingresos.. A continuación, encontrarás algunas pautas que te permitirán conocer modalidades de estafa y así evitar ser víctima de posibles robos de información y dinero a través de canales digitales:

4.1 Robo De Identidad Digital ... ¡Tus Datos Son Importantes!

El Término Robo de Identidad digital se refiere a la obtención de información personal de una víctima, para cometer fraudes electrónicos en nombre de esta. Un delincuente buscará robar datos personales como nombres, número de identificación, números de tarjeta de débito/crédito, contraseñas, entre otros.

¿Cómo se realiza el Robo de identidad digital?

El delincuente siempre estará al acecho de su víctima y a la espera de que esta se descuide, por esto debes prestar mucha atención al entorno que te rodea, cada vez que hagas algún tipo de diligencia fuera de tu casa o lugar de trabajo, procura utilizar conexiones seguras para acceder a tus contenidos en internet, evita ingresar a páginas web que puedan comprometer la seguridad de tu dispositivo y la información que allí tienes almacenada.

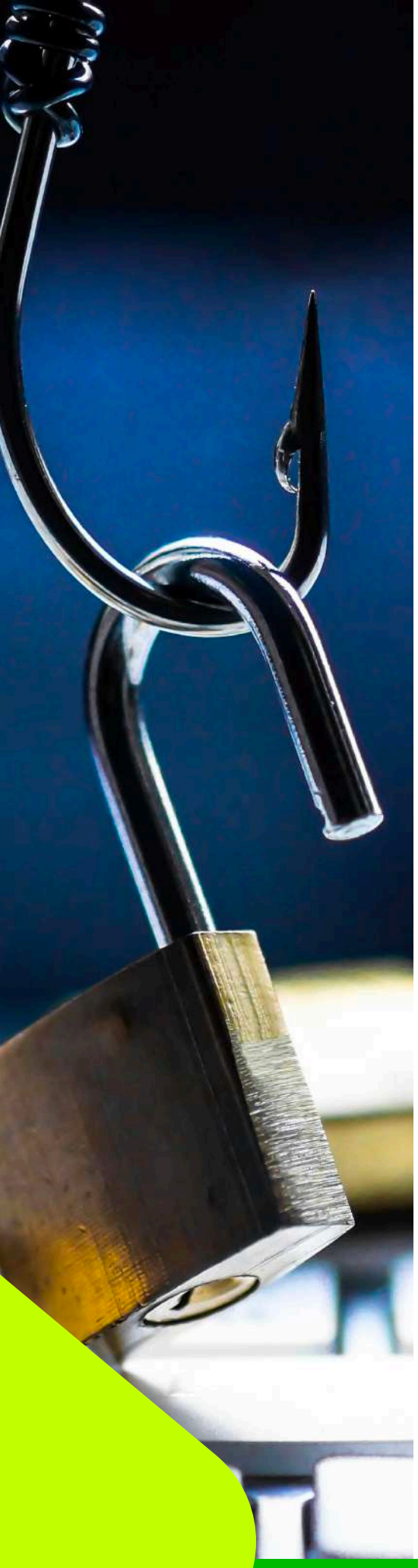
Robo identidad

- Robo o perdida de tu billetera o bolso, esto puede ocasionar la pérdida de tu información personal, dinero y tarjetas débito/crédito.
- Robo de información personal en tu propia casa o la que recibes a través de correspondencia urbana; es conveniente que deseches y destruyas adecuadamente los documentos que contengan información personal; en lo posible, toma el hábito de administrar tu correspondencia a través de correo electrónico y no por medio físico.
- Instalación silenciosa de un software malicioso, esto puede ocurrir si accedes a páginas inseguras o ejecutas contenidos inmersos en correos de dudosa procedencia, al final lo que el delincuente busca es el robo de tu información personal y financiera.
- Brechas de seguridad por las cuales el delincuente podría tomar control remoto del dispositivo, robar tu información y cometer fraudes electrónicos, causado por hacer uso de software ilegal para configurar tus distintos dispositivos, te puede ocasionar la generación de.

Ten en cuenta que, con el robo de tu información personal e identidad digital, un delincuente puede realizar fraudes y conseguir objetivos en beneficio propio tales como:

- Suplantar tu identidad con el fin de abrir cuentas bancarias, solicitar tarjetas de crédito o préstamos a tu nombre.
- Suplantar tu identidad con el fin de adquirir planes y servicios de telefonía celular.
- Usar la información que te robó, con el objetivo de falsificar tarjetas débito / crédito.
- Realizar movimientos transaccionales sin tener tu consentimiento como titular de una cuenta.
- Registrarse en canales digitales que no son frecuentados por ti.
- Registrar otros dispositivos electrónicos para acceder a las aplicaciones móviles bancarias en donde tengas acceso.

Para evitar que seas víctima de fraudes electrónicos por causa del robo de tu identidad digital, **ten en cuenta las siguientes recomendaciones:**



4.2 Ingeniería Social...

¡No Permitas Que Te Manipulen!

¿Sabías que la ingeniería social es un método muy utilizado por los delincuentes para realizar el robo de identidad e información confidencial de sus víctimas, y que esto lo realiza a través de la manipulación de las personas? Un delincuente usará comúnmente la comunicación telefónica, el envío de correos electrónicos maliciosos u otros métodos; siempre su objetivo será engañar a sus víctimas y llevarlas a entregar su información confidencial o de la organización en la que trabajan.

Para que un delincuente no tenga éxito con el robo de tu información, ten en cuenta las siguientes recomendaciones:

- Nunca entregues tu información personal a personas extrañas que se comuniquen contigo a través de correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales.
- No digites claves o códigos a través de tu teclado, durante una llamada telefónica.
- Sé precavido con la información que compartes y publicas en sitios de redes sociales, activa y personaliza las configuraciones de privacidad; ten presente que esta es una de las fuentes predilectas usadas por los delincuentes para realizar un "perfilamiento" de sus víctimas.
- Cuando seas abordado para ofrecerte algún tipo de servicio bancario, mantente muy atento y alerta a las preguntas que te realizan y piensa muy bien en las respuestas que brindarás; recuerda que de eso trata la ingeniería social, de como "trabajar a una persona" para que suministre su información confidencial inconscientemente.
- Para los servicios que utilices en internet, procura asignar contraseñas seguras y robustas y evita utilizar una misma contraseña para más de uno.
- Adopta hábitos de cambio y asignación de nuevas contraseñas con cierta periodicidad, cuyos lapsos no sean muy extensos (aconsejable que no sea mayor a 60 días).
- En la media que te sea posible, habilita la opción de autenticación en dos pasos para el ingreso a tus portales bancarios, correos electrónicos, redes sociales y todo aquel servicio que consideres sensible para el manejo de tu información.

Phishing

4.3 Phishing... *¡Cuidado con los sitios web falsos!*

Esta es una técnica (Ciberamenaza) utilizada por un delincuente, que consiste en aplicar elementos de ingeniería social para engañar a su víctima y así robar tu información personal a través de servicios de mensajería electrónica. El delincuente envía a su víctima un mensaje por correo electrónico o un sistema de mensajería instantánea como WhatsApp, suplantando a una entidad legítima y de confianza (Ej. Un banco, red social, entidades públicas, entre otras), en el cuerpo de dicho mensaje insertará un enlace web que, al momento de dar clic por su víctima, conectará con una página web falsa pero que su apariencia es muy similar a la de un sitio legítimo. Una vez que la víctima cae en el engaño y confía que está accediendo a una página verdadera, termina por suministrar datos personales o financieros; cuando el delincuente obtiene este tipo de información, comienza a ejecutar fraudes monetarios o robo de más información de sus víctimas, para luego extorsionarlas económicamente.

Para evitar ser víctima de un fraude por causa de un ataque de phishing, ten en cuenta las siguientes recomendaciones:

- Identifica muy bien los remitentes de tus correos electrónicos, si recibes mensajes con información o contenido que no guarde relación contigo, evita abrirlos y ejecutar cualquier tipo de enlace web o archivos adjuntos.
- Si recibes mensajes de parte de una supuesta entidad financiera para pedirte que actualices tus datos haciendo clic en un enlace, ten cuidado de no caer en un engaño, recuerda que ninguna entidad bancaria pide a sus clientes que realicen este proceso y mediante estos canales de comunicación; adicionalmente, recuerda que tu información la podrás actualizar cada vez que lo consideres necesario y a través de los canales oficiales de tu entidad bancaria.
- Evita ingresar a portales bancarios por medio de enlaces web que recibas a través de correos electrónicos, estos atajos te pueden conducir a páginas falsas que suplantan la identidad de entidades legítimas, con el fin de engañar a sus víctimas y así robar su información.
- Mantén actualizado tu computador y dispositivo móvil, implementa herramientas como un antivirus, que te ayude a revisar y bloquear el acceso a páginas que sean consideradas como inseguras.
- Haz un monitoreo frecuente sobre el movimiento de tus cuentas bancarias, perfiles de redes sociales y toda fuente que tenga información confidencial.
- Ante la duda de saber si el mensaje recibido es legal o fraudulento debido a que desconoces su procedencia, evita abrirlo y, si lo haces, no ejecutes enlaces o archivos que estén adjuntos; puede tratarse de un ataque de phishing que ponga en riesgo tu información confidencial.
- Procura estar informado en temas de seguridad y ciberseguridad, esto te ayudará a entender mucho mejor los riesgos a los que se expone tu información cada vez que se cae en este tipo de engaños.

Recuerda que, con tus datos, un delincuente puede cometer fraudes electrónicos en tu contra u otra persona, podrías verte envuelto en posibles delitos informáticos si no reportas inmediatamente a las autoridades el posible robo de sus datos.

Vishing

4.4 Vishing... *¡Cuidado con las llamadas telefónicas!*

Este un ataque similar al Phishing, solo que en este caso el delincuente hace uso de las llamadas telefónicas, haciéndose pasar por un representante de la entidad que está suplantando, su objetivo será engañar a su víctima para obtener información confidencial. Cuando un delincuente suplanta a una entidad bancaria, al momento de llamar a su víctima, este se hace pasar por un empleado de dicha entidad; mediante el uso de un "guion" muy bien estructurado en la llamada que hace a su víctima, su objetivo es captar la atención de su víctima hasta el punto "someterlo" a su engaño.

Luego empieza a suministrar una serie de instrucciones (a veces a través del envío de mensajes falsos al telefóno móvil de la víctima) indicándole la necesidad de proporcionar información confidencial, ya sea de manera verbal o digitándola en el teclado de su dispositivo móvil, por ejemplo: contraseñas de ingreso a sus portales transaccionales, clave de la tarjeta débito/crédito, número y código de seguridad de la tarjeta crédito, códigos recibidos por mensaje de texto (OTP) o clave de línea verde; bajo el supuesto propósito de evitar el bloqueo de alguno de sus productos o el ofrecimiento de apertura de nuevos.

Una vez que el delincuente obtiene la información de su víctima por medio de la llamada, accede al portal bancario con las credenciales del cliente, allí puede realizar distintas operaciones que terminan defraudando a la persona y robando el saldo del dinero, o también, generando solicitudes de crédito a nombre de dicho cliente.

Ten en cuenta las distintas situaciones que se pueden presentar en este tipo de ataque (llamadas falsas):

- Puedes escuchar una grabación que te alerte sobre tu cuenta bancaria, tarjeta de crédito, etc., indicándote que está siendo utilizada de forma fraudulenta y que debes llamar al número telefónico que te indican inmediatamente; este número telefónico puede ser una línea gratuita falsa, haciéndola pasar como legítima y perteneciente a la entidad financiera que pretenden suplantar.
- Se presenta una persona que se hace pasar por un agente de la entidad financiera, te brinda información sobre el trámite de devolución del IVA o del 4X1000, te indican que para hacer efectivo el procedimiento, deberás suministrar o digitar la clave que te acaba de llegar por mensaje de texto a tu dispositivo móvil.
- Se presenta una persona que se hace pasar por un agente de la entidad financiera, te informa sobre un posible fraude con alguno de tus productos financieros, es por esto que, debes gestionar de inmediato el bloqueo de tus productos, para ello, dicha persona te solicitará que le digas o digites la clave de tu token (OTP), la de tus productos o la del mensaje de texto que te enviará al dispositivo móvil.

Para evitar ser víctima de un fraude por causa de un ataque de Vishing, ten en cuenta las siguientes recomendaciones:

Presta mucha atención a la conversación y a la información que te brindan o te solicitan.
Es posible que el delincuente conozca algunos de tus datos personales, si te pide que los confirmes o complementes, ¡no lo hagas!.
Recuerda que el banco no te llamará para solicitarte datos personales y confidenciales.
Si la llamada te genera dudas o sospechas, lo más conveniente es que la termines y te comuniques de inmediato con el banco.
No presiones botones o digites números en tu teclado cuando te lote soliciten en la llamada
Procura obtener la identidad de la persona que te está contactando.
Toma nota de los detalles de la llamada, pero por ningún motivo entregues tus datos.

Malware

4.5 Malware *(Programa Malicioso)... ¡Cuidado con lo que instalas!*

Son programas o archivos dañinos para los computadores, diseñados para infectarlos con virus, Spyware, troyanos, entre otros; su propósito una vez se han instalado en los dispositivos comprometidos, es recolectar información de todo tipo y que se relacione con el usuario y equipo. Con esta información el delincuente puede ejecutar ataques remotos en contra de su víctima, su objetivo será su propio beneficio y la defraudación de la persona afectada.

Normalmente, un malware es enviado a través de correos electrónicos que aparentemente son legítimos, allí se adjuntan archivos o enlaces web para que la víctima descargue el archivo y lo ejecute, o que haga clic en el enlace y acceda a un sitio malicioso, cayendo en el engaño y entregando su información confidencial por haber infectado su dispositivo. Una vez se ejecuta este programa en el equipo de la víctima y, dependiendo su función, puede robar información personal, monitorear las actividades que el usuario realiza en su equipo, o tomar control remoto del dispositivo para realizar más ciberataques en contra de la misma persona u otras.

Un malware también puede comprometer dispositivos móviles a través de la instalación de aplicaciones que son descargadas desde tiendas no oficiales (App Store, Play Store) o a través de aplicaciones que aparentemente son legitimas y "gratuitas" y que son infiltradas por los delincuentes en las tiendas oficiales.

- Para evitar ser víctima de un fraude por causa de un ataque de Malware, ten en cuenta las siguientes recomendaciones:

- Instala un antivirus en los dispositivos que utilizas para realizar tus operaciones en internet; así mismo, procura que la instalación corresponda a un producto licenciado por el fabricante (así sea una versión gratuita incialmente) y no programas que se ofrezcan en internet como manipulados y licenciados de por vida.
- No abras archivos adjuntos que provengan de remitentes que desconozcas, si no es posible la comprobación de su origen, es preferible que elimines el mensaje.
- Ejecuta análisis programados a través de tu herramienta de antivirus, para el escaneo de tus dispositivos móviles y de cómputo.
- Procura mantener actualizados tus dispositivos, teniendo en cuenta la liberación de "Paches" de seguridad emtidos por los fabricantes, así mismo, la instalación de la nueva versión de las aplicaciones o sistemas que utilices.
- Habilita las condiciones de seguridad en la conexión que realice a una red WIFI, existen parámetros de cifrado que contribuyen a garantizar el buen manejo de los datos (Ej. WPA2).
- Evita conectarte y navegar en redes WIFI que sean públicas y abiertas, estas no poseen condiciones de seguridad y podrían exponer tu información ante los delincuentes informáticos.
- Procura hacer uso de contraseñas seguras e independientes una de la otra, cada vez que accedas a servicios web (Ej. Redes sociales, correo electrónico, portales bancarios, entre otros).
  Procura realizar una copia segura de tus archivos, en caso de verte afectado por una infección de malware, para que puedas restaurar tu información en caso de una reinstalación de tu dispositivo.

Quishing

4.6 Quishing... *¡No todos los códigos QR son seguros!*

Esta modalidad de estafa consiste en el escaneo de código QR falsos, los cuales conducen al ingreso de sitios web falsos o la descarga e instalación de software malicioso; los atacantes están realizando la suplantación de estos códigos cuando se encuentran en folletos, panfletos, pegatinas (Stickers) para pagos en comercios, entre otros medios de interacción con estos códigos; el objetivo será el mismo y que conduzca al robo de información confidencial de las víctimas para la ejecución de fraudes electrónicos.,

- Para evitar ser víctima de un fraude por causa de un ataque de Quishing, ten en cuenta las siguientes recomendaciones:

- Evita escanear códigos QR (en páginas web, folletos, stickers, afiches, entre otros) de establecimientos o contenidos que desconozcas, pueden dirigirte a un sitio malicioso y comprometer tu información confidencial.

- No ingreses a los sitios web que se habiliten como resultado del escaneo de códigos QR sospechosos, puede tratarse de una página maliciosa y, al ingresar en ella, puedes ser víctima del robo de tu información o de un fraude electrónico.

- Mantén actualizado tu dispositivo móvil y evita instalar aplicaciones que descarguen de sitios web escaneados por códigos QR, puede tratarse de software malicioso con el propósito de robar tu información o de tomar control de tu dispositivo.

- Procura activar la autenticación de dos pasos en tus aplicaciones de correo electrónico, redes sociales, portales bancarios, entre otros; así evitarás que un delincuente acceda a tu información en caso que se comprometa tu dispositivo.

4.7 Sim Swapping... *¡Vigila tu dispositivo móvil!*

El SIM Swap o intercambio de SIM Card es una técnica utilizada por delincuentes para robar información financiera o dinero mediante el bloqueo o portabilidad numérica de la tarjeta o SIM Card y la reexpedición de una nueva en los operadores de telefonía.

Con esta nueva tarjeta SIM, los defraudadores tienen acceso a las claves temporales (OTPs) enviadas por SMS, a las alertas de los movimientos financieros de la víctima; así mismo, los delincuentes pueden autenticarse en los portales bancarios y hacer fraudes en nombre de la víctima a la cual están estafando.

Para evitar ser víctima de un fraude por causa de un ataque de Sim Swapping, ten en cuenta las siguientes recomendaciones:

Recomendaciones

- Cuida muy bien los datos que te puedan identificar y ubicar geográficamente, datos como número de identificación, dirección de domicilio (casa u oficina), fecha de nacimiento o fecha de expedición de su documento de identificación, entre otros.
- Haz una revisión de los posibles sitios en donde hayas registrado los datos mencionados, elimínalos de aquellas aplicaciones o perfiles a los cuales ya no accedes o que simplemente no es necesario que tengan esta información.
- Revisa tu dispositivo móvil y evita guardar los datos confidenciales que te puedan identificar, recuerda que con ellos los delincuentes pueden robar tu identidad y cometer fraudes en tu nombre.
- Procura instalar en tu dispositivo móvil una aplicación (segura) que te sirva de “bloqueo de acceso”, con ello podrás proteger aún más tu información confidencial y las aplicaciones sensibles.
- Con cierta periodicidad, valida con tu operador de telefonía móvil si en un lapso determinado se han registrado requerimientos de reexpedición de tarjeta SIM, en caso afirmativo, verifica que corresponda a solicitudes que tú has hecho o, de lo contrario, solicita urgentemente un cambio de la tarjeta SIM y el bloqueo de las otras que puedan estar activas.
- Si es hurtado tu teléfono móvil, solicita a tu operador de servicio de telefonía que bloquee el IMEI del teléfono.
- En caso de ser posible, realiza de forma remota el bloqueo y borrado de la información de tu dispositivo.
- Acude a las autoridades e informa sobre este hecho para radicar un denuncio.

No descuides tus datos personales, estos pueden ser utilizados fraudulentamente en tu contra.

Smishing

4.8 Smishing...

¡Cuidado con los mensajes de texto!

Este es un ataque similar a un Phishing o Vishing, la diferencia se encuentra en el medio que utiliza el delincuente para engañar a sus víctimas; para este caso, se utiliza el envío de mensajes de texto (SMS) a los celulares de las personas; por lo general, la información enviada por este medio busca alertar o captar la atención de la víctima, haciéndole creer que sus productos presentan irregularidades, que han sido favorecidos con premios, beneficios, etc.

En el mensaje el delincuente enviará a su víctima la instrucción de acceder a un enlace web o comunicarse con alguna línea telefónica; ambos casos son falsos y una vez que la persona los accede, el delincuente hará lo posible por robar su información y así cometer fraudes bancarios o realizar acciones extorsivas.

Para evitar ser víctima de un fraude por causa de un ataque de Smishing, ten en cuenta las siguientes recomendaciones:

- Si recibes un mensaje de texto cuyo remitente no conoces o consideras sospechoso, no lo respondas ni interactúes con el contenido inmerso en este.
- No ingreses a sitios web cuyo enlace venga dentro del mensaje de texto, esta es la forma que usa el delincuente para que su víctima caiga en el engaño y acceda a sitios falsos.
- Si te solicitan a través de un mensaje de texto actualizar tus datos o ingresar contraseñas de alguno de tus productos, informa inmediatamente al Banco sobre este evento y posteriormente elimina el mensaje, por ningún motivo suministres la información que te solicitan.
- Ante mensajes de texto que informen sobre algún bloqueo o restricción de alguno de tus productos, no realices ninguna acción de respuesta ni suministres información confidencial, solo comunícate inmediatamente con el Banco a través de los canales autorizados, los cuales puedes consultar en la página www.bancopopular.com.co.

Bating

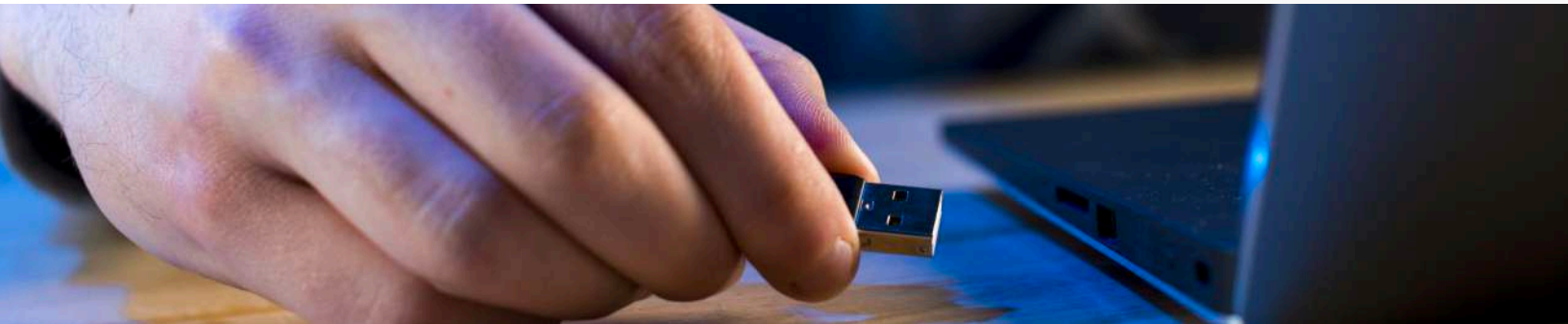
4.9 Bating O Cebo... *¡Sospecha De Una "Usb" Gratis!*

Esta es una técnica utilizada por los delincuentes, que consiste en dejar abandonados en sitios públicos, pasillos, plazoletas, entre otros; dispositivos de almacenamiento externo (Ej. USB, CD/DVD, MicroSD, entre otros) infectados por algún tipo de malware para que, producto de la curiosidad de una persona, sean recogidos y conectados en dispositivos personales o corporativos y así lograr la infección de estos para poder controlarlos remotamente.

Es así, como el delincuente puede llegar a capturar la información personal o corporativa de su víctima, posteriormente, someterla a fraudes electrónicos tanto a ella como a la empresa en la que esta labora.

Para evitar ser víctima de un fraude por causa de un ataque de Bating, ten en cuenta las siguientes recomendaciones:

- No recojas dispositivos de almacenamiento externo, los cuales se encuentren abandonados.
- Si uno de estos elementos capta tu atención, por ningún motivo lo conectes a tu dispositivo personal o corporativo; puedes ser víctima de la descarga e instalación de un software malicioso, el cual es utilizado por un delincuente para el robo de tu información o de la empresa en la que trabajas.
- En lo posible, destruye este tipo de elementos y así evitarás que otras personas caigan en este tipo de engaño.
- Ante la conexión de dispositivos de almacenamiento externo en tu equipo de cómputo o tableta; mantén instalada y actualizada una herramienta de antivirus que se encargue de revisar el contenido de estos elementos.
- Procura deshabilitar la reproducción automática de los dispositivos de almacenamiento externo, esto evitará que se ejecute de forma automática cualquier tipo de software malicioso.



Dumpster

4.10 Dumpster Diving (Husmear En La Basura)...
¿Conocías Esta Técnica?

Esta es una técnica utilizada por los delincuentes, que consiste en dejar abandonados en sitios públicos, pasillos, plazoletas, entre otros; dispositivos de almacenamiento externo (Ej. USB, CD/DVD, MicroSD, entre otros) infectados por algún tipo de malware para que, producto de la curiosidad de una persona, sean recogidos y conectados en dispositivos personales o corporativos y así lograr la infección de estos para poder controlarlos remotamente.

Es así, como el delincuente puede llegar a capturar la información personal o corporativa de su víctima, posteriormente, someterla a fraudes electrónicos tanto a ella como a la empresa en la que esta labora.

Para evitar ser víctima de un fraude por causa de un ataque de Bating, ten en cuenta las siguientes recomendaciones:

- Revisa muy bien los documentos o papeles que arrojas a la basura, verifica que no existe
- información que se relacione contigo o personas cercanas, ni tampoco que te identifique.
  Si recibes información impresa sobre tus productos bancarios, no la dejes en lugares visibles y a disposición de cualquier persona, ten presente que esta es información personal y confidencial.
- Cuando desees eliminar la información impresa, destrúyela adecuadamente y de forma tal que no se pueda reconstruir algún dato; para ello, haz cortes muy diminutos de cada papel, para ello utiliza
- tus propias manos, una picadora de papel, unas tijeras, entre otros.
  Cuando arrojes a la basura sobres de correspondencia, revisa primero que tus datos personales (nombres, dirección, identificación, etc.) no se encuentren impresos o visibles, si lo están, raya o
- tacha esta información y ahí sí arrójalo a la basura.
  Evita acumular demasiada información impresa en lugares que sean de fácil acceso para distintas personas, lo más aconsejable es que elimines esta información en la medida que ya no la necesites.

  Siempre presta atención a lo que estás arrojando a la basura, recuerda que puede existir información que sea de gran utilidad para un delincuente, con ella podría realizar fraudes en tu contra; por ello, procura recibir tu información a través de correo electrónico.

Rogueware

4.11 Rogueware... *¡Cuando un antivirus no es lo que parece!*

Este es un ataque basado en el uso de software malicioso, que al estar instalado en un dispositivo toma la apariencia de un programa de antivirus, con el fin de enviar falsas alertas a los usuarios e indicando que el equipo presenta anomalías de seguridad, que la información se encuentra comprometida, entre otras alertas.

El delincuente que usa esta técnica busca que su víctima se vea obligada a prestar atención a la información falsa, terminando con la instalación de un software malicioso que le ofrecen en cada alerta y cuyo objetivo es el robo de la información confidencial de la persona, obtener usuarios y contraseñas para acceder a portales bancarios, correos electrónicos y demás servicios personales.

Para evitar ser víctima de un fraude por causa de un ataque de Rogueware, ten en cuenta las siguientes recomendaciones:

- Instala un antivirus legal en cada uno de los dispositivos que utilizas para navegar en internet, verifica que se actualice a diario y así evitarás infecciones por nuevas amenazas.
- Mantén actualizado el sistema operativo y las aplicaciones de tus dispositivos, en caso de no hacerlo, podrías verte afectado por una brecha de seguridad que podría ser explotada por un atacante.
- Sé cauteloso con las páginas que consultas en internet, algunos sitios maliciosos toman la apariencia de sitios “auténticos” para engañar a sus víctimas y poder robar su información.
- Constantemente haz una limpieza de archivos temporales e historial de navegación en tu equipo de cómputo.
- Configura tareas programadas en tu herramienta de antivirus, con el fin de realizar un escaneo profundo de tu dispositivo por lo menos tres (3) veces por semana.
- Evita descargar programas y archivos que se encuentren en páginas sospechosas, recuerda que un malware se puede instalar de forma silenciosa.

4.12 Aplicaciones Maliciosas...
¡Ten cuidado con tus aplicaciones!

Otra técnica utilizada por delincuentes es la utilización de aplicaciones maliciosas, estas son diseñadas para suplantar a una legítima y están publicadas en tiendas “no oficiales” y con publicidad llamativa para que sean descargadas por los usuarios.

Sin embargo, estas aplicaciones una vez se instalan en los dispositivos de las víctimas, comienzan a pedir un sin número de permisos sobre este y pueden considerarse de tipo abusivo, pues el objetivo del delincuente es tomar control total del dispositivo y de la información que reposa en él, así podrá tener los insumos suficientes para generar fraudes en contra del dueño del dispositivo.

Para evitar ser víctima de un fraude por causa de un ataque de Aplicaciones maliciosas, ten en cuenta las siguientes recomendaciones:

Descarga e instala aplicaciones que se encuentren en las tiendas oficiales como

App Store – Apple, Play Store – Google, Microsoft Store, entre otras.

Evita descargar aplicaciones de sitios web que te ofrezcan productos aparentemente “licenciados y legales”, esto podría tratarse de una estafa que terminaría en el robo de tu información personal y confidencial.

Al momento de instalar una aplicación en tus dispositivos, verifica la información publicada por el fabricante y, sobre todo, los permisos que requieren de tu aprobación para su funcionamiento, si observas que el acceso requerido se torna abusivo (acceso a fotos, contactos, llamadas, mensajería, configuración, etc.) es mejor que evites su descarga e instalación.

Revisa la calificación que otros usuarios han brindado sobre la aplicación que deseas descargar, este puede ser un indicio para continuar o no con el proceso.

En el caso de aplicaciones relacionadas con entidades bancarias, verifica que estas realmente hayan sido publicadas por tu entidad bancaria y no por terceras partes.

Es de vital importancia mantener instalado y actualizado un antivirus dentro de tus dispositivos, esto te ayudará a verificar el comportamiento de las aplicaciones que instalas y te pondrá en alerta en caso de detectar algún evento sospechoso.

4.13 Shoulder Surfing

(Mirar por encima del hombro)...
¡Revisa quien te acompaña!

Esta es una técnica en la cual un delincuente roba información de su víctima, lo hace simplemente mirando por encima del hombro y desde una ubicación cercana a su objetivo a ella.

Este acto puede ocurrir en la fila para acceder a un cajero automático, o también, cuando una persona está en frente de su computador o dispositivo móvil y hace uso de servicios de internet, sin percatarse que hay otra persona detrás observando lo que se está digitando en el respectivo teclado del dispositivo o computador; con lo cual, un atacante podría obtener de su víctima información confidencial y relacionada con claves de acceso a portales bancarios, correo electrónico, redes sociales, entre otros.

Para evitar ser víctima de un fraude por causa de un ataque de Shoulder surfing, ten en cuenta las siguientes recomendaciones:

- Cuando te encuentres en un lugar público o en la fila de un cajero automático, vigila tu entorno y evita que personas extrañas, que estén detrás de ti, tengan acceso visual a la actividad que estás realizando en el momento.
- En el caso de un cajero automático, al momento de digitar tu clave de acceso ten la precaución cubrir tu mano al momento pulsar las teclas, así no será visible el número que ingresaste.
- En el caso que alguien se encuentre revisando lo que haces en un tu equipo de cómputo o dispositivo móvil, no realices movimientos transaccionales y ten la precaución de hacer un cambio de contraseñas de ingreso a portales web, redes sociales, entre otros; así mismo, valida la habilitación de un segundo factor de autenticación (2FA), el cual impida el acceso no autorizado a personas que hayan descubierto tu contraseña.
- Cuando realices actividades que involucren el uso de información personal, revisa primero a tu alrededor y cerciórate que no hay nadie vigilando tus acciones.

Spam

4.14 SPAM... *¡Cuando la información no deseada es un peligro!*

Spam o correo basura, consiste en el envío de un gran número de mensajes desde internet y que llegan al buzón de correo de un usuario y sin que hayan sido solicitados por este. Por lo general, la información que se envía bajo esta modalidad corresponde a contenido de tipo publicitario y comercial, no obstante, este también puede convertirse en un medio para propagar algún tipo de malware y afectar los equipos a donde llega el mensaje.

Para evitar ser víctima de un fraude por causa de un ataque de Spam, ten en cuenta las siguientes recomendaciones:

No inscribas tu dirección de correo personal o corporativo en sitios que te ofrezcan información sobre ofertas, promociones, productos que capten tu atención, entre otros.

Realiza la creación de una cuenta de correo que te sirva como "auxiliar", con el fin de usarla para la inscripción a servicios gratuitos, de ofertas, de promociones, entre otros; que dicha cuenta se la encargada de recibir este tipo de mensajes SPAM (Basura).

Cuando revises el contenido de los mensajes en su cuenta de correo auxiliar, ten la precaución de no acceder a enlaces que conduzcan a sitios web sospechosos, no descargues ni abras archivos adjuntos que vengan en estos correos, en lo posible, si desconoces y desconfías del remitente, procede con el bloqueo de este y elimina sus mensajes.

Procura configurar en tu cliente de correo electrónico, reglas que identifiquen y bloqueen mensajes que se consideren como Spam, así evitarás que se descargue algún archivo malicioso y se instale algún tipo de malware que ponga en riesgo tu información.

Si lo consideras pertinente, ignora este tipo de mensajes y elimínalos sin llegar a revisar su contenido.

Ataque

4.15 Ataque De Fuerza Bruta...

¡Una contraseña fuerte vence a la fuerza bruta!

Este es un ataque que emplea un delincuente para la contraseña de acceso que utilizar su víctima para ingresar a un sistema, portal bancario, perfil de redes sociales, correo electrónico, entre otros; la principal característica se encuentra en el método de "Ensayo y Error", en donde el atacante utiliza distintas combinaciones de palabras, letras, números, posibles datos de su víctima o contraseñas comunes; hasta lograr el objetivo de adivinar la contraseña e ingresar de forma no autorizada a la plataforma que ha marcado como objetivo de ataque.

Se debe tener en cuenta que un delincuente siempre buscará la forma de conseguir la información confidencial de su víctima, la cual usará en la ejecución de fraudes electrónicos en contra de ella.

Para evitar ser víctima de un fraude por causa de un ataque de Fuerza bruto, ten en cuenta las siguientes recomendaciones:

- Con cierta periodicidad realiza el cambio de contraseñas en los servicios que consideres que son de gran importancia para ti y, sobre todo, que contengan información de tipo personal y confidencial.
- Construye contraseñas complejas, pero de fácil uso y recordación para ti; para esto puedes tener en cuenta los siguientes tips:

  - Emplea una longitud de mínimo diez (10) caracteres.
  - Si el sistema lo permite, haz la combinación entre letras, números y caracteres especiales (*, $, %, &, #).
  - Si el sistema al que ingresas no cuenta con la funcionalidad de cambio forzado de contraseña después de cierto tiempo, toma el hábito de hacerlo por cuenta propia y define una periodicidad de cambio de por lo menos cada 30 días.

- Por ningún motivo realices una lista en "papel" que contenga tus nuevas contraseñas, dado que estos elementos son susceptibles de dejarlos a la vista de personas extrañas.
- Tampoco construyas archivos que contengan tus nuevas contraseñas, esto si desconoces la forma de asignarles una contraseña de apertura.
- En lo posible, genera patrones que te hagan recordar tus contraseñas y así evitarás ponerlas en conocimiento de personas extrañas.
- En la medida de lo posible, habilita el uso de un segundo factor de autenticación (2FA) para acceder a tus aplicaciones.

4.16 Ataques De Diccionario...
¡Cuando la gramática no es el problema!

Este es un ataque similar al de “Fuerza bruta” y el objetivo es el mismo, la diferencia consiste en los mecanismos que utiliza el atacante para su ejecución, pues en esta modalidad se hace uso de programas (software) que se encargan de generar contraseñas de forma aleatoria o a partir de secuencias de letras, palabras, o algún parámetro de combinación que configure el atacante.

Las medidas que se pueden tomar para defenderse de este tipo de ataque son similares al ataque de “Fuerza bruta”.

Para evitar ser víctima de un fraude por causa de un ataque de Diccionario, ten en cuenta las siguientes recomendaciones:

- Con cierta periodicidad realiza el cambio de contraseñas en los servicios que consideres que son de gran importancia para ti y, sobre todo, que contengan información de tipo personal y confidencial.
- Construye contraseñas complejas, pero de fácil uso y recordación para ti; para esto puedes tener en cuenta los siguientes tips:
- Emplea una longitud de mínimo diez (10) caracteres.
- Si el sistema lo permite, haz la combinación entre letras, números y caracteres especiales (*, $, %, &, #).
- Si el sistema al que ingresas no cuenta con la funcionalidad de cambio forzado de contraseña después de cierto tiempo, toma el hábito de hacerlo por cuenta propia y define una periodicidad de cambio de por lo menos cada 30 días.
- Por ningún motivo realices una lista en “papel” que contenga tus nuevas contraseñas, dado que estos elementos son susceptibles de dejarlos a la vista de personas extrañas.
- Tampoco construyas archivos que contengan tus nuevas contraseñas, esto si desconoces la forma de asignarles una contraseña de apertura.
- En lo posible, genera patrones que te hagan recordar tus contraseñas y así evitarás ponerlas en conocimiento de personas extrañas.
- En la medida de lo posible, habilita el uso de un segundo factor de autenticación (2FA) para acceder a tus aplicaciones.

4.17 Recomendaciones Generales

Con el fin de protegerte de los ataques mencionados hasta este punto, es conveniente que tengas en cuenta un conjunto de recomendaciones adicionales, que te ayudarán a proteger tu información y defenderte de los delincuentes

- Nunca respondas a solicitudes de información personal a través de correo electrónico, mensaje de texto o vía whatsapp,el Banco nunca te solicitará por este medio los datos relacionados con contraseñas, números de tarjeta de crédito u otro tipo de información personal. Si recibes un mensaje de este tipo no lo respondas, comunícate con el banco y, por último, elimínalo.
- Al visitar sitios Web, digita la dirección (URL) en la barra de direcciones del navegador de Internet, nunca hagas clic a un enlace que te envíen a través de un correo y que te lleven a ingresar a un sitio web, ya que puede tratarse de un sitio falso.
- Cerciórate de que el sitio Web es seguro antes de ingresar cualquier tipo de información personal, compruebe si el sitio utiliza cifrado para transmitir tu información personal.
- Para comunicarte con el Banco, marca los números telefónicos publicados en el sitio web oficial.
  Nunca entregues información personal a "alguien" que llame a tu teléfono y se haga pasar como empleado del Banco.
- Cuando realices transacciones por Internet, hazlo en lugares conocidos y seguros, por ejemplo, tu casa u oficina. Evita realizarlas desde sitios públicos o computadores de acceso público.
- Nunca suministres información personal (claves secretas, números de cuentas, números de tarjetas de crédito y/o débito, documentos de identidad) a personas que te lo soliciten bajo el argumento de participar en concursos, premios o cualquier otro tipo de oferta.
- Cuando termines tus transacciones y operaciones bancarias no olvides cerrar cada sesión, nunca abandones el computador mientras estés en medio de una sesión abierta o una transacción iniciada.
- Desconfía de cualquier llamada donde te soliciten tus datos personales o confidenciales.
- Sé precavido con las llamadas donde te ofrezcan promociones, premios, descuentos, etc. no proporciones tu información personal o sensible.
- Desconfía si tu servicio de telefonía móvil no funciona correctamente por un tiempo prolongado. Llama a tu operador y verifica el estado de tu línea telefónica. En caso de que hayas sido víctima de este fraude, verifica el estado y saldo de tus productos. Si encuentras que se han realizado transacciones sin tu consentimiento, bloquea inmediatamente sus productos.

Seguridad

5. Seguridad En Línea Verde Y Banca Móvil

Teniendo en cuenta que el Banco Popular te permite realizar transacciones monetarias a través de otros canales, como son la Línea Verde y Banca Móvil, los ciberdelincuentes también buscan robar tu información y tus claves de acceso a estos canales y, así mismo, utilizarlas para realizar fraudes electrónicos en tu contra.

A continuación, te presentamos otras recomendaciones para tener en cuenta al momento de proteger tu información:

- No prestes tu celular a un desconocido, allí puedes tener información personal, bancaria como las alertas que recibes sobre las transacciones que realizas desde tu celular.
- Evita utilizar celulares ajenos para realizar operaciones telefónicas, solo inscribe números celulares sobre los cuales tengas control, para que puedas realizar tus transacciones con mayor seguridad y confianza.
- En lo posible elimina de tu celular los mensajes de alerta, que contengan información personal o financiera.
- Si realizas tus operaciones de Línea Verde a través de un teléfono con pantalla digital, verifica que la información digitada no quede almacenada en el teléfono, lo cual puedes hacerlo pulsando la tecla “Redial”.
- En caso de que alguna información quede registrada marca otro número, y así la información podrá eliminarse.
- Evita utilizar servicios telefónicos de cabinas públicas o minutos de celular en la calle, para consultas o transacciones bancarias.

  Evita utilizar el altavoz del teléfono, alguien puede escuchar tu información financiera.

6. Bloqueo De Productos Y Servicios

¡Recuerda! El Banco Popular tiene definidos canales especializados para atender tus requerimientos, consultas y solicitudes relacionadas con tus productos. Así mismo, por ningún motivo te pedirá que actualices tus datos personales o codiciones de tus productos, a través del uso de mensajes de texto, correos electrónicos o llamadas telefónicas.

A continuación, encontrarás la lista de los canales definidos por el Banco Popular para comunicarse con sus clientes, haciendo uso de distintas plataformas:

Mensajes de texto (SMS)

El Banco Popular dispone de los siguientes códigos para el envío de SMS:

85676, 87678, 87770, 890038, 899920

Líneas telefónicas

Bogotá (601) 743 46 46
Línea Nacional 01 8000 184646

Direcciones de correo electrónico (E-Mail)

extractos@bancopopular.com.co
informacion@email-bancopopular.com
popular@bancopopular.com.co
email@emailbancopopular.com

Otros medios

Red de oficinas
Chat
Contáctanos
Ingresa a www.bancopopular.com.co