BANCO POPULAR

CARTILLA DE SEGURIDAD PARA NUESTROS CLIENTES

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

Versión 1.6

GERENCIA INTEGRAL DE RIESGOS
BOGOTÁ D.C.
Octubre 2022

Cuidando nuestra casa nos protegemos todos.

CONTENIDO

Pág.

ADVERTENCIA

Las siguientes recomendaciones son tomadas de autoridades a nivel nacional e internacional. Son únicamente una guía educativa para protegerse 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 sus transacciones monetarias.

Queremos brindarle una serie de recomendaciones para el uso de sus tarjetas Débito y Crédito en cajeros automáticos, que sea más seguro y pueda 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 SKIMMING

El Skimming o Clonación, consta de la copia de la banda magnética y de la clave de la tarjeta, para esto, los delincuentes dentro de los cajeros colocan elementos tecnológicos en el lector de las tarjetas, lo que permite copiar los datos de esta. Así mismo, colocan cámaras encima del teclado, lo que les permite capturar la clave introducida por el cliente.

Por lo tanto, antes de iniciar su transacción dentro del cajero automático, tenga en cuenta las siguientes recomendaciones:

- ☐ Revise que no haya algún dispositivo extraño y que se encuentre ubicado en el lector de la tarjeta , en caso de hallarlo, evite hacer uso de este cajero y avise a la entidad bancaria.
- ☐ Realiza sus operaciones sin recibir ningún tipo de ayuda por parte de personas extrañas, en caso de requerir compañía, acuda a una persona de confianza (amigo, familiar, etc.)
- ☐ Al momento de digitar la clave en el cajero automático, cubra su mano mientras realice este proceso, evite que se vea las teclas y las pulsaciones que haga en ellas.
- ☐ Cuando realice el cambio del plástico de la tarjeta, cerciórese usted mismo de destruir la banda magnética y el microchip.
- ☐ Nunca conserve en un mismo lugar la tarjeta débito / crédito y la clave para transacciones en cajeros o datáfonos.

- Cada vez que reciba una nueva clave o la cambie, memorícela y nunca la cargue escrita en un papel o impresa en un sobreflex.
- Cambie la clave de su tarjeta periódicamente y no la escriba en un lugar cerca de la misma, ni al reverso.
- Nunca acepte ayuda con teléfonos celulares para que llame a su banco

¡Tenga en cuenta, que en la medida en que la tecnología avanza, así mismo los delincuentes actualizan sus técnicas de robo y estafas!

1.2 CAMBIAZO EN CAJEROS AUTOMÁTICOS

Este es un tipo de fraude en el cual personas externas ofrecen ayudar u orientar al cliente a realizar su retiro de dinero en un cajero automático; la excusa utilizada es que el cajero se encuentra presentando fallas técnicas al momento de efectuar la transacción. Es aquí en donde estas personas ágilmente logran ver la clave que digita el cliente, posteriormente, haciendo uso de ciertas artimañas, llevan a cabo el cambio del plástico real por otro de características similares, con ello, una vez el cliente 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 de su víctima antes que se produzca algún tipo de bloqueo de la cuenta.

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

Para evitar ser víctima de este tipo de fraudes, tenga en cuenta las siguientes recomendaciones:

- Revise y vigile que no haya personas extrañas a su alrededor al momento de realizar un retiro en cajero automático.
- Procure hacer uso, en la medida de lo posible, de cajeros automáticos que cuenten con una puerta y permitan bloquear el acceso desde adentro.
- Siempre oculte el teclado al momento de digitar su clave de acceso, esto evitar que cualquier persona la conozca e intente defraudarlo.
- Si presenta algún tipo de inconveniente con la transacción, evite pedir ayuda a las personas que se encuentren cerca a usted, tampoco acepte de estos su ofrecimiento para colaborarle con el inconveniente, es allí donde se puede presentar la oportunidad para estafarlo.
- No permita que se le acerque un tercero a ayudarle o a indicarle pasos sobre la transacción que pretende realizar.

- No pierda de vista su tarjeta y si requiere estar acompañado para realizar operaciones en cajeros automáticos, procure que sean personas conocidas y de mucha confianza.
- Cuando finalice la transacción, por precaución, valide que en la tarjeta estén registrado su nombres y apellidos o esté firmada por usted.
- Por ningún motivo preste su tarjeta ni divulgue su clave.
- Si observa cualquier situación sospechosa en el cajero no realice la transacción.
- Si debe salir rápidamente de un cajero electrónico, presione la tecla cancelar.
- Nunca acepte ayuda con teléfonos celulares para que llame a su banco.

2. SEGURIDAD EN ESTABLECIMIENTOS COMERCIALES

Otro escenario para ser víctima de fraudes con tarjeta débito/Crédito es cuando se realiza compras en establecimientos comerciales a través de este medio.

A continuación, conocerá 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 devolverle la tarjeta se la cambian con otra similar, de otro cliente al que han estafado o una falsa. Posteriormente, vigilan al cliente al momento de digitar su clave cuando está autorizado el cargo a su tarjeta, esta es memorizada o anotada por el delincuente y junto con la tarjeta que ha cambiado, procede a realizar retiros o avances desde la cuenta o producto del cliente.

Para evitar ser víctima de este tipo de hurto, tenga en cuenta las siguientes recomendaciones:

- Cuando vaya a realizar una compra en establecimientos comerciales con cualquiera de sus tarjetas, entréguela únicamente al encargado de hacer la transacción en la caja y no lo pierda de vista a él, ni a su tarjeta.
- Nunca permita que deslicen su tarjeta en dispositivos diferentes a los definidos para el pago (Ej. Datáfonos).
- Siempre verifique el monto de la compra, si requiere cerciorarse, solicite copia del voucher de compra y verifique.

- Cuando digite la clave cubra el teclado numérico de tal forma que nadie lo pueda ver.
- No olvide reclamar su tarjeta después de realizar el pago.
- Destruya los comprobantes de pago de sus compras, antes de arrojarlos a la basura.
- Valide que en la tarjeta que le entregan estén registrados sus nombres y apellidos o esté firmada por usted.
- Si su tarjeta cuenta con tecnología “contactless”, usted puede efectuar todo el proceso del pago de la compra sin tener que entregar el plástico.

3. SEGURIDAD EN RED DE OFICINAS BANCARIAS

Otro escenario utlizado por los delincuentes para la realización de fraudes a los clientes, es una oficina bancaria. 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, conocerá algunas modalidades usadas por los delincuentes para defraudar a un cliente que se encuentra dentro de una oficina bancaria, realizando algún tipo de operaciónen 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 una 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 ser víctima de esta modalidad de hurto, tenga en cuenta las siguientes recomendaciones, analizando muy bien los diferentes momentos que harán parte de las transacciones que realice en una oficina bacaria:

- Valide con la entidad los tipos de transacciones que esta le ofrece, en lo posible evite el manejo de grandes sumas de dinero y que deba desplazarse hasta una oficina bancaria.

- Si necesita realizar el pago de una obligación con la entidad o un tercero, explore 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 tener que realizar su transacción en una oficina bancaria, evite comentar o mencionar el detalle de la operación a realizar, a personas que no sean de su entera confianza.
- Estando dentro de una oficina bancaria, revise constantemente su entorno, las personas que lo rodean, evite entablar conversaciones mientras está esperando a ser atenido por un cajero en la ventanilla respectiva.
- Cuando sea llamado por un cajero, procure estar solo en la ventanilla y no permita que personas extrañas se acerquen a su lado mientras usted realiza su transacción en efectivo.
- En caso de realizar un retiro en efectivo, tenga presente el ser muy discreto mientras está verificando el monto recibido por parte del cajero, cuando finalice, guarde el dinero de forma segura.
- En caso de tratarse de una gran suma de dinero la que está retirando por ventanilla, solicite el servicio de escolta de la policía antes de retirarse de la oficina bancaria.
- Para el caso de depósitos en efectivo, entregue el dinero únicamente al cajero de ventanilla cuando este lo llame por su turno.
- No entregue su dinero a personas que se acercan a usted 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 su dinero en efectivo.
- Procure llegar a la entidad con los formatos de consignación, o retiro, debidamente diligenciados, evite 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 aborde vehículos de transporte ubicados al frente de esta, procure tomarlos en un sitio diferente.
- Cambie su rutina de desplazamiento y así evitará ser “perfilado” por un delincuente.
- En caso de que perciba que está siendo perseguido, ubique prontamente una estación de policía y exponga su situación.
- Por último, si termina siendo víctima de un hurto después de abandonar la oficina bancaria, no exponga su integridad física ni ponga resistencia, intente memorizar las características de las personas que lo atacan, para que después los pueda denunciar a las autoridades.
- Siempre piense en resguardar su seguridad personal y de las personas que lo acompañen.

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, tenga en cuenta las siguientes recomendaciones:

- ☐ Verifique si su cheque tiene restricción de pago “únicamente al primer beneficiario”
- ☐ Si lo anterior es afirmativo, verifique si tiene algún tipo de cruce para consignar en cuenta de primer beneficiario o si es posible su cobro en ventanilla.
- ☐ Cuando necesite cambiar un cheque por efectivo, procure hacer con tiempo y sin endosos a terceras personas que no tengan relación con usted, puede verse involucrado en un fraude.
- ☐ Procure consignar a su cuenta bancaria los cheques recibidos.
- ☐ No sea parte de un fraude al entregar un título valor a un tercero, de quién no guarde relación con usted o sus actividades.
- ☐ Ante la imposibilidad de realizar el cobro de un cheque por ventanilla, valide 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. Es aquí cuando el cliente se confía de esta persona

y termina entregándole el dinero que lleva para realizar su transacción en ventanilla a cambio de recibir el comprobante de recibido y 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, tenga en cuenta las siguientes recomendaciones:

- ☐ Cuando llegue a una oficina bancaria a realizar consignaciones o pagos en efectivo, no ponga al descubierto el dinero correspondiente a la transacción.
- ☐ Evite 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.
- ☐ Procure presentarse a la oficina con los comprobantes diligenciados, ya sea un pago o consignación en efectivo.
- ☐ Disponga de un tiempo considerable para realizar este tipo de operaciones, tenga presente que se puede presentar situaciones relacionadas con alto flujo de clientes o fallas en los sistemas de la oficina, lo cual puede ocasionarle algunas demoras para ser atendidos.
- ☐ Por ningún motivo acepte 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, puede tratarse de personas ajenas a la entidad que buscan ganar su confianza y hurtar su dinero.
- ☐ No olvide que los únicos autorizados para recibir dinero en efectivo son los cajeros por ventanilla, no caiga en la trampa de personas que le prometan ahorrarse tiempo haciendo la fila.
- ☐ Tenga paciencia y espere el llamado del cajero para ser atendido.
- ☐ Si evidencia alguna situación anormal o que se presenta alguna situación de las mencionadas anteriormente, avise inmediatamente al Gerente o Director administrativo de la oficina, para que tomen las medidas correspondientes.
- ☐ No solicite ni reciba ayuda de extraños, solicítela únicamente a personal de la entidad.
- ☐ Al realizar trámites con cierta periodicidad, evite crear rutinas que permitan conocer días, y horarios de sus 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. SEGURIDAD EN CANALES DIGITALES (INTERNET)

Dada la evolución que ha tenido el uso de los servicios digitales al momento de realizar operaciones bancarias, así mismo, los delincuentes han desarrollado técnicas para estafar más clientes y con menor grado de exposición, ellos han encontrado en el uso de internet una fuente de mayores ingresos que los delitos presenciales en oficinas bancarias o cajeros automáticos. A continuación, encontrará algunas pautas que le permitirá conocer modalidades de estafa y así evitará ser víctima de posibles robos de información y dinero a través de canales digitales:

4.1 ROBO DE IDENTIDAD DIGITAL

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 un descuido por parte de esta, es por esto por lo que una persona debe prestar mucha atención al entorno que la rodea, cada vez que haga algún tipo de diligencia fuera de su casa o lugar de trabajo, procurar utilizar conexiones seguras para acceder a contenidos en internet, evitar ingresar a páginas web que puedan comprometer la seguridad de su dispositivo y la información almacenada en estos. Por lo tanto, tenga en cuenta que puede ser víctima en situaciones como:

- Robo de su billetera o bolso le puede ocasionar la pérdida de su información personal, dinero y tarjetas débito/crédito.
- Realizar transacciones en cajero automáticos y no percatarse del estado de este; puede caer en la trampa de “Skimming” (mencionada anteriormente).
- Robo de información personal en la propia casa o la que recibe a través de correspondencia urbana; es conveniente que deseche y destruya adecuadamente los documentos que considere que no son relevantes; en lo posible, tome el hábito de administrar su correspondencia a través de correo electrónico y no por medio físico.
- No mantener actualizado y asegurado el dispositivo con el cual accede a internet, puede ser víctima de la instalación silenciosa de un software malicioso, producto del acceso a páginas inseguras o la apertura y ejecución de contenidos inmersos en correos de dudosa procedencia.

- Hacer uso de software ilegal para la configuración de sus distintos dispositivos, lo que puede ocasionar la generación de brechas de seguridad por las cuales el delincuente podría tomar control remoto del dispositivo, robar la información de su víctima y cometer fraudes electrónicos en contra de esta.

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

- Suplantar su identidad con el fin de abrir cuentas bancarias, solicitar tarjetas de crédito o préstamos en su nombre.
- Suplantar su identidad con el fin de adquirir planes y servicios de telefonía celular.
- Usar su información que ha sido robada, con el objetivo de falsificar tarjetas débito / crédito.
- Realizar transferencias electrónicas sin tener su consentimiento como titular de una cuenta.
- Registrarse en canales digitales que no son frecuentados por la persona afectada.
- Registrar otros dispositivos electrónicos para acceder a las aplicaciones móviles bancarias.

Para evitar ser víctima de fraudes electrónicos por causa del robo de su identidad digital, tenga en cuenta las siguientes recomendaciones:

- No pierda de vista los objetos personales que contengan información que lo puedan identificar (Bolsos, billeteras, documentos, entre otros).
- Deseche adecuadamente la información que no considera necesaria, en caso de ser física, destrúyala minuciosamente antes de arrojarla a la basura.
- Cambie constantemente el pin de acceso para sus tarjetas débito/crédito, nunca use el mismo pin para estos productos y menos si son de diferentes entidades bancarias.
- Cambie las contraseñas de acceso a sus cuentas de correo electrónico, perfiles de redes sociales, portales bancarios, entre otros. Tome el hábito de realizar este cambio en un lapso no mayor a 60 días.
- Cuando interactúe con su información personal en internet, hágalo siempre conectándose a redes seguras y en sitios de confianza (casa propia, lugar de trabajo, etc.), evite conectarse a redes inalámbricas (Wifi) públicas y sin protección, lo mismo, en lugares como plazoletas, sitios de “café internet”, o espacios públicos que ofrezcan conexión gratuita a internet.
- Mantenga actualizados sus dispositivos móviles y de cómputo, incluya el uso de un antivirus reconocido y legal, que se encargue de verificar la limpieza de sus archivos y evitar la instalación de software malicioso.

4.2 INGENIERÍA SOCIAL

La ingeniería social es un método muy utilizado por los delincuentes para realizar el robo de identidad a sus víctimas, esta práctica permite obtener información confidencial a través de la manipulación de las personas; el delincuente usará comúnmente la comunicación telefónica, el envío de correos electrónicos maliciosos u otros métodos; cuyo 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 su información, tenga en cuenta las siguientes recomendaciones:

- Nunca entregue su información personal a personas extrañas que se comuniquen con usted a través de correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales.
- Sea precavido con la información que comparte y publica en sitios de redes sociales, active y personalice las configuraciones de privacidad; tenga presente que esta es una de las fuentes predilectas de los delincuentes para realizar un “perfilamiento” de sus víctimas.
- Cuando sea abordado para ofrecerle algún tipo de servicio bancario, esté muy atento a las preguntas que le realizan y piense muy bien las respuestas que brinda; recuerde que de eso trata la ingeniería social, de como “trabajar a la persona” para que suministre su información confidencial inconscientemente.
- Para los servicios que utilice en internet, procure asignar contraseñas seguras y robustas y evite utilizar una misma contraseña para más de una plataforma.
- Adopte hábitos de cambio y asignación de nuevas contraseñas con cierta periodicidad, cuyos lapsos no sean muy extensos.
- En la media que le sea posible, habilite la opción de autenticación en dos pasos para el ingreso a portales bancarios, correos electrónicos, redes sociales y todo aquel servicio que considere sensible para el manejo de su información.

4.3 PHISHING

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 su 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, tenga en cuenta las siguientes recomendaciones:

- ☐ Identifique muy bien los remitentes de sus correos electrónicos, si recibe mensajes con información o contenido y que no guarde relación con usted, evite abrirlos y ejecutar cualquier tipo de enlace web o archivos adjuntos.
- ☐ Si recibe mensajes de parte de una supuesta entidad financiera para pedirle que actualice sus datos haciendo clic en un enlace, tenga cuidado en caer en un engaño, recuerde que ninguna entidad bancaria pide a sus clientes que realicen este proceso y mediante estos canales de comunicación; adicionalmente, recuerde que usted es el dueño de su información y podrá actualizarla cada vez que lo considere necesario.
- ☐ Evite ingresar a portales bancarios por medio de enlaces web que reciba a través de correos electrónicos, estos atajos lo pueden conducir a páginas falsas que suplantan la identidad de entidades legítimas, con el finde engañar a sus víctimas y así robar su información.
- ☐ Mantenga actualizado su computador y dispositivo móvil, implemente herramientas como un antivirus, que le ayude a revisar y bloquear el acceso a páginas que se consideren como inseguras.
- ☐ Haga un monitoreo frecuente sobre el monitoreo de sus cuentas bancarias, perfiles de redes sociales y toda fuente que considere que tenga información confidencial; en caso de
- ☐ Ante la duda de saber si el mensaje recibido es legal o fraudulento debido a que desconoce su procedencia, evite abrirlo y, si lo hace, ejecutar algún tipo de enlace o archivo que esté

adjunto; puede tratarse de un ataque de phishing que ponga en riesgo su información confidencial.

- ☐ Procure estar informado en temas de seguridad y ciberseguridad, esto le ayudará a entender mucho mejor los riesgos a los que se expone su información cada vez que se cae en este tipo de engaños.

Recuerde que, con sus datos, un delincuente puede cometer fraudes electrónicos en su contra o de otras personas, podría verse envuelto en posibles delitos informáticos al no reportar inmediatamente a las autoridades el posible robo de sus datos.

4.4 VISHING

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 “guion” muy bien estructurado en la llamada que hace a su víctima, suobjetivo 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 de mensajes falso a su telefóno celular) 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 o clave de línea verde; bajo el supuesto objetivo de evitar el bloqueo de alguno de sus productos o el ofrecimiento de apertura de otros nuevos.

Una vez que el delincuente obtiene la inforamación 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.

Tenga en cuenta las distintas situaciones que se pueden presentar en este tipo de llamadas:

- ☐ Se escucha una grabación que alerta a la persona sobre su cuenta bancaria, tarjeta de crédito, etc., indicándole que está siendo utilizada de forma fraudulenta y que debe llamar al número telefónico que le indican inmediatamente, este número telefónico puede ser una línea gratuita falsa de la compañía financiera que se pretende suplantar.

- Se presenta una persona haciéndose pasar por agente de la entidad financiera, comunicando el trámite de devolución del IVA o del 4X1000, e indicando que para hacer efectivo el procedimiento, deberá el cliente indicar o digitar la clave que le acaba de llegar por mensaje de texto al celular.
- Se presenta una persona haciéndose pasar por agente de la entidad financiera, informando sobre un posible fraude en sus productos financieros o comunicando la existencia de un token “duplicado”, es por esto que, para gestionar el bloqueo de estas irregularidades, dicha persona le solicita al cliente que le diga o digite la clave de su token, de sus productos o del mensaje de texto que le llegará a su celular.

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

- Preste mucha atención a la conversación y y a la información que le brindan y le solicitan.
- Es posible que el delincuente conozca algunos de sus datos personales, si le pide que se los confirme o complemente, no lo haga, valide con la persona el “por qué” y “para qué” de su solicitud.
- Recuerde que el banco no lo llamará para solicitarle datos personales y confidenciales.
- Si la llamada le genera dudas o sospechas, lo más conveniente es que la termine y se comunique de inmediato con el banco.
- No presione botones o digite números que le soliciten en la llamada
- Procure obtener la identidad de la persona que lo está contactando.
- Tome nota de los detalles de la llamada, pero por ningún motivo entregue sus datos.

4.5 MALWARE (Programa Malicioso)

Son programas o archivos dañinos para los computadores, diseñados para infectarlos con virus, Spyware, troyanos, entre otros; el propósito de estos, una vez se han instalado en los dispositivos comprometidos, es recolectar información de todo tipo y que se relacione con el usuario y equipo comprometido. 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 a descargue el archivo y lo ejecute, o que haga clic en enlace y acceda a un sitio malicioso, allí la persona puede caer en el engaño y entregar su información confidencial o infectar su dispositivo. Una vez se

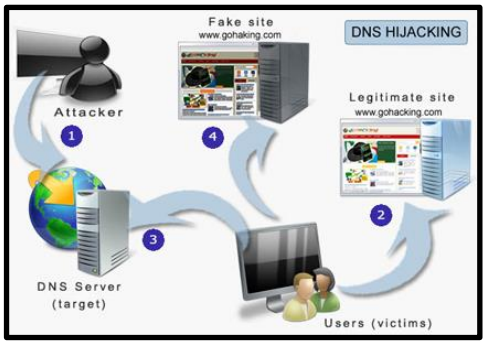
ejecuta este programa y se instala en el equipo de la víctima y, dependiendo su función, puede robar información personal, monitorear las actividades que el usuario realiza en su equipo, o tomar control remoto del dispositivo para realizar más ciberataques en contra de la misma persona u otras.

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, tenga en cuenta las siguientes recomendaciones:

- Es importante que instale un antivirus en los dispositivos que utiliza para realizar sus operaciones en internet; así mismo, procure 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 abra archivos adjuntos que provengan de remitentes que desconozca, si no es posible la comprobación de su origen, es preferible que elimine el mensaje.
- Ejecute análisis programados a través de su herramienta de antivirus, para el escaneo de sus dispositivos móviles y de cómputo.
- Procure mantener actualizados sus 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 utilice.
- Habilite condiciones de seguridad en la conexión que realice a una red WIFI, existen parámetros de cifrado que contribuyen a garantizar el manejo de los datos (Ej. WPA2).
- Evite conectarse y navegar en redes WIFI que sean públicas y abiertas, estas no poseen condiciones de seguridad y podrían exponer su información ante los delincuentes informáticos.
- Procure hacer uso de contraseñas seguras e independientes una de la otra, cada vez que de requiera acceder a servicios alojados en la web (Ej. Redes sociales, correo electrónico, portales bancarios, entre otros).
- Procure realizar una copia segura de sus archivos, en caso de verse afectado por una infección de malware.

4.6 HIJACKING



Conocido como “Secuestrador de navegadores”, es un malware que puede considerarse como “poco peligroso” pero sus acciones finales pueden llegar a serlo; ya que su objetivo principal es redirigir a sus víctimas hacia páginas falsas o maliciosas, la cuales podrían robar la información confidencial de un usuario si este cayera en el engaño.

Cuando un equipo se encuentra afectado por este malware, al momento de abrir el navegador predeterminado en el equipo, su motor de búsqueda ha sido reemplazado por una página maliciosa (Ej. Cambia la página del buscador de Google por un buscador falso), así mismo, esta amenaza le impedirá al usuario restablecer su página de inicio dentro de su navegador.

Existen otros tipos de Hijacking como “Secuestro de dominio web” (El atacante logran apoderarse del registro de un dominio legal, para luego estafar a sus víctimas), “Secuesto de URL” (Se reemplaza una URL legítima por una falsa dentro de la lista de resultados que arroja un motor de búsqueda, así una víctima podría seleccionar una página falsa que se encuentra en el primer lugar),

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

- Ponga mucha atención cuando ingrese a una página web, salga inmediatamente de esta si observa que se abren diversas ventanas de distintas fuentes, o si empieza a realizarse la descarga e instalación de algún tipo de software, el cual resulta malicioso en la mayoría de los casos.
- Utilice dentro de sus dispositivos un antivirus que tenga funciones de control de tráfico de red, el cual se encargará de detectar y bloquear la conexión a una dirección web cuya IP es maliciosa.
- Mantenga actualizado su equipo y la solución de antivirus (legal) que tenga instalado en este.
- Evite el ingreso a páginas web que ofrezcan servicios gratuitos, descargas de aplicaciones manipuladas para su activación, entre otras; podría ser víctima de este tipo de malware.
- Procure digitar dentro del navegador la dirección web a la cual desea acceder, tenga en cuenta que los resultados que arroja un motor de búsqueda pueden ser alterados, lo que conlleva a que ingrese a un sitio malicioso al momento de hacer clic en este registro.

4.7 SIM SWAPPING

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, tenga en cuenta las siguientes recomendaciones:

- ☐ Cuide muy bien los datos que lo 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.
- ☐ Haga una revisión de los posibles sitios en donde haya registrado los datos mencionados, elimínelos de aquellas aplicaciones o perfiles a los cuales ya no accede o que simplemente no es necesario que tengan esta información.
- ☐ Revise su dispositivo móvil y evite guardar en este todos los datos confidenciales y que lo puedan identificar, recuerde que con ellos los delincuentes pueden robar su identidad y cometer fraudes en su nombre.
- ☐ Procure instalar en su dispositivo móvil una aplicación (segura) que le sirva de “bloqueo de acceso”, con ello podrá proteger aún más sus datos personales y las aplicaciones sensibles.
- ☐ Con cierta periodicidad, valide con su operador de telefonía móvil si en un lapso determinado se han registrado requerimientos de reexpedición de tarjeta SIM, en caso afirmativo, verifique que corresponde a solicitudes que usted ha hecho o, de lo contrario, solicite urgentemente un cambio de la tarjeta y el bloqueo de las otras que puedan estar activas.
- ☐ Si es hurtado su teléfono móvil, solicite a su operador de servicio de telefonía que bloquee el IMEI del teléfono.
- ☐ En caso de ser posible, realice de forma remota el bloqueo y borrado de información del dispositivo.
- ☐ Acuda a las autoridades e informe sobre este hecho para radicar un denuncio.
- ☐ No descuide sus datos personales, estos pueden ser utilizados fraudulentamente en su contra.

4.8 SMISHING

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, tenga en cuenta las siguientes recomendaciones:

- Si recibe un mensaje de texto cuyo remitente no conoce o considera sospechoso, no lo responda ni interactúe con el contenido inmerso en este.
- No ingrese 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 le solicitan a través de un mensaje de texto actualizar sus datos o ingresar contraseñas de alguno de sus productos, informe inmediatamente al Banco sobre este evento y posteriormente elimine el mensaje, por ningún motivo suministre la información que le solicitan.
- Ante mensajes de texto que informen sobre algún bloqueo o restricción de alguno de sus productos, no realice ninguna acción de respuesta ni suministre información confidencial, solo comuníquese inmediatamente con el Banco a través de los canales autorizados y los cuales puede consultar en la página www.bancopopular.com.co.

4.9 BATING O CEBO

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, tenga en cuenta las siguientes recomendaciones:

- ☐ No recoja dispositivos de almacenamiento externo, los cuales se encuentren abandonados en los sitios mencionados.
- ☐ Si uno de estos elementos capta su atención, por ningún motivo lo conecte a su dispositivo personal o corporativo; puede ser víctima de la descarga e instalación de un software malicioso, el cual es utilizado por un delincuente para el robo de su información o de la empresa en la que labora.
- ☐ En lo posible, destruya este tipo de elementos y así evitará que otras personas caigan en este tipo de engaño.
- ☐ Ante la conexión de dispositivos de almacenamiento externo en su equipo de cómputo o tableta; mantenga instalada y actualizada una herramienta de antivirus que se encargue de revisar el contenido de estos elementos.
- ☐ Procure deshabilitar la reproducción automática de los dispositivos de almacenamiento externo, esto evitará que se ejecute de forma autónoma cualquier tipo de software malicioso.

4.10 DUMPSTER DIVING (Husmear en la basura)

Esta es una técnica donde el delincuente estará muy atento a los documentos que su víctima arroja a la basura. Su objetivo es revisar minuciosamente los elementos encontrados y analizar si la información que halló le sirve para diseñar y ejecutar algún tipo de fraude en contra de la persona que la arrojó a la basura.

Es por esto que se debe prestar mucha atención a la información que se arroja a la basura y, sobre todo, la forma en que se ejecuta esta acción, ya que se podría encontrar información sensible de la persona como lo son sus datos bancarios (números de tarjetas, cuentas bancarias), claves de acceso a portales web o aplicativos personales/corporativos, direcciones de correo electrónico, o cualquier tipo de dato que la identifique y la relacione con algo que le permita generar fraudes electrónicos.

Tenga en cuenta, que un delincuente siempre le encontrará valor a la información que su víctima descuide o no proteja adecuadamente.

Para evitar ser víctima de un fraude por causa de un ataque de Dumpster Diving, tenga en cuenta las siguientes recomendaciones:

- Revise muy bien los documentos o papeles que va arrojar a la basura, verifique que no exista información que se relacione con usted o lo identifique.
- Si recibe información impresa sobre sus productos bancarios, no la deje en lugares visibles y a disposición de cualquier persona, tenga presente que esta es información personal y confidencial.
- Cuando desee eliminar la información impresa, destrúyala adecuadamente y de forma tal que no se pueda reconstruir algún dato; para ello, haga cortes muy diminutos de cada papel, para ello utilice sus propias manos, una picadora de papel, unas tijeras, entre otros.
- Cuando arroje a la basura sobres de correspondencia, revise primero que sus datos personales (nombres, dirección, identificación, etc.) no se encuentren impresos o visibles, en caso de ser así, raye o tache esta información y ahí si arrójelo a la papelera.
- Evite acumular demasiada información impresa en lugares que sean de fácil acceso para distintas personas, lo más aconsejable es que elimine esta información en la medida que ya no requiera de ella.
- Siempre preste atención a lo que está arrojando a la basura, recuerde que puede existir información que sea de gran utilidad para un delincuente, con ella podría realizar fraudes en su contra; por ello, procure recibir su información a través de correo electrónico.

4.11 ROGUEWARE

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, tenga en cuenta las siguientes recomendaciones:

- Instale un antivirus legal en cada uno de los dispositivos que utiliza para navegar en internet, verifique que se actualice a diario y así evitar infecciones por nuevas amenazas.
- Mantenga actualizado el sistema operativo y las aplicaciones de sus dispositivos, en caso de no hacerlo, podría verse afectado por una brecha de seguridad que podría ser explotada por un atacante.
- Sea cauteloso con las páginas que consulta en internet, algunos sitios maliciosos toman la apariencia de sitios “auténticos” para engañar a las víctimas y poder robar su información.
- Constantemente haga una limpieza de archivos temporales e historial de navegación en los equipos de cómputo.
- Configure tareas programadas en su herramienta de antivirus, con el fin de realizar un escaneo profundo de su dispositivo por lo menos tres (3) veces por semana.
- Evite la descarga de programas y archivos que se encuentren en páginas sospechosas, recuerde que un malware se puede instalar de forma silenciosa.
- Proteja su información confidencial a través del uso de contraseñas o aplicaciones que permitan realizar bloqueos de acceso en sus dispositivos.

4.12 APLICACIONES MALICIOSAS

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, tenga en cuenta las siguientes recomendaciones:

- ☐ Descargue e instale aplicaciones que provengan de tiendas oficiales como App Store – Apple, Play Store – Google, Microsoft Store, entre otras.
- ☐ Evite descargar aplicaciones de sitios web que le ofrezcan productos aparentemente “licenciados y legales”, esto podría tratarse de una estafa que terminaría en el robo de su información personal y confidencial.
- ☐ Al momento de instalar una aplicación en sus dispositivos, verifique la información publicada por el fabricante y, sobre todo, los permisos que requiere aprobación por parte del usuario para su funcionamiento, si observa que el acceso requerido se torna abusivo (acceso a fotos, contactos, llamadas, mensajería, configuración, etc.) es mejor que evite su descarga.
- ☐ Revise la calificación que otros usuarios han brindado sobre la aplicación que desea descargar, este puede ser un indicio para continuar o no con el proceso.
- ☐ En el caso de aplicaciones relacionadas con entidades bancarias, verifique que estas realmente fueron publicadas por la entidad que desea y no por terceras partes.
- ☐ Es de vital importancia mantener instalado y actualizado un antivirus dentro de sus dispositivos, este le ayudará a verificar el comportamiento de las aplicaciones que instala y lo pondrá en alerta en caso de detectar algún evento sospechoso.

4.13 SHOULDER SURFING (Mirar por encima del hombro)

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, tenga en cuenta las siguientes recomendaciones:

- Cuando se encuentre en un lugar público o en la fila de un cajero automático, vigile su entorno y evite que personas extrañas, que estén detrás de usted, tengan acceso visual a la actividad que está realizando en el momento.
- En el caso de un cajero automático, al momento de digitar la clave de acceso tenga la precaución cubrir su mano al momento pulsar las teclas, así no será visible el número que ingresó.
- En el caso que alguien se encuentre revisando lo que usted hace en un computado o dispositivo móvil, tenga la precaución de hacer un cambio de las contraseñas de ingreso a portales web, redes sociales, entre otros; así mismo, valide la habilitación de un segundo factor de autenticación (2FA), el cual impida el acceso no autorizado de personas que hayan descubierto su contraseña.
- Cuando realice actividades que involucren el uso de información personal, revise primero a su alrededor y cerciórese que no hay nadie vigilando sus acciones.

4.14 SPAM

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, tenga en cuenta las siguientes recomendaciones:

- No inscriba su dirección de correo personal o corporativo en sitios que le ofrezcan información sobre ofertas, promociones, productos que capten su atención, etc.
- Realice la creación de una cuenta de correo que le 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 re recibir este tipo de mensajes SPAM (Basura).
- Cuando revise el contenido de los mensajes en su cuenta de correo auxiliar, tenga la precaución de no acceder a enlaces que conduzcan a sitios web sospechosos, no descargue ni abra archivos adjuntos que vengan en estos correos, en lo posible, si desconoce y desconfía del remitente, proceda con el bloqueo de este y elimine sus mensajes.
- Procure configurar en su cliente de correo electrónico reglas que identifiquen y bloqueen mensajes que se consideren como Spam, así evitará que se descargue algún archivo malicioso y se instale algún tipo de malware que ponga en riesgo su información.
- Si lo considera pertinente, ignore este tipo de mensajes y elimínelos sin llegar a revisar su contenido.

4.15 ATAQUE DE FUERZA BRUTA

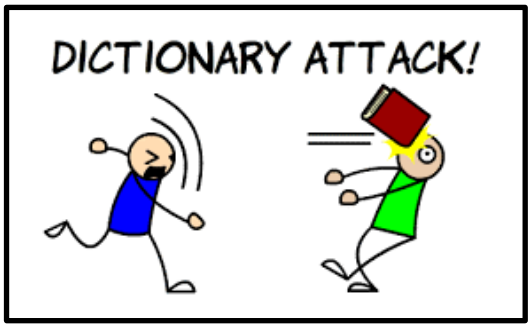
Este es un ataque que emplea un delincuente para la contraseña de acceso que utilizar su víctima para ingresar a un sistema, portal bancario, perfil de redes sociales, correo electrónico, entre otros; la principal característica se encuentra en el método de “Ensayo y Error”, en donde el atacante utiliza 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, tenga en cuenta las siguientes recomendaciones:

- Con cierta periodicidad realice el cambio de contraseñas en los servicios que considere de gran importancia para usted y, sobre todo, contengan información de tipo personal y confidencial.
- Construya contraseñas complejas, pero de fácil uso y recordación para usted; para esto puede tener en cuenta los siguientes parámetros:
  - Emplee una longitud de mínimo ocho (8) caracteres.
  - Si el sistema lo permite, haga la combinación entre letras, números y caracteres especiales (*, $, %, &, #).
  - Si el sistema al que ingresa no cuenta con la funcionalidad de cambio forzado de contraseña después de cierto tiempo, tome el hábito de hacerlo por cuenta propia y defina una periodicidad de cambio de por lo menos cada 30 días.
- Por ningún motivo realice una lista en “papel” que contenga sus nuevas contraseñas, dado que estos elementos son susceptibles de dejarlos a la vista de personas extrañas.
- Tampoco construya archivos que contenga sus nuevas contraseñas, si desconoce la forma de asignar una contraseña de apertura.
- En lo posible, genere patrones que le hagan recordar sus contraseñas y así evitará ponerlas en conocimiento de personas extrañas.
- En la medida que sea posible, habilite el uso de un segundo factor de autenticación (2FA) para acceder a sus aplicaciones.

4.16 ATAQUES DE DICCIONARIO



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.

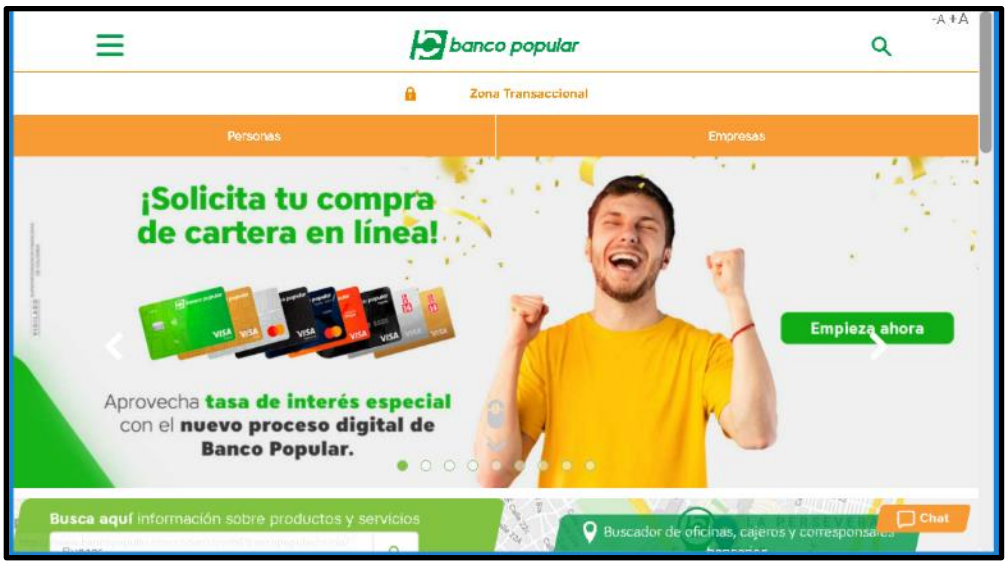
Las medidas que se pueden tomar para defenderse de este tipo de ataque son similares al ataque de “Fuerza bruta”.

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

- ☐ Con cierta periodicidad realice el cambio de contraseñas en los servicios que considere de gran importancia para usted y, sobre todo, contengan información de tipo personal y confidencial.
- ☐ Construya contraseñas complejas, pero de fácil uso y recordación para usted; para esto puede tener en cuenta los siguientes parámetros:
  - ✎ Emplee una longitud de mínimo ocho (8) caracteres.
  - ✎ Si el sistema lo permite, haga la combinación entre letras, números y caracteres especiales (*, $, %, &, #).
  - ✎ Si el sistema al que ingresa no cuenta con la funcionalidad de cambio forzado de contraseña después de cierto tiempo, tome el hábito de hacerlo por cuenta propia y defina una periodicidad de cambio de por lo menos cada 30 días.
- ☐ Por ningún motivo realice una lista en “papel” que contenga sus nuevas contraseñas, dado que estos elementos son susceptibles de dejarlos a la vista de personas extrañas.
- ☐ Tampoco construya archivos que contenga sus nuevas contraseñas, si desconoce la forma de asignar una contraseña de apertura.
- ☐ En lo posible, genere patrones que le hagan recordar sus contraseñas y así evitará ponerlas en conocimiento de personas extrañas.
- ☐ En la medida que sea posible, habilite el uso de un segundo factor de autenticación (2FA) para acceder a sus aplicaciones.

4.17 RECOMENDACIONES GENERALES

Con el fin de protegerse de los ataques mencionados hasta este punto, es conveniente que tenga en cuenta un conjunto de recomendaciones adicionales, que le ayudarán a proteger su información y defenderse de los delincuentes:



- Nunca responda a solicitudes de información personal a través de correo electrónico. El Banco nunca solicita por este medio datos relacionados con contraseñas, números de tarjeta de crédito u otro tipo de información personal. Si recibe un mensaje de este tipo no lo responda, notifique comuníquese con el banco y, por último, elimínelo.
- Al visitar sitios Web, digite la dirección (URL) en la barra de direcciones del navegador de Internet, nunca haga clic a un enlace que le envíen a través de un correo y que lo induzcan a ingresar a un sitio web, ya que puede tratarse de un sitio falso.
- Cerciórese de que el sitio Web es seguro, antes de ingresar cualquier tipo de información personal, compruebe si el sitio Web utiliza cifrado para transmitir la información personal.
- Para comunicarse con su entidad financiera, marque los números telefónicos publicados en los sitios web oficiales.
- Nunca entregue información personal a “alguien” que llame a su teléfono. Si cree que es necesario retorne la llamada a los números de confianza.
- Cuando realice transacciones por Internet, realícelas desde sitios conocidos, por ejemplo, su casa o su oficina. Evite realizarlas desde sitios públicos, como Café Internet o Computadores de acceso público.
- Nunca suministre información personal (claves secretas, números de cuentas, números de tarjetas de crédito y/o débito, documentos de identidad) a personas que se lo soliciten bajo el argumento de participar en concursos, premios o cualquier otro tipo de oferta.

- Cuando termine sus transacciones y operaciones cierre cada sesión, nunca abandone el computador mientras esté en medio de sesión abierta o una transacción iniciada.
- Desconfíe de cualquier llamada donde le soliciten sus datos personales o confidenciales.
- Sea precavido con las llamadas donde le ofrecen promociones, premios, descuentos, etc. no proporcione su información personal o sensible a cambio de estos.
- Desconfíe si su servicio de telefonía móvil no funciona correctamente por un tiempo prolongado. Llame a su operador y verifique el estado de su línea telefónica. En caso de que haya sido víctima de este fraude, verifique el estado y saldo de sus productos. Si encuentra que se han realizado transacciones sin su consentimiento, bloquee inmediatamente sus productos.

5. SEGURIDAD EN LÍNEA VERDE Y BANCA MÓVIL

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

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

- No preste su celular a un desconocido, allí usted puede tener información personal, como las alertas que recibe sobre las transacciones que realiza desde su celular.
- Evite utilizar celulares ajenos para realizar operaciones telefónicas, solo inscriba números celulares sobre los cuales tenga control de estos, para que pueda realizar sus transacciones con mayor seguridad y confianza.
- En lo posible elimine de su celular los mensajes de alerta, que contengan información personal o financiera, una vez hayan sido leídos por usted.
- Si realiza sus operaciones de Línea Verde a través de un teléfono con pantalla digital, verifique que la información que digitó no quede almacenada en el teléfono, lo cual puede verificar pulsando la tecla “Redial”. En caso de que alguna información quede registrada marque otro número, y así la información podrá eliminarse.
- Evite utilizar servicios telefónicos de cabinas públicas o minutos de celular de la calle para consultas o transacciones bancarias.
- Evite utilizar el altavoz del teléfono, alguien puede escuchar su información financiera.

6. BLOQUEO DE PRODUCTOS Y SERVICIOS

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

A continuación, encontrará 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

Direcciones de correo electrónico (E-Mail)

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

Líneas telefónicas

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

Otros medios

- Red de oficinas
- Chat
- Contáctanos
- Ingrese a www.bancopopular.com.co

Banco Popular

Gerencia Integral de Riesgos
Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información

Octubre 2022