Julio
2022

Estudio de mecanismos comportamentales frente al fraude digital

Juan Camilo Cardenas

(Universidad de Massachusetts Amherst y Universidad de los Andes) en colaboración con Sensata Research UX

Aso Ban Caria

Acerca la Banca a los Colombianos

Estudio de mecanismos comportamentales frente al fraude digital

Agradecimientos:

Un sincero agradecimiento al equipo de SENSATA, por su apoyo en el diseño y desarrollo del estudio. El desarrollo metodológico de los datos ha permitido tener unos resultados concretos sobre como la sociedad se comporta frente al fraude digital.

sensata UX RESEARCH

Aso Ban Caria | Acerca la Banca a los Colombianos

Introducción:

Este documento está centrado en mostrar experimentos sobre los diferentes tipos de mensajes para prevenir el fraude digital, midiendo el comportamiento de los usuarios al recibir mensajes centrados en prevenir el riesgo de ser víctima de fraude.

Por lo cual, se realizó un experimento aleatorio para observar las actitudes más sensibles de los consumidores financieros frente a las campañas de sensibilización. Esto con el objetivo de diseñar mejores campañas de prevención. Por eso es relevante caracterizar a los consumidores financieros digitales según su propensión al riesgo, confianza en las transacciones digitales y comportamiento frente a posibles intentos de fraude.

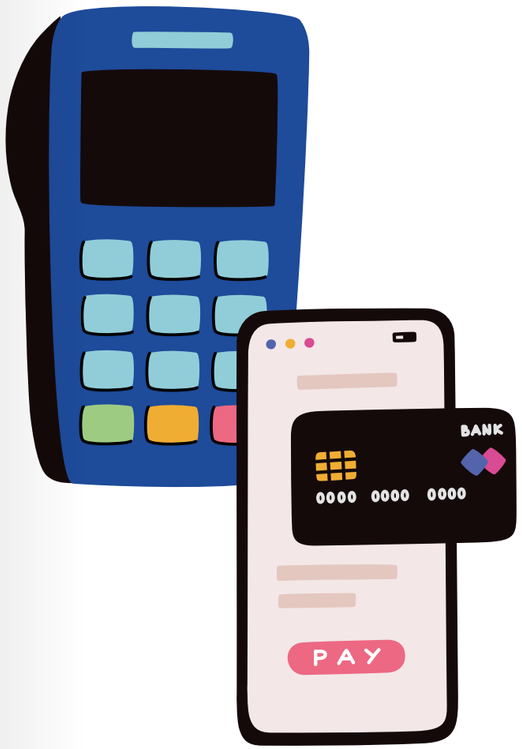
De esta forma, este documento muestra resultados interesantes sobre los tipos de mensaje utilizados en las campañas de prevención y se relaciona con el comportamiento digital de los clientes del sistema financiero.

El desafío que Asobancaria nos puso al frente.

Con el aumento de la bancarización digital se vienen retos grandes para el sector financiero alrededor del mundo. Dos desafíos aparentemente en contradicción se nos aparecen al frente: ¿cómo generar entre los usuarios del sistema financiero una confianza en que la banca digital llegó para quedarse y al mismo tiempo crear en ellos una cultura de prácticas digitales sanas de autocuidado para reducir su exposición al fraude? Alertar sobre los riesgos de los fraudes digitales podría ahuyentar a los usuarios del sistema financiero a hacer un mayor uso de los medios electrónicos para manejar sus productos financieros.

Con ese doble desafío de generar confianza y autocuidado a la vez, Asobancaria se aproximó a nosotros para hacer un estudio basado en las ciencias del comportamiento. El objetivo del proyecto es ofrecer lecciones para diseñar estrategias en donde los clientes del sistema financiero y, en especial, de la banca digital aprendan conductas digitalmente saludables con sus productos financieros. Además se espera que generen confianza en la banca digital como una forma segura en las transacciones diarias de compras, ahorro y crédito.

Con este reto, Asobancaria y Sensata UX Research se unieron para desarrollar un proyecto a través de plataformas digitales para estudiar el fraude digital desde la perspectiva del Colombiano común. Este artículo recoge los principales hallazgos con la aspiración de que todos los actores del sistema financiero puedan beneficiarse de este estudio.



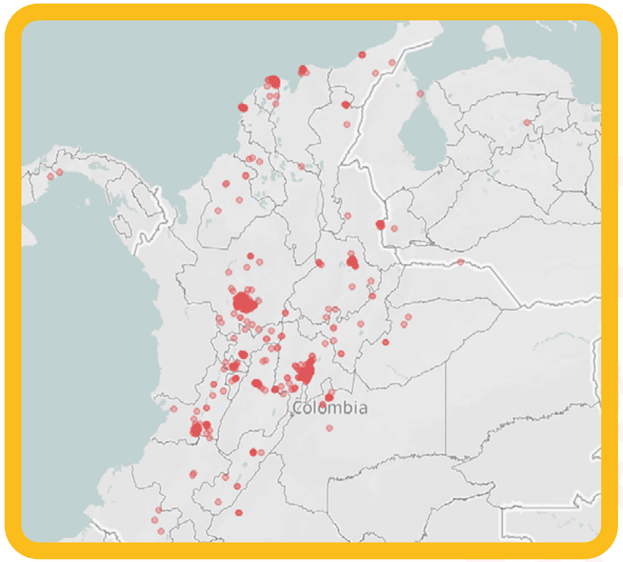
Cómo diseñamos el estudio:

Para desarrollar el estudio y recoger información que nos permitiera responder al desafío teníamos que cumplir varias condiciones. En primer lugar, debíamos diseñar un instrumento de recolección de datos que fuera anónimo, ágil, sencillo, de corta duración, y que nos permitiera recoger datos de una muestra de participantes suficientemente diversa de la población colombiana, y con cobertura en las cuatro principales ciudades del país. Queríamos además que al final del ejercicio los participantes recibieran un saldo pedagógico en el que, basados en las respuestas que nos dieran, damos retroalimentación sobre su perfil de usuario de la banca digital y consejos para reducir su riesgo . Por otra parte, necesitábamos desarrollar un ejercicio que tuviera elementos experimentales en el que pudiéramos aleatorizar diferentes opciones que enfrentarían los participantes y así poder comparar de manera más “limpia” las respuestas comportamentales que queríamos observar en ellos para aprender de sus actitudes, percepciones y acciones cotidianas. Como parte del diseño, debíamos recoger información que evitara algunos sesgos cognitivos que emergen cuando recolectamos información de este tipo. Para mencionar solo un par de ellos, necesitábamos reducir la posibilidad de que las personas nos dieran respuestas que ellos pensaran eran las deseadas por los investigadores en lugar de las que realmente estaban en sus mentes (sesgo de deseabilidad), o reducir los problemas de que unas preguntas fueran “guiando” al encuestado hacia ciertas respuestas sobre otras (efecto de aprendizaje). Finalmente, queríamos que el ejercicio fuera lo menos invasivo posible en términos de la privacidad de los participantes al momento de entrar al aplicativo pero que nos permitiera comparar entre grupos demográficos bien por región, nivel educativo, edad o sexo.

Con base en estos criterios o principios de diseño, y después de algunas pruebas piloto, logramos desarrollar un ejercicio en el que los usuarios, en un tiempo de entre de 4 a 5 minutos, completaron un total de algo más de treinta preguntas. Con base a esto generamos algunos aprendizajes y resultados para quienes en el sistema financiero están preocupados por aumentar la profundización de la bancarización digital y a la vez mantener en su nivel más bajo posible el fraude digital que sufren los usuarios del mismo.

¿Quiénes participaron en nuestro estudio?

Al final del estudio logramos recolectar datos válidos de más de 2,500 personas, distribuidos principalmente (82%) en las cuatro principales ciudades de Colombia como se había propuesto, y con un 18% de personas que estaban distribuidas en otras regiones del país. Algo más del 64% de participación fue por mujeres. Cerca de un 20% de los participantes contaba con educación secundaria, otro 20% con educación técnica o tecnológica, y el resto de participantes con educación universitaria (37%) o posgraduada (22%). Con esta variación regional y demográfica podemos derivar algunas conclusiones sobre las actitudes y comportamientos de grupos diversos de la sociedad colombiana en nuestro estudio.



Personas de distintos perfiles demográficos respondieron la encuesta

Ciudad	Encuestas (%)
Barranquilla	287 (11.2%)
Bogotá	1020 (39.8%)
Cali	170 (6.6%)
Medellín	629 (24.5%)
Otra	455 (17.8%)
Total	2561

Edad	Encuestas (%)
18 a 25	520 (20.3%)
26 a 35	535 (20.9%)
36 a 45	558 (21.8%)
46 a 55	382 (14.9%)
56 a 65	321 (12.5%)
66 o +	179 (7.9%)
Saltar pregunta	66 (2.6%)
Total	2561

Nivel educativo	Encuestas (%)
Ninguno	32 (1.2%)
Primaria	72 (2.8%)
Secundaria	426 (16.6%)
Técnico/tecnólogo	517 (20.2%)
Universitario	947 (36.9%)
Posgrado	567 (22.1%)
Total	2561

Género	Encuestas (%)
Hombre	170 (32.3%)
Mujer	629 (64.6%)
Otro	80 (3.1%)
Total	2561

Los primeros tropiezos en el camino.

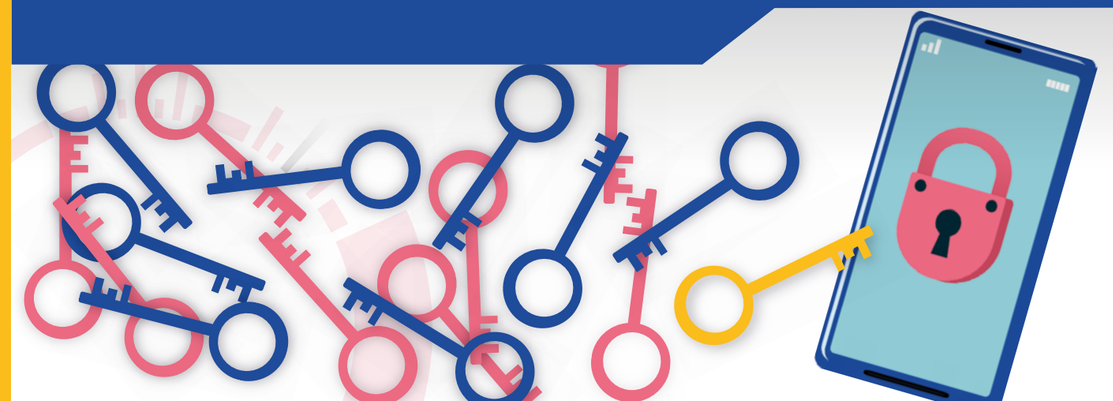
Parte de las buenas prácticas de un estudio comportamental incluye realizar un piloto para probar nuestro instrumento con una pequeña muestra aleatoria y así evaluar amigabilidad, tiempo de respuesta, y coherencia de las respuestas. Sensata UX Research, con su amplia experiencia en este tipo de estudios, fue la primera sorprendida cuando comenzaron a llegar los primeros datos del piloto. ¡O más bien, cuando NO comenzaron a llegar datos completos del piloto! Analizando los metadatos y los datos de tráfico en la plataforma Sensata detectamos una desconfianza mayor a la esperada cuando hacíamos preguntas sobre las heurísticas o trucos que la gente usaba para definir sus claves personales en las plataformas digitales.

Con estas preguntas queríamos precisamente explorar qué algoritmos mentales, heurísticas o reglas usaban las personas para crear sus claves de acceso, y así comprender mejor la forma en que los mismos usuarios de la banca digital podrían protegerse o abrirles las puertas a los delincuentes digitales. El piloto nos mostró que, al llegar a estas preguntas sobre cómo escogen sus claves de acceso a plataformas digitales, los usuarios desertaban sin completar el resto del ejercicio, muy probablemente preocupados porque nuestra encuesta fuera una estrategia fraudulenta de recolección de información personal de ellos.

En retrospectiva, podríamos anticipar que preguntar por los algoritmos mentales que usa la gente para definir sus claves iba a generar sospecha, pero no esperábamos tanta duda y abandono de los participantes en el piloto. Es por esto que rediseñamos nuestro instrumento para mantener la confianza, y lograr que los usuarios llegaran hasta el final de las preguntas. Si hubiéramos seguido con estas preguntas habríamos generado un enorme sesgo de selección en nuestra muestra. Habríamos perdido muchas personas que al desconfiar podrían ser precisamente parte del grupo de usuarios más cautelosos de la banca digital, y quienes hubieran completado el ejercicio estarían sobre representando al grupo de personas con menos atención a las trampas digitales.

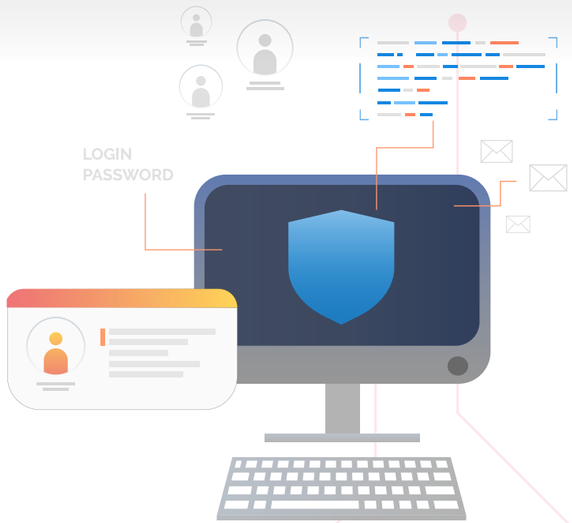
Esta reacción de sospecha en el piloto nos dio un primer campanazo de cómo reaccionan los usuarios del sistema financiero ante posibles amenazas de fraude. Estas primeras alertas nos dieron algunas lecciones para posibles campañas futuras sobre un uso cuidadoso y a la vez frecuente de la banca digital, de lo cual hablaremos al final del artículo.

Finalmente logramos diseñar un ejercicio que sí generó confiabilidad, que fuera ágil y sencillo y que nos dio información valiosa sobre las actitudes, percepciones y acciones de los usuarios del sistema financiero y de sus canales digitales en particular.



El diseño de nuestro ejercicio.

Nuestro instrumento estuvo compuesto de tres secciones. En primer lugar, recolectamos información sobre las actitudes, prácticas y creencias de los usuarios en sus interacciones a través de los canales digitales con sus productos financieros. En una segunda etapa, expusimos aleatoriamente a los participantes a diferentes tratamientos experimentales con el propósito de evaluar qué tipo de mensajes alertando sobre el riesgo de fraude digital podrían llamar su atención, y evaluar si el tipo de canal de llegada del intento de fraude podría también hacer una diferencia. En esta sección del ejercicio también exploramos experimentalmente la propensión de los usuarios a cambiar su clave en su sucursal virtual, dado que es una de las prácticas con mayor efectividad para reducir la posibilidad de acceso de terceros a los productos financieros por vía digital. La tercera y última sección del ejercicio recogía algunos datos demográficos de los participantes y cerraba con una descripción del perfil pedagógico del tipo de usuario, basado en las respuestas dadas a lo largo del ejercicio.



Cuatro perfiles de usuarios digitales del sistema financiero: describiendo las actitudes, percepciones y comportamientos de los encuestados.

La primera sección del instrumento nos permitió caracterizar a los encuestados en cuanto a sus actitudes, prácticas, creencias y experiencias hacia el sistema financiero, la banca digital y el fraude virtual. En primer lugar arrancamos con algunas preguntas rápidas sobre el nivel de prudencia o preferencia por el riesgo del participante al momento de manejar su dinero, y sobre su confianza en el sistema financiero colombiano al momento de realizar compras o pagos por internet y hacia las demás personas en general.

A continuación, hicimos un par de preguntas sobre las percepciones que tenía el usuario del sistema financiero frente a su control sobre el riesgo ante un fraude, y su percepción de la probabilidad de ser víctima del mismo. Seguimos entonces con algunas preguntas que nos dieran una idea de la frecuencia con que esta persona interactuaba a través de medios digitales y algunas prácticas comunes en sus transacciones financieras en medios digitales. Estas preguntas incluían aspectos como los dispositivos a usar, la frecuencia en el uso de medios digitales para transacciones financieras.

En medio de estas preguntas le presentamos al participante una “tentación” para indagar sobre su conocimiento del sistema financiero en general y del tipo de anzuelos que los delincuentes usan para atraer incautos. El anzuelo fue: “Si te ofrecen una inversión donde recibirías una rentabilidad del 5% mensual, tú… Inviertes inmediatamente / Rechazas la oferta / Tomas un tiempo para decidir”.

Este grupo de preguntas previo al bloque experimental nos permite conocer el tipo de perfiles de usuarios que respondieron nuestra encuesta. Utilizando un análisis de correspondencias múltiples identificamos dimensiones que sintetizan las respuestas y ubicamos a los encuestados en ellas. Seguido de esto, usamos un análisis de cluster jerárquico sobre estas dimensiones que nos dió como resultado cuatro grupos, a quienes llamamos, según las actitudes y comportamientos que los caracterizan como: “Usuarios prudentes”, “Usuarios arriesgados”, “Prevenidos” e “Inexpertos desconfiados”. Estos perfiles los describimos a continuación:

Usuarios arriesgados

Son **los que realizan más de 10 transacciones por internet** al mes.
Usan la sucursal virtual

Son **autónomos** para hacer transacciones y valoran ser **arriesgados** con el dinero

Perciben que el sistema financiero y las transacciones por internet son **seguras**

En general **confían** en los demás

Los más conectados **permanecen más de 5 horas conectados a internet**

Tienen comportamientos inseguros (utilizan la misma clave, utilizan redes públicas)

Es el grupo con más víctimas

Usuarios prudentes

Realizan **con frecuencia transacciones por internet** al mes.

Son **autónomos** para hacer transacciones y valoran ser **prudentes** con el dinero

Perciben que el sistema financiero y las transacciones por internet son **seguras**

En general **confían** en las demás personas

Conscientes de que **caer en fraude digital depende de ellos**

Permanecen entre 1 y 4 horas conectados a internet

Prevenidos

Realizan **transacciones por internet con poca frecuencia**

Perciben que el sistema financiero y las transacciones por internet son **inseguras**

Por lo general **confían poco** en las demás personas

Valoran ser prudentes con el dinero y piden apoyo para hacer transacciones digitales

Son más tradicionales usan la mente para guardar claves tienen antivirus gratuito

Creen que es probable que sean víctimas de fraude digital, pero creen que no depende de ellos

Inexpertos desconfiados

Realizan pocas o ninguna transacción financiera o compras por internet

Radicales en su desconfianza hacia el sistema financiero o de realizar compras/pagos por internet

Por lo general **desconfían** en las demás personas

Piden ayuda para transacciones digitales. Prefieren se prudentes frente a temas relaconados con dinero

Permanece menos de 1 hora conectado

Creen probable que sean víctimas de fraude digital

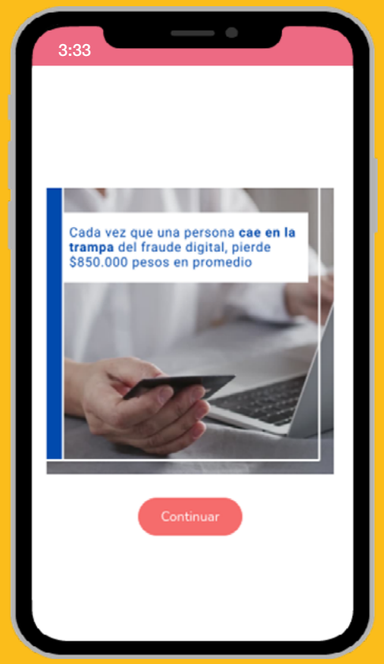
Los dos grupos que denominamos como “Usuarios” realizan transacciones con frecuencia, los usuarios prudentes entre 1 y 4 veces al mes y los arriesgados más de diez al mes. Ambos grupos confían en el sistema financiero y en las demás personas y son autónomos para hacer transacciones. Pero se diferencian en su perfil de riesgo y comportamientos. Los “usuarios prudentes” son prudentes con el dinero ante inversiones fáciles, y son conscientes de que caer en el fraude digital depende de ellos. Por otro lado, los usuarios arriesgados lo son frente a las inversiones, tienen comportamientos arriesgados como utilizar la misma clave para distintas cuentas y utilizar redes públicas y son el grupo que tiene una proporción más alta de personas que han sido víctimas.

El grupo de prevenidos realiza transacciones por internet con poca frecuencia. Son algo desconfiados hacia el sistema financiero y las transacciones por internet, pero confían un poco en las personas, son prudentes al invertir y piden ayuda a la hora de hacer transacciones digitales. Además creen que es probable que sean víctimas de fraude digital, pero consideran que no depende de ellos si lo son.

Finalmente el grupo de inexpertos desconfiados nunca o casi nunca realizan transacciones virtuales, desconfían mucho del sistema financiero y de la banca digital y son desconfiados hacia las demás personas. También piden ayuda para hacer transacciones digitales y son prudentes con el dinero. Además, consideran que es probable que sean víctimas de fraude digital.

Consideramos clave tener en cuenta estos perfiles a la hora de desarrollar campañas o estrategias que ayuden a los usuarios a mejorar la confianza en el sistema, aumentar el uso de los canales digitales y en mejorar su autoeficacia para prevenir el fraude digital.

¿Respondieron los usuarios a nuestras alertas o mensajes de “priming”?



Una vez recogidos los datos de las acciones, actitudes y percepciones de riesgo de los usuarios de la primera parte, procedimos a asignar aleatoriamente a cada participante a una frase que alertaba sobre los riesgos y costos asociados al fraude digital. La siguiente tabla muestra las tres frases que recibieron los grupos en los tratamientos A a C. Un cuarto grupo (Tratamiento D) fue nuestro grupo de control al que no le presentamos ninguna frase de este tipo. Estos mensajes fueron presentados dentro de un diseño idéntico para los tres grupos tipo campaña para que fuera más real el tratamiento.

El propósito de este primer paso experimental era el de explorar qué tipo de información particular podría despertar mayor atención entre los participantes y por ende afectar sus respuestas en los ejercicios a continuación de estas frases. Como se puede apreciar en el contenido de las mismas, queríamos saber la sensibilidad al monto promedio de los fraudes, la frecuencia con que ocurren o a hacer explícito el hecho de que cuando éstos ocurren es porque el cliente voluntariamente entregó datos personales valiosos.

Tratamiento A	Cada vez que una persona cae en la trampa del fraude digital, pierde $850.000 pesos en promedio
Tratamiento B	En TODOS los fraudes digitales, las personas dieron voluntariamente sus datos personales
Tratamiento C	Cada día alrededor de 340 personas caen en la trampa del fraude digital en Colombia
Tratamiento D ***(Grupo de Control)***	No recibe mensaje

Una vez las personas recibían esta información, enfrentaban situaciones hipotéticas de intentos de fraude y en las que queríamos evaluar la propensión de los participantes a caer en el intento de trampa o no. Para ello, creamos los siguientes tres intentos de fraude, o “anzuelos” y sobre los cuales les pedíamos en la pantalla que escogieran entre dos opciones: Ignorar la información o Acceder a la información. Los tres anzuelos que probamos fueron estos:

- ***“Te llega un email con un link para que confirmes una transacción reciente de tu banco, tú…”***
- ***“Te llega un mensaje de texto SMS con un link para que confirmes una transacción reciente de tu banco, tú…”***
- ***“Te llaman de tu banco para confirmar una transacción reciente y te piden unos datos personales, tú…”***

Estas preguntas se realizaron de manera aleatoria a una tercera parte de la población, es decir cada encuestado sólo respondía una de estas preguntas. Esto nos permite evaluar la hipótesis de que hay canales en donde la gente está más dispuesta a caer que otros. Dado que ninguna entidad financiera usa este tipo de mecanismos de correo, SMS o llamadas para confirmar transacciones, pensaríamos que quienes escogieron la opción de acceder a la información haciendo click en el enlace o atendiendo la llamada entregando información personal estarían claramente vulnerando su privacidad, su identidad digital o sus productos financieros.

Siguiendo con nuestra estrategia experimental, también le preguntamos a los usuarios que tan propensos son a cambiar su clave con frecuencia. Para ellos les pedimos que escogieran entre dos opciones ante la pregunta “Preferirías cambiar tu clave de la sucursal virtual”: Nunca o casi nunca, y Cambiar la clave cada ___ meses. Asignamos a los usuarios a tres grupos aleatorios de frecuencia de cambio de clave, con 3, 6 y 12 meses para evaluar si alguna de estas frecuencias podría ser preferida sobre las demás.

En esta etapa de elecciones de escenarios hipotéticos, le presentamos a los participantes con una última situación hipotética en la que le mostramos una imagen como la que se muestra en la siguiente figura y les preguntamos: “Si recibes este mensaje ¿qué haces?” ante lo cual debían responder entre dos opciones: “Lo borro o lo ignoro” o ”Le doy click para saber más”. Esta pregunta fue idéntica para todos los encuestados.

Con estas preguntas en que los participantes podían elegir entre exponerse a una situación de fraude o evitarla, y dado que aleatorizamos los mensajes de “priming” ya mencionados, podíamos evaluar el efecto de esta información de alerta para reducir la exposición al riesgo.

Le entra por una oreja y le sale por la otra o el efecto “alarma de carro”

Es muy probable que mientras usted está leyendo este artículo, en su buzón de correos electrónicos o sus mensajes de texto sin leer, hay una cantidad importante de mensajes de alerta de sus entidades financieras quienes están haciendo un esfuerzo grande por alertar a sus usuarios del creciente riesgo de fraude digital.

Aquí apareció nuestra segunda gran sorpresa en este estudio. El análisis de nuestros datos sugiere que los mensajes de “priming” que enviamos (esos $850 mil pesos que en promedio pierde cada cliente en cada ocasión, o esos 340 casos diarios, o el recordatorio que todos los casos involucraban una entrega voluntaria de datos personales) no generó cambios en las respuestas de acciones para evitar el fraude tales como borrar o ignorar estos mensajes, correos o llamadas que podrían provenir de manos delincuentes. No observamos que la probabilidad de evitar el fraude cambiara por el tipo de mensaje recibido al azar, ni con respecto al grupo de control. Alguien podría argumentar que simplemente los tres mensajes generaban el mismo efecto positivo de alerta y por ello no observamos diferencias entre los tres mensajes, pero tampoco las encontramos cuando comparamos con el grupo de control lo que sugiere más bien que nuestros participantes simplemente no prestaban atención a esta información.

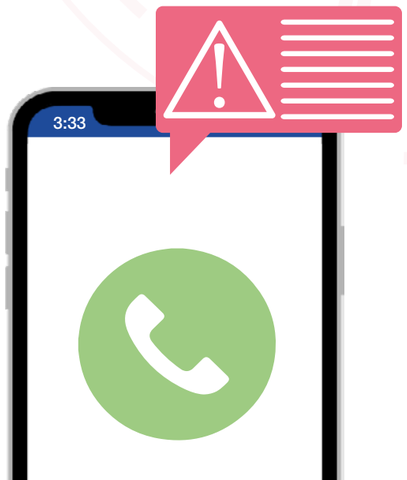
Para el total de nuestra muestra, el 83.4% de nuestros participantes optó por el camino de ignorar los mensajes de texto, correos o llamadas potencialmente fraudulentas, lo cual nos indica que aun tuvimos un 16.6% de personas que podrían estar en más riesgo de picar uno de estos anzuelos. Sin embargo, estas probabilidades no cambian frente al grupo de control o al comparar entre los diferentes mensajes de “priming” que enviamos. Un porcentaje de estos, extrapolado al total de usuarios del sistema financiero, podría significar un riesgo agregado alto de fraude y pérdidas para los bolsillos de los usuarios, las entidades financieras, incluyendo las aseguradoras, podría significar pérdidas económicas importantes para la sociedad. De igual manera, cuando en otro momento del ejercicio presentamos al encuestado con un mensaje de SMS con un enlace probablemente fraudulento, vimos que un 96.2% de las personas seleccionó la opción de borrarlo, lo cual es una señal de esperanza que al menos en estos casos hay una gran mayoría que lo detecta como sospechoso. Sin embargo, ninguno de los mensajes de “priming” cambiaban la probabilidad de que fuera ignorado.

Nuestra interpretación de estos resultados nulos de la primera parte del experimento es que este tipo de mensajes, y para efectos prácticos, para cualquier tipo de campaña a futuro, no llega a ser incorporado en el procesamiento de información de los usuarios del sistema financiero quienes simplemente están filtrando esta información sin incorporarla a su toma de decisiones. Simplemente se ha vuelto ruido de contexto al que poca atención prestamos, como una alarma de carro en el vecindario, que puede dar una sensación falsa de que “el sistema financiero si está tratando el problema”.

El canal por el que llega el fraude puede hacer una diferencia.

Otro de los ejercicios que probamos durante nuestro experimento fue el de aleatorizar entre los participantes si el anzuelo del fraude llegaba por un correo, por un mensaje de texto SMS o por una llamada telefónica. Aquí sí encontramos una diferencia interesante que vale la pena mencionar. La probabilidad de evitar el intento de fraude al ignorar el intento cambió en un 10% entre el caso en que con más probabilidad podrían caer nuestros participantes (20.8% si llegara un correo electrónico del banco), al que menos probabilidad tendría (11.8% si entrara una llamada del banco a confirmar una transacción). En el caso de la llegada de un mensaje de texto esta probabilidad de caer estuvo en un 17.3%. Esto levantaría las alertas especialmente en que hay más vulnerabilidad entre los clientes cuando se trata de los clásicos correos de phishing que con frecuencia cuentan con un nivel de sofisticación al usar logos y diagramaciones aparentemente legítimas, lo que sugiere que puede ser más costo efectivo atacar estos canales.

Las personas conocen parte de sus vulnerabilidades.



Otro resultado que nos llamó la atención es que aquellos usuarios que reconocieron que podrían caer víctimas de fraude con mayor probabilidad, precisamente mostraron una mayor propensión a caer en alguno de nuestros anzuelos de un mensaje, sms o llamada telefónica fraudulenta.

El riesgo de las inversiones sospechosamente atractivas.

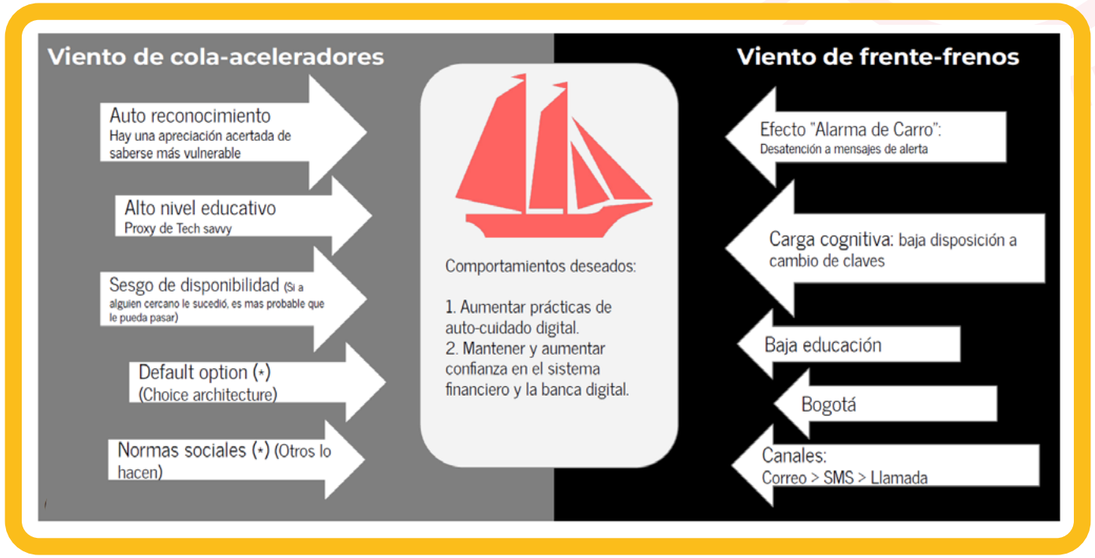
Como el lector recordará, al comienzo describimos que, entre nuestra batería de preguntas sobre actitudes, percepciones y conductas, incluimos el caso de una oferta de inversión que generaba el 5% mensual de rentabilidad. Dado que es imposible que una inversión legal dentro del sistema financiero formalizado pudiera generar este tipo de ganancias, y que con frecuencia los fraudes digitales comienzan por invitaciones sospechosamente atractivas, queríamos probar qué acciones tomarían nuestros participantes ante esta invitación. Del total de participantes, un 5.8% contestó que invertiría inmediatamente, y un 72.7% adicional mencionó que tomaría un tiempo para decidir. Solamente un 21.4% contestó categóricamente que rechazaría dicha oferta. Cuando analizamos estas respuestas frente a las acciones de evitar el fraude ignorando los mensajes, correos o llamadas sospechosas, encontramos algo de coherencia en las respuestas. Por ejemplo, quienes categóricamente contestaron que rechazarían una oferta tan atractiva de una rentabilidad del 5% mensual aumentaban en un 8% adicional la probabilidad de evitar el fraude en nuestros anzuelos de correo, sms o llamadas fraudulentas.

El cambio frecuente de contraseñas continúa siendo un reto grande.

Finalmente, nuestro diseño experimental incluyó el explorar la propensión de los usuarios del sistema financiero virtual a cambiar sus contraseñas, dado que muchas de las vulnerabilidades de los canales digitales están asociadas al acceso de estas claves personales. Ustedes recordarán nuestro fallido intento por explorar qué métodos usaba la gente para crear sus contraseñas. En su reemplazo, enfrentamos a los participantes a que nos contaran de sus preferencias entre no cambiar sus claves o hacerlo en periodicidades diferentes de 3, 6 o 12 meses. Este experimento nuevamente lo hicimos aleatorizando quienes enfrentaban la opción de no cambiar o hacerlo en una de esas periodicidades. Aquí nuevamente no encontramos efecto alguno de nuestros mensajes de priming, y en general, hay una fracción importante de personas que siguen prefiriendo no cambiar su clave o contraseña. En el mejor escenario, un 63% de usuarios cambiaría su clave cada 6 meses, pero ese porcentaje bajaría a 61% si fuese cada 12 meses y a un 58% si fuese cada tres meses. Esto nos deja en un escenario en que cerca de 4 de cada 10 usuarios no está interesado en cambiar sus claves abriendo más probabilidades al robo de esta valiosa información por parte de los delincuentes digitales.

Lecciones

Elementos a favor y en contra del comportamiento seguro



En este diagrama resumimos los factores que pueden ser aprovechados (vientos de cola) y los frenos o vientos de frente que enfrentamos para poder diseñar estrategias de comunicación y acción. Estas deben apuntar generar en los usuarios del sistema financiero un comportamiento que logre nuestros dos objetivos: que se genere una confianza en la banca digital por parte de los clientes del sistema financiero y a su vez una serie de comportamientos de autocuidado o salud digital para evitar los riesgos de fraude que tantas pérdidas le deja al sistema.

Estos factores a favor y en contra de estos dos objetivos expuestos en nuestro diagrama resumen, resultan del análisis estadístico que hemos hecho de los datos, aunque el espacio nos limita a expandir en varios de ellos. Por ejemplo, encontramos que se requiere trabajar en una estrategia aún mayor para el caso de quienes viven en Bogotá y donde encontramos que la probabilidad de tener comportamientos que evitan el fraude es un poco mayor. Igualmente encontramos que mayores niveles de educación de los participantes estaban asociados a una mayor propensión a ignorar los anzuelos de mensajes, correos o llamadas fraudulentas, o a rechazar la oferta de una inversión sospechosamente rentable, igualmente encontramos que las mujeres son más vulnerables al fraude digital

Basados en estos resultados, futuras campañas de promoción de una cultura de cuidado en los canales digitales tendrán que trabajar en evitar estos vientos contra y aprovechar aquellos vientos de cola que, basados en las ciencias comportamentales puedan lograr mayor efectividad en los dos objetivos de confianza en la banca digital y mayor autocuidado.

Entre estas recomendaciones podríamos enfatizar las siguientes:

1

Creemos que las campañas de levantar alertas sobre el fraude van a ser ignoradas por el público. Los mensajes de alerta sobre estos riesgos se han convertido en ruido al que ya no se presta atención. Hay que encontrar formas más creativas de llamar la atención para cambiar las percepciones de riesgo, especialmente entre ciertos grupos que ya hemos mencionado.

2

Aprovechando los mecanismos de normas sociales en donde los individuos escogen con frecuencia ir con la corriente, sugerimos generar campañas en que se apele a perfiles o arquetipos de usuarios que jueguen un papel de modelos de rol a seguir, dependiendo de los grupos demográficos a los que se enfoquen las campañas. Estos arquetipos pueden estar basados en ser un usuario que conoce los medios digitales, conoce los riesgos pero maneja con responsabilidad y confianza sus productos en la banca digital.

3

Basados en características demográficas y en actitudes y preferencias de cada grupo, se pueden diseñar campañas adaptativas y dinámicas, incluso usando estrategias de “gammification” para ir caminando con los usuarios digitales por los diferentes pasos de exposición al riesgo, en donde se pueda dar retroalimentación inmediata al cliente, para que el proceso de interacción genere saldos pedagógicos en cada participante de la campaña.

4

Es necesario diseñar estrategias de cambio de claves o contraseñas que sean percibidas como sencillas y de fácil recordación para eliminar el fenómeno de letargo o inercia que muestran tantos usuarios. El trabajo con diseñadores y desde el concepto mismo de diseño de sistemas (system design) puede ofrecer ideas para que los usuarios encuentren heurísticas para crear sus propias claves de manera rápida, frecuente y segura. Aquí también se puede recurrir a estrategias de arquitectura de diseño de opciones en que las plataformas digitales inviten amablemente a cambiar las contraseñas sugiriendo trucos o heurísticas sencillas y a la vez que garanticen la privacidad, y a la vez a hacer un poco más difícil continuar con la misma contraseña (usualmente denominados “sludges” en oposición a los “nudges”).

Anexo 1. Perfiles pedagógicos

Perfiles pedagógicos que construimos basados en las respuestas a diferentes preguntas de creencias, actitudes y comportamientos seguros. Los encuestados veían esto como una recompensa simbólica por haber completado la encuesta, con el fin también de darles consejos de cómo mejorar sus prácticas.

67-100	**Creencias y Actitudes Seguras**	1. Ciberconocedor desprotegido o ciberconocedor sin antivirus	4. Ciberprotector en entrenamiento	7. Inspector gadget
34-66		2. Ciberescéptico	5. Cibernauta persuasible	8. Cibernauta amateur
0-33		3. Cibernauta en riesgo	6. Cibernauta confiado	9. Cibernauta Pragmático
		Practicas Seguras		
		0-33	**34-66**	**67-100**

1. Ciberconocedor sin antivirus	Reconoces fácilmente el fraude digital, pero podrías estar mejor preparado ante él. Toma el control de tu seguridad digital con estos tips: (1) Ingresa a los portales web de las entidades financieras digitando la dirección. (2) No accedas a través de enlaces enviados en emails o sms. Asegúrate de tener un antivirus licenciado instalado en tu computador y actualizarlo. (3) Cambia tu clave frecuentemente y trata de usar letras, números y caracteres especiales.
2. Ciberescéptico	No crees mucho en el fraude digital, pero es sin duda una amenaza latente. Recuerda que, como usuario, tienes el poder de prevenirlo cuidando tus datos. Aquí te dejamos unos tipos para empezar: (1) Nunca des tus datos personales, claves o números de productos a nadie. Las entidades financieras no piden esta información. (2) Si te ofrecen promociones o premios y te piden acceso a tus datos personales, CUIDADO: de eso tan bueno no dan tanto. (3) Realiza las transacciones desde tu propio celular o computador.
3. Cibernauta en riesgo	A veces tomas decisiones apresuradas al hacer compras o transacciones en internet. Para no caer en el fraude digital, es necesario pensar bien cada acción. El fraude digital le puede suceder a todos, pero podemos evitarlo siendo más precavidos con nuestros datos. Toma el control de tu seguridad digital con estos tips: (1) Ingresa a los portales web de las entidades financieras digitando la dirección. No accedas a través de enlaces enviados en emails o sms. (2) Asegúrate de tener un antivirus licenciado instalado en tu computador y actualizarlo. (3) Cambia tu clave frecuentemente y trata de usar letras, números y caracteres especiales.
4. Ciberprotector en entrenamiento	Sabes mucho sobre el fraude digital y algunas veces tomas medidas para evitarlo, pero podrías mejorar un poco tus prácticas digitales con estos tips: (1) Cambia tu clave frecuentemente y trata de usar letras, números y caracteres especiales. (2) No confíes en los remitentes de tus correos así sus nombres parezcan auténticos. ¡Verifica su autenticidad antes de dar cualquier click! (3) Cuida los códigos de validación y acceso a tus cuentas bancarias. No se los des a nadie.
5. Cibernauta persuasible	Aunque tomas algunas precauciones, el fraude digital toma muchas formas. No te confíes. Tu seguridad digital está en tus manos y puedes mejorarla con estos tips: (1) Accede a los portales web de las entidades financieras digitando la dirección. No accedas a través de enlaces enviados en emails o sms. (2) Realiza las transacciones desde tu propio celular o computador y evita utilizar WiFi público. (3) No confíes en los remitentes de tus correos así sus nombres parezcan auténticos. ¡Verifica su autenticidad antes de dar cualquier click!
6. Cibernauta confiado	Implementas algunas prácticas de seguridad, pero no te tomas el fraude digital muy en serio. El fraude digital toma muchas formas y nos puede afectar a todos. Comienza a informarte más y cuidar más tu seguridad digital con estos tips: (1) Nunca des tus datos personales, claves o números de productos a nadie. Las entidades financieras no piden esta información. (2) Cuida los códigos de validación y acceso a tus cuentas bancarias. (3) Asegúrate de tener un antivirus licenciado instalado en tu computador y actualizarlo.
7. Inspector gadget	¡Felicitaciones! Estás preparado para evitar cualquier fraude digital. Tienes las herramientas y sabes cómo hacerlo. Sin embargo, no te confíes, los ciberdelincuentes siempre encuentran nuevas formas de hacer fraude. Por ello, no olvides estos tips: (1) Nunca des tus datos personales, claves o números de productos a nadie. Las entidades financieras no piden esta información. (2) Cambia tu clave frecuentemente y trata de usar letras, números y caracteres especiales. (3) Realiza las transacciones desde tu propio celular o computador y evita hacer estas diligencias en WiFi públicas.
8. Cibernauta amateur	Reconoces con facilidad los intentos de fraude digital y procuras tener prácticas digitales seguras. ¡No bajes la guardia! Recuerda que siempre podemos prepararnos mejor para evitar estos ciberataques siguiendo tips como estos: (1) Nunca des tus datos personales, claves o números de productos a nadie. Las entidades financieras no piden esta información. (2) Cuida los códigos de validación y acceso a tus cuentas bancarias. (3) Asegúrate de tener un antivirus licenciado instalado en tu computador y actualizarlo.
9. Cibernauta Pragmático	Tienes prácticas digitales seguras, pero no siempre reconoces el peligro del fraude digital. Recuerda que la información es poder. Ayúdate de ella para seguir protegiendo tu seguridad digital y la de tus seres queridos. Comienza a informarte con estos tips: (1) Ingresa a los portales web de las entidades financieras digitando la dirección. (2) No accedas a través de enlaces enviados en emails o sms. Asegúrate de tener un antivirus licenciado instalado en tu computador y actualizarlo. (3) Cambia tu clave frecuentemente y trata de usar letras, números y caracteres especiales.

Anexo 2. Caracterización detallada de los perfiles identificados con los clusters jerárquicos

Esta tabla muestra las respuestas que caracterizan a los distintos perfiles de usuarios identificados durante el análisis de la encuesta.

	Usuarios arriesgados	**Usuarios prudentes**	**Usuarios arriesgados**	**Usuarios prudentes**
Confianza en el sistema financiero y en los demás	Perciben menos seguro el sistema financiero (32%) y hacer compras/ pagos por internet (64%) Por lo general son personas que confían en los demás (62%)	Perciben menos seguro el sistema financiero (32%) y hacer compras/ pagos por internet (64%) Por lo general son personas que confían en los demás (62%)	Perciben inseguro el sistema financiero (9%) y hacer compras/pagos por internet (25%) Por lo general son personas que confían en los demás (35%)	Desconfían de la seguridad del sistema financiero (15%) y hacer de compras/pagos por internet (15%) Por lo general son personas que confían en los demás (32%)
Creencias sobre el fraude digital	Evitar caer en el fraude digital depende completamente de mi, de acuerdo 62% 32% cree que es probable que sea víctima de fraude digital	Evitar caer en el fraude digital depende completamente de mi, de acuerdo 62% 32% cree que es probable que sea víctima de fraude digital	Evitar caer en el fraude digital depende completamente de mi, de acuerdo 59% 42% cree que es probable que sea víctima de fraude digital	Evitar caer en el fraude digital depende completamente de mi, **de acuerdo 71%** 55% cree que es probable que sea víctima de fraude digital
Prácticas seguras	Para realizar trámites bancarios o hacer compras virtuales siempre piden ayuda a algún familiar (7%) Uso de redes de wifi públicas: nunca (39%), en caso de emergencia (48%) y **frecuentemente (13%)** Percepción de la mejor forma de guardar claves: **mente 57%, app 17%**, PC 5%, libreta 15% y otro 6% **Siempre utilizan la misma contraseña** para diferentes cuentas bancarias **(25%)**	Para realizar trámites bancarios o hacer compras virtuales siempre piden ayuda a algún familiar (9%) Uso de redes de wifi públicas: nunca (42%), **en caso de emergencia (53%)** y frecuentemente (5%) Percepción de la mejor forma de guardar claves: **mente 45%**, app 13%, PC 12%, **libreta 19%** y otro 11% Siempre utilizan la misma contraseña para diferentes cuentas bancarias (11%)	Para realizar trámites bancarios o hacer compras virtuales siempre piden ayuda a algún familiar (22%) Uso de redes de wifi públicas: nunca (47%), en caso de emergencia (45%) y frecuentemente (8%) Percepción de la mejor forma de guardar claves: **mente 59%,** app 8%, PC 4%, **libreta 21%** y otro 7% Siempre utilizan la misma contraseña para diferentes cuentas bancarias (18%)	Para realizar trámites bancarios o hacer compras virtuales **siempre piden ayuda a algún familiar (43%)** Uso de redes de wifi públicas: **nunca (72%)**, en caso de emergencia (19%) y frecuentemente (9%) Percepción de la mejor forma de guardar claves: **mente 57%**, app 3%, PC 3%, **libreta 38%** y otro 9% **Siempre utilizan la misma contraseña** para diferentes cuentas bancarias **(25%)**
Experiencia digital	Conexión a internet: menos de 1 hora (2%), entre 1 y 4 horas (40%) y **más de 5 horas (58%)** Compras por internet en el último mes: ninguna (6%), entre 1 y 4 (42%), entre 5 y 10 (21%) y **más de 10 (31%)** Transacciones financieras por canales digitales: ninguna (1%), entre 1 y 4 (8%), entre 5 y 10 (19%) y **más de 10 (72%)**	Conexión a internet: menos de 1 hora (2%), entre 1 y 4 horas (40%) y **más de 5 horas (58%)** Compras por internet en el último mes: ninguna (6%), entre 1 y 4 (42%), entre 5 y 10 (21%) y **más de 10 (31%)** Transacciones financieras por canales digitales: ninguna (1%), entre 1 y 4 (8%), entre 5 y 10 (19%) y **más de 10 (72%)**	Conexión a internet: menos de 1 hora (7%), entre 1 y 4 horas (67%) y más de 5 horas (25%) Compras por internet en el último mes: **ninguna (39%), entre 1 y 4 (59%)**, entre 5 y 10 (2%) y más de 10 (1%) Transacciones financieras por canales digitales: ninguna (8%), **entre 1 y 4 (69%)**, entre 5 y 10 (16%) y más de 10 (8%)	Conexión a internet: **menos de 1 hora (32%)**, entre 1 y 4 horas (47%) y más de 5 horas (21%) Compras por internet en el último mes: ninguna (76%) y entre 1 y 4 (24%) Transacciones financieras por canales digitales: **ninguna (46%), entre 1 y 4 (43%)**, entre 5 y 10 (7%) y más de 10 (4%)
Acceso a productos y canales digitales	96% tiene cuenta de ahorros/corriente 17% usa el PC con mayor frecuencia para realizar transacciones financieras, 83% el celular Siempre o la mayoría de veces utilizan la sucursal virtual del banco 91%	95% tiene cuenta de ahorros/corriente 33% usa el PC con mayor frecuencia para realizar transacciones financieras, 67% el celular Siempre o la mayoría de veces utilizan la sucursal virtual del banco 87%	82% tiene cuenta de ahorros/corriente 11% usa el PC con mayor frecuencia para realizar transacciones financieras, 89% el celular Siempre o la mayoría de veces utilizan la sucursal virtual del banco 47%	**66%** tiene cuenta de ahorros/corriente 21% usa el PC con mayor frecuencia para realizar transacciones financieras, 79% el celular Siempre o la mayoría de veces utilizan la sucursal virtual del banco 20%

Actitudes frente al dinero	En lo que tienen que ver con dinero prefieren ser prudentes 73%, arriesgados 27% Ante una oferta de inversión (con una promesa de 5% de rentabilidad mensual) 72% toma un tiempo para decidir, 17% rechaza la oferta, 11% invierte	En lo que tienen que ver con dinero prefieren ser prudentes 92%, arriesgados 8% Ante una oferta de inversión (con una promesa de 5% de rentabilidad mensual) 81% toma un tiempo para decidir, 14% rechaza la oferta, 5% invierte	En lo que tienen que ver con dinero prefieren ser prudentes 90%, arriesgados 10% Ante una oferta de inversión (con una promesa de 5% de rentabilidad mensual) 76% toma un tiempo para decidir, 19% rechaza la oferta, 5% invierte	En lo que tienen que ver con dinero prefieren ser prudentes 91%, arriesgados 9% Ante una oferta de inversión (con una promesa de 5% de rentabilidad mensual) 57% toma un tiempo para decidir, 37% rechaza la oferta, 6% invierte
Relación con el fraude digital	35% alguna vez ha sido víctima de fraude digital El fraude sucedió en los último 2 años 47% Ocurrió por: internet 52%, sucursal telefónica 12%, banca móvil 6%, datáfono 8%, otro 22% 46% reporta que alguien del núcleo cercano ha sido víctima de fraude	26% alguna vez ha sido víctima de fraude digital El fraude sucedió en los último 2 años 40% Ocurrió por: internet 53%, sucursal telefónica 15%, banca móvil 8%, datáfono 5%, otro 20% 44% reporta que alguien del núcleo cercano ha sido víctima de fraude	25% alguna vez ha sido víctima de fraude digital El fraude sucedió en los último 2 años 49% Ocurrió por: internet 45%, sucursal telefónica 10%, banca móvil 8%, datáfono 6%, otro 25% 47% reporta que alguien del núcleo cercano ha sido víctima de fraude	24% alguna vez ha sido víctima de fraude digital El fraude sucedió en los último 2 años 34% Ocurrió por: internet 32%, sucursal telefónica 17%, banca móvil 7%, datáfono 7%, otro 38% 42% reporta que alguien del núcleo cercano ha sido víctima de fraude

Aso Ban Caria

Acerca la Banca a los Colombianos