

## LOS RIESGOS PARA LOS USUARIOS DE SERVICIOS FINANCIEROS DERIVADOS DE LA TRANSFORMACIÓN DIGITAL

III Congreso de Educación Financiera Edufinet “Realidades y Retos”  
Málaga, 16-20 noviembre 2020

*Working Paper 3/2022*

José Francisco Domínguez Franco  
Edufinet

---

### Resumen

En el presente artículo se ponen de manifiesto los principales riesgos en la contratación de productos financieros por internet, así como del uso de servicios de pago. También se señalan las posibles acciones que se pueden acometer para hacer frente a dichos riesgos.

**Palabras clave:** digitalización; competencias digitales; contratación de productos financieros *online*.

**Códigos JEL:** G53; Q55.

---

El proceso de digitalización es algo imparable; sin entrar en multitud de datos de los que se publican diariamente, conviene mostrar los resultados de un estudio que elabora la Comisión Europea todos los años: el Índice de la Economía y la Sociedad Digital, que resulta bastante útil ya que ofrece datos país por país de la Unión Europea además de realizar una comparativa frente a la media, de manera que se obtiene la información de la situación de cada país.

En este sentido, los usuarios de banca *online* en España, en el año 2020, suponían ya el 60% de los usuarios de internet. La media de la UE se sitúa en un 66%, dato que indica que España se encuentra todavía lejos de la media pero sí habría que indicar que se avanza rápidamente en este aspecto.

Estos datos se están acelerando a raíz de la pandemia del COVID-19, que está prácticamente obligando a llevar al entorno digital muchísimas actuaciones y acciones que antes se realizaban en un entorno físico. Incluso podríamos decir que, según diversos estudios, la digitalización va mucho más rápido de lo que inicialmente se pensó.

Otro dato a destacar del estudio es el resultado del nivel de competencias digitales básicas en España, según el cual, el 43% de la población entre 16 y 74 años carecen de estas competencias. Éste es un dato preocupante ya que

supone que casi la mitad de la población española no tiene unas competencias básicas en el mundo digital e implica que aún queda mucho camino por recorrer desde el punto de vista educativo.

En definitiva, la digitalización aporta múltiples ventajas tanto para usuarios como para entidades. Desde el punto de vista del usuario podemos hablar de comodidad, rapidez, conectividad en cualquier lugar y momento; pero también tiene desventajas o inconvenientes, ya que supone un aumento de los riesgos.

### **Riesgos en la contratación de productos por internet**

Según el subgobernador del Banco de España en la clausura de un seminario en la Universidad Menéndez Pelayo en el año 2018 y refiriéndose a la contratación de productos a través de teléfonos, tabletas o dispositivos digitales: “El tamaño de la pantalla, la aparente amabilidad de las aplicaciones y la inmediatez en la aceptación, limitan la capacidad del diente para saber qué es realmente lo que está consintiendo y obstaculizan determinados aspectos básicos en la contratación de productos financieros tales como la lectura de los términos y condiciones de los contratos o la interacción para resolver preguntas sobre ellos”.

En estas palabras podemos ver sintetizados cuáles son los principales riesgos de la contratación de productos financieros por internet. En definitiva, propicia una facilidad de acceso muy grande pero con una serie de limitaciones como son los tamaños de la pantalla, la presentación atractiva que puede hacer “bajar la guardia” o la inmediatez que hace a veces tomar decisiones de una forma precipitada o poco reflexiva. La situación se ve agravada en tanto en cuanto, el diente asume una mayor autonomía, teniendo el control absoluto del proceso, tanto en la recopilación de la información como a la hora de tomar la decisión.

Los desarrollos tecnológicos propician el acceso a activos y productos financieros más complejos que no están disponibles inicialmente a través de los canales tradicionales, como pueden ser las criptomonedas a las que cualquier persona puede acceder, adentrándose en un mundo en el que, si no se tienen unos sólidos conocimientos, puede ser bastante peligroso.

En definitiva, estos riesgos llevan a que se tomen decisiones de forma poco reflexiva. Esta sería la conclusión fundamental de los riesgos que nos acechan en la contratación de productos *online*. Las consecuencias de esta situación pueden venir tanto del lado de la inversión como del endeudamiento, es decir, un usuario se puede introducir en el camino de invertir en productos financieros complejos o en activos sofisticados lo que puede implicar pérdidas totales del capital o pérdidas de rentabilidad en sus inversiones. Desde el punto de vista del endeudamiento, lo más peligroso sería encontrarse en una situación de sobreendeudamiento, es decir, que el consumidor caiga en un elevado índice de deuda en su economía familiar o doméstica.

### **Servicios de pago**

En este apartado nos referimos a transferencias, tarjetas o cualquier pago *online* que se realizan en estos días. En este caso, los principales riesgos los constituyen los fraudes y las estafas.

Hay que hacer referencia a dos documentos que ilustran muy daramente estas situaciones. En primer lugar la ‘Memoria de la Fiscalía General del Estado’ del año 2019 en el que se habla de un incremento del 44,92% de delitos informáticos con respecto a 2018, aquí se incluyen todos los delitos informáticos como pueden ser delitos sobre la integridad moral, contra la libertad, etc.; las estafas supondrían el 70% de estos delitos. Más sorprendente es el incremento producido desde el año 2017 que alcanza el 97%.

En este sentido se da un dato bastante elocuente sobre lo que está pasando y es que el peso que tienen los ciberdelitos respecto a la totalidad de los delitos que se cometen en España ha pasado de un 2,1% en 2011 al 9,9% en 2019, sin contar lo que ha propiciado la aceleración de la digitalización que ha supuesto la pandemia del COVID-19. De cada 100 delitos que se cometen en España, ya hay 10 que se producen en el entorno digital. Así mismo hay que tener en cuenta que estos datos no muestran la totalidad de la actividad delictiva ya que muchos delitos no son

denunciados ni detectados o que, dada la dificultad para averiguar quiénes son los responsables las actuaciones quedan archivadas sin incoar procedimientos judiciales.

Esta memoria conduce que hay una cifra oculta de cibercriminalidad bastante alta y que es muy difícil saber cuál es su índice real.

El segundo documento al que hay que hacer referencia es la 'Memoria anual del Departamento de Conducta de Entidades del BdE' de 2019 que incluye las redamaciones efectuadas ante esta entidad.

El aspecto clave de este documento es que las redamaciones por fraude se han incrementado un 94% respecto a 2018. En números absolutos no son muchas, pero el porcentaje de crecimiento y el ritmo de crecimiento sí resulta importante.

Esta memoria hace una serie de recomendaciones a los usuarios sobre precauciones a tomar, sobre las comunicaciones recibidas y de contrastar siempre con su banco la veracidad de las informaciones o comunicaciones que se reciban. Igualmente, en el portal del cliente bancario, que es una web del Banco de España, se publica bastante información sobre estos temas.

Dentro de los servicios de pago hay que tener en cuenta la denominada ingeniería social, ya que la mayoría de los ataques que antes comentábamos no se llevan a cabo aprovechando vulnerabilidades de *hardware* o *software* sino engañando a las víctimas para que ellas mismas faciliten el fraude (ingeniería social).

Según el Instituto Nacional de Ciberseguridad (INCIBER), la ingeniería social es una técnica que utilizan los ciberdelincuentes para ganarse la confianza del usuario y conseguir que haga algo bajo manipulaciones y engaños, como, por ejemplo, ejecutar un programa malicioso, facilitar sus datos o comprar en sitios web fraudulentos. En definitiva, el principio que sustenta la ingeniería social es que la persona, el usuario, es el eslabón más débil de la cadena, por lo que es más fácil engañar a alguien para que proporcione información confidencial que vulnerar la seguridad de una máquina o un sistema.

En este sentido la oficina de seguridad del internauta, ha publicado que el 93% de las brechas de seguridad son debidas a la ingeniería social. Un dato que resulta demoledor dejando bastante bien ubicada la cuestión, es decir, estamos hablando de engaños a las personas y por tanto se pueden prevenir; no hace falta ser un experto informático o en tecnologías, sino que, con una serie de acciones, se puede intentar evitar que esto ocurra.

La lista de técnicas utilizadas es muy extensa y muy variada, además de que se van creando nuevas, siendo las más conocidas: el *phishing*, que consiste en enviar *e-mails* a los usuarios haciéndose pasar por una institución de confianza y en el que se le incita a pinchar un enlace a través del cual o bien se descarga un *software* malicioso o lleva a una página web simulada con la excusa de que la cuenta del usuario ha sido bloqueada o han intentado hacer operaciones no autorizadas, etc., jugando con la urgencia, con el miedo, de manera que realizando la acción solicitada va a revelar sus datos a los delincuentes.

El *smishing*, es similar al anterior, pero en lugar de *e-mails* el formato utilizado es el envío de mensajes a móviles y el *vishing* que se realiza a través de llamadas de teléfono. También el *dumpster diving* que intenta obtener información financiera revisando la basura, el *shoulder surfing* o 'mirar por encima del hombro' es una técnica muy utilizada para obtener los datos que el usuario está tratando de pagar por ejemplo en un supermercado para después sustraer la tarjeta utilizada y utilizarla con el número secreto obtenido.

En definitiva estas técnicas pueden parecer simples o poco sofisticadas pero son muy efectivas y por tanto es necesario que sean conocidas, ya que el ritmo de crecimiento de este tipo de delitos está siendo muy grande.

## ¿Cuáles son las posibles acciones que se puede acometer para hacer frente a estos riesgos?

Desde la perspectiva de la prevención, está claro que la información sobre la existencia de estos riesgos y la formación, en definitiva, la educación financiera, ha de ser los dos pilares a través de los cuales se aborden estos riesgos. En este arduo trabajo deben de estar implicados tanto instituciones públicas como privadas y.

Dentro de las distintas aportaciones de la educación financiera, me gustaría citar la definición de la OCDE que la define como “los distintos procesos para que los inversores tengan un mejor entendimiento de los productos y lleguen a ser más conscientes de los riesgos”, incluyendo ya el concepto de riesgo.

En este sentido, el Proyecto Edufnet declara en su página que: “la pretensión esencial es que los ciudadanos puedan adquirir los conocimientos que le permitan adoptar sus decisiones en el ámbito financiero de manera consciente e informada”; siendo, quizás, la palabra clave ‘consciente’, que sería la contraposición a los automatismos, o a las actuaciones poco meditadas que puede llevar la contratación de productos en el entorno digital.

Finalmente, también en el portal del cliente bancario del Banco de España, se habla de que “la educación financiera debe ir más allá de la mera disponibilidad de información y se extiende a los conocimientos, conductas y actitudes que permiten tomar decisiones acertadas”, es decir, habla de conductas y actitudes marcando ya el camino en el sentido de que hay que ir más allá abordando la educación financiera desde otras perspectivas como la psicología financiera y el conocimiento de las limitaciones o de los posibles errores del conocimiento que puede tener una persona ante la realización de una acción precipitada o poco meditada.

Las posibles acciones son muy similares tanto en el caso de contratación de productos como con respecto a los servicios de pago, aunque sí podríamos hacer una pequeña distinción:

En la contratación de productos estamos hablando de falta de reflexión, es decir, de no dar los pasos aconsejados a la hora de adoptar una decisión. Hay que saber que una toma de decisiones no ha de entenderse como la elección entre una alternativa u otra sino como un proceso que tiene varios pasos: recopilar información, consideraciones disponibles, necesidades del usuario, los objetivos a cubrir y, por supuesto, valorar las posibles consecuencias.

En este sentido la educación financiera puede ayudar al aumento de las competencias digitales, que en el caso de la población española necesita una mejora clara; concienciando en el cambio que supone operar a través de los canales digitales: la revolución que esto supone y los riesgos a los que nos enfrentamos los usuarios a la hora de operar a través de estos canales. Todo ello, independientemente del conocimiento del producto, que es el mismo en todos los canales lo único que varía es la forma de contratación, que conlleva una serie de riesgos, donde entra en juego el proceso de toma de decisiones responsables y las aportaciones que pueda realizar la psicología financiera o finanzas conductuales, para una mejor comprensión de cual es el proceso de toma de decisiones financieras y que ayude a evitar caer en sesgos cognitivos o en decisiones poco racionales o poco meditadas.

En cuanto a los servicios de pago, el principal riesgo es ser víctima de un engaño o fraude, y donde la clave residiría en el conocimiento de la ingeniería social, que quizás sea un concepto poco conocido, y la explicación de sus técnicas y mecanismos y de cómo influye la mente humana para engañarnos, en definitiva implicaría también conocimientos de psicología para poder hacer frente a ellos.

En este aspecto, es básico, al igual que cuando hablamos de la contratación de productos, tener unas competencias digitales básicas; conocimientos sobre las técnicas y la casuística que se utilizan a través de la ingeniería social, pero también resulta muy importante la utilización del pensamiento crítico, que puede ser la clave. Esto es la capacidad para evaluar una información, cuestionarla y saber cómo contrastarla mediante las preguntas adecuadas para poder llegar a la veracidad de la información.

En resumen, fraudes y estafas han existido siempre y seguirán existiendo. Lo que ha cambiado es el terreno de juego, en el que, para poder participar, los usuarios deben de tener unos conocimientos suficientes para no encontrarse en inferioridad de condiciones. Por tanto, hace falta mucha información, mucha divulgación sobre estos riesgos y por supuesto, formación.

Para terminar, podríamos exponer las siguientes conclusiones:

1. La transformación digital avanza de forma imparable.
2. Este proceso aporta indudables beneficios, si bien tiene ciertos riesgos que se deben mitigar.
3. En la contratación de productos por internet, el riesgo más relevante es la falta de reflexión a la hora de suscribir dichos productos.
4. En cuanto a los servicios de pago, el principal riesgo lo podemos encontrar en los fraudes y estafas, sobre todo a través de técnicas de ingeniería social. Por tanto, es importante incidir en este aspecto con la divulgación y desarrollo de pensamiento crítico.
5. Todos estos riesgos pueden ser mitigados a través de la educación financiera. Al igual que en el entorno físico, el conocimiento adecuado de los distintos productos son el punto de partida esencial. No obstante, el entorno virtual tiene una serie de particularidades que aconsejan adaptar los contenidos de la educación financiera ante el nuevo terreno de juego digital, que hace que estos productos ya conocidos tengan unas características y unas especificidades propias que los ciudadanos deben de conocer para ser conscientes de los riesgos y poder actuar adecuadamente en el mundo digital.