«Protección de los beneficiarios de seguros de vida», por José Ramón Lozano Petit

escrituraPublica.es/operar-de-forma-segura-en-internet-por-jose-luis-martinez-campuzano

12 de septiembre de 2022

PROTECCIÓN AL CONSUMIDOR

JOSÉ LUIS MARTÍNEZ CAMPUZANO,

portavoz de la Asociación Española de Banca
Twitter: @Aebanca

"¿Qué se puede hacer en caso de haber sufrido algún fraude Es fundamental contactar con las autoridades y poner una denuncia"

Operar de forma segura en internet

Seguro que alguna vez han recibido un correo, un mensaje o una llamada identificándose como su empresa de servicios, administración pública o su banco. En muchos casos no trataban de darles información, sino más bien de pedírsela y acceder de esta forma a sus datos, o a aquellos que les faltaban.

En la mayoría de los casos sería un engaño. Recurramos al sentido común para prevenirlo: ¿por qué dar nuestros datos a un tercero sin comprobar antes si es quien dice? Los procedimientos que emplean los delincuentes en ámbitos no presenciales son cada vez más generalizados, ni siquiera son muy sofisticados; utilizan la manipulación emocional y casi siempre urgiendo. Por eso nosotros también debemos ser más prudentes y precavidos. La clave es asumir que es necesario reforzar las medidas de precaución y seguridad en internet como hacemos en nuestra vida diaria.

El Instituto Nacional de Ciberseguridad (Incibe) gestionó el año pasado más de 100.000 estafas digitales, la inmensa mayoría a ciudadanos particulares. Pero la delincuencia digital nos afecta a todos, con cada vez más ataques a empresas y administraciones públicas. Aunque la mejora de la coordinación entre sectores y a nivel internacional no ceja y los mecanismos de blindaje se hacen más sofisticados, con el coste que eso entraña, los ataques también se hacen más atrevidos y avanzados.

Combatir la ciberdelincuencia se ha convertido en una de las principales prioridades para todos: ya seamos particulares, o trabajemos en empresas, instituciones o gobiernos. Y todos tenemos la responsabilidad de prevenirla y combatirla: las compañías y las autoridades deben invertir en protección y en reforzar la colaboración entre todas las partes implicadas; los individuos debemos asumir también la responsabilidad de proteger nuestros propios datos y actuar con cautela. Ya que conviene proteger nuestra información, no solo por el daño que su robo puede implicarnos, sino también porque puede ser utilizada para atacar a nuestros seres queridos.

Está claro que avanzar en la capacitación digital de la sociedad nos permitirá sacar el máximo provecho a la transformación que estamos viviendo. La innovación, en su versión digital, ha sido clave para mejorar nuestra vida diaria durante el confinamiento y los peores momentos de la pandemia. En esta época ya es impensable un mundo sin las ventajas de la innovación en su versión digital. Sin embargo, un mejor uso de internet también incluye sensibilizarnos frente a sus riesgos, que tendemos a olvidar y son muy reales.

Solemos pensar que los ciberataques son cosas que les ocurren a otros, pero hoy todos podemos ser víctimas. Ante una amenaza cada vez más global y sofisticada, la concienciación es el mejor escudo para protegernos. En todos los casos, más allá de sus enormes consecuencias financieras, los ataques infligen un daño a la seguridad y confianza de los consumidores. Es importante reconocer que todos estamos potencialmente amenazados, porque no hacerlo así es ponérselo fácil a los delincuentes.

La cooperación y especialmente la colaboración público-privada es clave para combatir la ciberdelincuencia en todas sus vertientes. Con este convencimiento, la Asociación Española de Banca (AEB) firmó hace unos meses el protocolo general del Plan de Acción contra el Fraude Financiero para potenciar y mejorar la prevención y la lucha contra las ofertas de productos y servicios potencialmente fraudulentos, que ocasionan graves perjuicios a los inversores y a todo el sector financiero regulado. Compartir la información con las administraciones es clave para combatir el fraude financiero en todas sus fases: concienciación, prevención y persecución del delito.

La ciberseguridad es fundamental para los bancos, que ponen todos los medios a su alcance para garantizar la seguridad de sus clientes y encarar los riesgos que seguro aparecerán en el futuro. El sector bancario tiene probada experiencia en la protección de los datos personales y financieros de sus clientes, y revisa continuamente su capacidad de defensa, detección y respuesta ante los ciberataques. Pero todo esto quizás no sea suficiente si los individuos no asumimos nuestra parte de responsabilidad para luchar contra esta lacra.

Hay unas recomendaciones sencillas que todos debemos seguir para protegernos frente a los delincuentes digitales.
Los canales de la banca son seguros para operar: páginas web oficiales, aplicaciones de la banca, teléfonos oficiales, siempre que se acceda directamente y no a través de enlaces

recibidos en mensajes. Cuidado por tanto con las comunicaciones o avisos recibidos por canales de mensajería instantánea, redes sociales, así como SMS y llamadas desde teléfonos que aun pareciendo oficiales no lo son.

Atendiendo al uso masivo que hacemos del móvil debemos protegerlo con claves de entrada que deben ser revisadas de forma periódica, realizar actualizaciones y siempre acceder a apps oficiales para descargar otras aplicaciones y, en la medida de lo posible, contar con un antivirus.

¿Qué se puede hacer en caso de haber sufrido algún fraude? Es fundamental contactar con las autoridades y poner una denuncia como haríamos ante un robo. También, si hay una pérdida financiera o de las credenciales de seguridad, hemos de contactar con nuestro banco a través de un canal seguro para que pueda tomar las medidas necesarias para mitigar al máximo las posibles consecuencias.

La prudencia y el sentido común son nuestros mejores aliados para luchar contra los ciberdelincuentes, ya que en muchos casos se aprovechan de nuestra versión más confiada para poder perpetrar sus ataques.

La prioridad, el cliente,