El Economista
martes, 24 de enero de 2023

CONCIENCIAR PARA PREVENIR

J. L. Martínez Campuzano
Portavoz de la Asociación Española de Banca

Operar de forma segura en Internet es una prioridad porque la red se ha convertido en una herramienta indispensable en nuestras vidas. Todos los días nos conectamos, buscamos información y accedemos a productos y servicios públicos y privados. Internet forma parte de nuestro día a día e influye en nuestra forma de actuar y hasta de pensar mucho más de lo que creemos.

Por eso combatir la ciberdelicuencia ha pasado de ser una necesidad a ser una obligación, ya seamos particulares o trabajemos en empresas, instituciones o gobiernos. Todos tenemos la responsabilidad de prevenirla: las empresas y las autoridades deben invertir en protección y en reforzar la colaboración entre todas las partes implicadas, y los individuos debemos asumir también la responsabilidad de proteger nuestros propios datos y recurrir a fuentes fiables para asesorarnos y actuar con cautela.

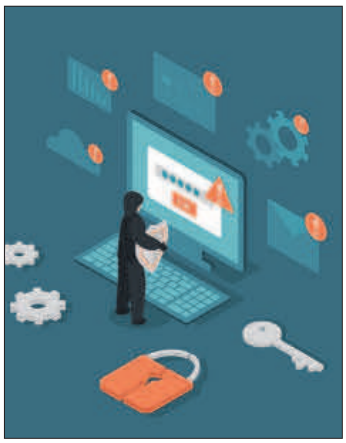
> Las estafas se están viendo potenciadas por la rápida transformación digital

De la misma forma que solemos pensar que los ciberataques son cosas que les ocurren a otros, también consideramos que nunca vamos a sufrir estafas en Internet. Pero todos estamos expuestos y hemos de estar alerta. No solo por nuestro bien, sino también por el de nuestro entorno. Aparte de las consecuencias financieras que los ciberataques y las estafas nos pueden acarrear, pueden tener impacto en nuestro entorno cercano y suponen un golpe a la seguridad y confianza de todos.

Con este objetivo de concienciar para prevenir damos la enhorabuena a la guía publicada por la CNMV sobre estafas y fraudes. En su introducción define la estafa financiera como una acción realizada por una persona o empresa que causa un perjuicio a un tercero mediante engaño y con ánimo de lucro. Y aunque existen muchos tipos de estafas y fraudes financieros, todas se han visto potenciadas por la transformación digital de la sociedad.

Las modalidades de engaño que recoge la guía son conocidas prácticas inmemoriales: promesas de cuantiosas ganancias, métodos de inversión infalibles o soluciones imposibles a problemas económicos y financieros y ofertas de corta duración. Aunque diferentes, todas tienen un factor común: ofrecen una elevada rentabilidad futura, lejos de las existentes en el contexto económico, a cambio de entregar un capital inicial al supuesto experto o entidad no autorizada para ofrecer este tipo de servicio.

Los términos de chiringuito financiero o entidades pirata definen de manera informal a aquellas entidades que ofrecen y prestan



ISTOCK

servicios de inversión sin estar autorizadas para hacerlo. Son estafadores que pueden utilizar los mismos canales comerciales que puede emplear cualquier entidad legítima: teléfono, correo electrónico, páginas web y redes sociales, entre otros. Mientras las empresas y entidades para prestar servicios de inversión están registradas y sometidas a las normas que regulan los mercados de valores y a estrictos controles por parte de los organismos supervisores, los chiringuitos financieros actúan al margen de la legalidad.

La cooperación, especialmente la público-privada, es clave para combatir la ciberdelincuencia en todas sus vertientes. Con este convencimiento, la Asociación Española de Banca firmó hace unos meses el protocolo general del Plan de Acción contra el Fraude Financiero para potenciar y mejorar la prevención y lucha contra la oferta de productos y servicios potencialmente fraudulentos, que ocasionan graves perjuicios a los inversores y a todo el sector financiero regulado.

A través de este Plan, impulsado por la Comisión Nacional del Mercado de Valores (CNMV), se articulan medidas para reducir la capacidad de actuación y expansión de los intentos de fraude financiero, restringir la publicidad de actividades para captar nuevos afectados, y facilitar a los clientes de servicios financieros los instrumentos y conocimientos necesarios para evitar ser una víctima. Un buen ejemplo es la guía publicada.

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. Las entidades están preparadas para detectar y prevenir el fraude financiero y sus canales son seguros para operar: páginas web oficiales, aplicaciones y banca telefónica. Pero siempre hay que acceder a ellos directamente y desconfiar de las comunicaciones o avisos recibidos por canales de mensajería instantánea, redes sociales, SMS o llamadas desde teléfonos que aún pareciendo oficiales no lo son.

Ninguna entidad financiera autorizada pedirá jamás a sus clientes información personal ni claves completas. Ellas ya disponen de estos datos y bajo ningún concepto necesitan pedirlos, y menos aún, por medios tan poco confidenciales como el correo electrónico o el teléfono. La prudencia y el sentido común son nuestros mejores aliados para luchar contra los ciberdelincuentes.