Cofinanciado por la Unión Europea

Centro Europeo del Consumidor España
ECC-Net

Nota informativa

12 de junio de 2023

España lanza una campaña para concienciar a los consumidores sobre las ciberestafas

España pone en marcha la campaña "Uno de Cada Cinco Delitos" para hacer frente al incremento de la cibercriminalidad

La campaña del Ministerio del Interior "Uno de Cada Cinco Delitos" -con la que se quiere luchar contra las ciberestafas que ya representan uno de cada cinco delitos cometidos en nuestro país- incluye una serie de vídeos en los que se hace hincapié en las estafas y fraudes más comunes cometidos en la red. Al mismo tiempo, ofrece las claves para que los ciudadanos puedan identificarlos fácilmente, así como una serie de consejos para evitar que se conviertan en víctimas. Por este motivo y con el fin de ayudar a que las personas consumidoras no caigan en la trampa, el Centro Europeo del Consumidor en España repasa algunos de estos delitos y las recomendaciones para prevenirlos.

Phising
Se trata de una técnica empleada por los ciberdelincuentes para "pescar" datos personales de las víctimas a través de enlaces incluidos en correos fraudulentos. Los mensajes atraen a las víctimas con los ganchos de un premio aleatorio, de la herencia recibida por parte de un familiar lejano o con peticiones solidarias para ayudar a los damnificados por conflictos bélicos o por catástrofes naturales. Para evitar caer en el engaño, se recomienda sospechar de cualquier sorteo en el que no se haya participado, así como de herencias de desconocidos. Se desaconseja, además, acceder a páginas web a través de enlaces incluidos en correos o en mensajes de remitente desconocido y advierte de que no se deben proporcionar nunca datos personales de la banca 'online' ni de las tarjetas de crédito.

Falsas tiendas online
Estas tiendas web fraudulentas, de apariencia similar a las oficiales, utilizan como reclamo grandes ofertas para el consumidor con precios muy por debajo de mercado. Los ciberdelincuentes se comprometen al envío rápido de los bienes adquiridos y solicitan a la víctima datos de filiación y bancarios, pero una vez abonado el pago y completada la compra, los productos nunca llegan y las páginas desaparecen sin dejar rastro. En estos casos, se aconseja consultar la información legal de la empresa y prestar atención a la apariencia de las páginas web que, aunque tratan de imitar plataformas oficiales, pueden estar mal construidas y estructuradas. Se recomienda también desconfiar de las páginas que no admiten protocolos de doble autenticación y pinchar en el candado de seguridad que figura en la dirección URL para comprobar su fecha de creación, puesto que los ciberdelincuentes crean dominios para periodos temporales muy concretos y reducidos.

Estafa de los códigos QR
Asimismo, los ciberdelincuentes también aprovechan la amplia implantación de los códigos QR para sustituir códigos reales -por ejemplo, de restaurantes o de multas de estacionamiento- por otros falsos que redirigen al usuario a una pasarela de pago falsa. Para evitar estas situaciones, se aconseja consultar directamente con el establecimiento si el usuario escanea un código de un restaurante para su pago que le redirige a una web sospechosa. En el caso de las sanciones por aparcamiento, es recomendable comprobar en internet la veracidad de la multa contrastando los datos con el emisor de la denuncia. Y si el usuario ya ha introducido los datos en la pasarela de pago falsa, entonces, se debe contactar de manera inmediata con la entidad bancaria para intentar evitar el cobro fraudulento.

Skimming
Otra estafa recurrente es aquella en la que los ciberdelincuentes utilizan el copiado físico de la tarjeta bancaria mediante la instalación de dispositivos camuflados en cajeros o terminales bancarias con la finalidad de obtener el contenido de la banda magnética para proceder a su clonado. Con el fin de evitar este robo, se recomienda prestar atención a la estructura de los cajeros automáticos y comprobar que el teclado o el hueco reservado para la tarjeta no estén manipulados.

Financiado por la Unión Europea. Las opiniones y los puntos de vista expresados son exclusivamente los del autor o autores y no reflejan necesariamente los de la Unión Europea ni los del Consejo Europeo de Innovación y la Agencia Ejecutiva de Pequeña y Mediana Empresa (EISMEA). Ni la Unión Europea ni la autoridad que concede la financiación pueden ser consideradas responsables de los mismos.

Carding
En los casos de carding, los ciberdelincuentes adquieren los datos de la tarjeta bancaria para su uso fraudulento a través de distintas técnicas, como el envío de enlaces, el uso de falsas páginas web, las notificaciones de supuestas compañías telefónicas, etc. La recomendación es que cuando se realiza un pago por Internet, el usuario se asegure de que los pagos se realizan en plataformas que permiten autorización bancaria y no se facilite nunca por teléfono el número completo de la tarjeta bancaria.

Peligros de proporcionar el número de la cuenta
Por otro lado, ocurre que para realizar numerosas gestiones en nuestro día a día, por ejemplo, al inscribirnos en un gimnasio o realizar una compra online, nos vemos obligados a facilitar nuestro número de la cuenta bancaria, lo cual puede plantearnos algunas dudas sobre los riesgos que este hecho puede conllevar. Con el fin de despejar estas dudas, Banco de España aclara que el mero hecho de que un tercero conozca nuestro número de cuenta bancaria no le permitirá extraer dinero.

Ahora bien, si además del número de la cuenta conoce nuestro DNI, en algunos casos, podría realizar una domiciliación de recibos. Si esto ocurre, cuando se produzca un cargo en la cuenta que no sea nuestro, la solución es fácil y rápida ya que podremos devolverlo sin problemas. Si, además, un tercero dispone del número de tarjeta de débito o crédito, en este caso podría hacer movimientos y robar el dinero. En este sentido, Banco de España recuerda algunas precauciones que hay que adoptar para utilizar de forma responsable la tarjeta bancaria y reducir el riesgo:

-No anotar ni llevar el pin o claves de seguridad escritas en un papel.
-En los cajeros, que nadie te vea marcar el pin.
-Comprobar los extractos del banco para detectar movimientos sospechosos.
-No utilizar la tarjeta de crédito como identificación personal.
-En las compras online, utilizar la autenticación reforzada, es decir, al menos dos factores de identificación independientes.

Fuente de la información: Ministerio del Interior

Folleto: Fraudes y Estafas Comerciales

Financiado por la Unión Europea. Las opiniones y los puntos de vista expresados son exclusivamente los del autor o autores y no reflejan necesariamente los de la Unión Europea ni los del Consejo Europeo de Innovación y la Agencia Ejecutiva de Pequeña y Mediana Empresa (EISMEA). Ni la Unión Europea ni la autoridad que concede la financiación pueden ser consideradas responsables de los mismos.