FRAUDE DIGITAL

LA MEJOR PROTECCIÓN ANTE LOS CIBERATAQUES: EL CONOCIMIENTO

GRUPO COOPERATIVO CAJAMAR

LA MEJOR PROTECCIÓN ANTE LOS CIBERATAQUES: EL CONOCIMIENTO

¿Cómo no caer en la trampa?

Siempre pensamos que a nosotros no nos va a pasar, no nos van a atacar y no vamos a caer en el engaño, pero la realidad nos demuestra que nos equivocamos y que todos debemos invertir en seguridad de nuestros dispositivos, así como tiempo en formarnos y conocer cuales son los principales peligros que nos podemos encontrar.

Para empezar es importante conocer la **diferencia entre un Fraude y una Estafa**:

FRAUDE
Consiguen tus credenciales y son los ciberdelincuentes los que realizan una operación fraudulenta.

ESTAFA
Los ciberdelincuentes engañan a la víctima para que realice voluntariamente un pago fraudulento. En estos casos, no hay robo de credenciales.

Casos más habituales que se dan de Fraude:

SMISHING Y PHISHING

Recibes un SMS (smishing) o correo electrónico (phishing) de alguien haciéndose pasar por un banco u otra empresa (de envíos, principalmente) con un enlace que te dirige a una web falsa para conseguir tus datos personales, claves o para que descargues un programa o app maliciosos.

VISHING

Recibes una llamada de alguien haciéndose pasar por tu banco alertándote de que tienes una incidencia con tu tarjeta, cuenta bancaria o alguna transacción pendiente de anular para conseguir tu Clave de Acceso, Clave de Firma o las claves de confirmación de tus operativas que enviamos por SMS. Y ten mucho cuidado porque pueden simular que te llaman desde el teléfono del banco.

RAT (REMOTE ADMINISTRATION TOOL)

Recibes una llamada de una empresa de servicios en la que te piden instalar un programa supuestamente legítimo para ayudarte a solucionar un problema que tienes con tu ordenador, con el fin de obtener acceso remoto a tu dispositivo. Una vez tengan el control de tu dispositivo pueden acceder a tus claves, obtener datos confidenciales, realizar transacciones, etc.

MALWARE BANCARIO

El malware se puede instalar descargando algún programa aparentemente seguro, entrando en páginas web infectadas o haciendo clic en anuncios o enlaces fraudulentos recibidos por correo o SMS. Si tu dispositivo está comprometido, los ciberdelincuentes pueden obtener acceso directo a tus SMS para obtener, por ejemplo, el código de confirmación que te enviamos para tus operativas, y así conseguir tus datos de tarjetas y acceso a la web y app del banco.

GRUPO COOPERATIVO CAJAMAR

Casos de Fraude en operaciones con tarjeta:

Los sms suplantando la identidad de empresas de correos, en los que se le indica al cliente tiene un producto pendiente de entrega, retenido en aduana, y tiene que realizar un pago de entre 1,50 - 2,00 € para poder recibir su mercancía.

El cliente cree que está realizando el pago por este importe y en este concepto, recibe un código OTP para autenticar la transacción, pero en este caso de enrolamiento de su tarjeta a un dispositivo móvil fraudulento.

Los sms suplantando a terceros (Ej. Correos, MRV, Agencia Tributaria, etc.) en los que le indican al cliente tienen en algún concepto de abono el pago o devolución a su favor.

Le solicitan al cliente datos de su tarjeta y que autentique para poder recibir este abono, igual que en el caso anterior el cliente lo que está autenticando con el código OTP recibido es el enrolamiento de su tarjeta a un dispositivo móvil fraudulento.

Casos más habituales que se dan de Estafa:

POR REDES SOCIALES
Contactan contigo, habitualmente por Whatsapp, haciéndose pasar por un familiar o amigo cercano que tiene un problema y te piden que les hagas una transferencia.

BIZUM "INVERSO"
Te piden que aceptes un Bizum haciéndote creer que recibes el dinero, pero realmente te están enviando una solicitud de cobro.

COMPRA O BENEFICIARIO MALICIOSO
Te piden que pagues por adelantado una compra o servicio que nunca vas a recibir o disfrutar. Por ejemplo, en el pago de alquileres vacacionales, especialmente comunes durante el verano.

DE INVERSIÓN
Te convencen para que traslades tu dinero a un fondo ficticio o que realices una inversión falsa.

Casos de Estafa en operaciones con tarjeta:

Las producidas en la compra/venta de productos/servicios realizadas a través de operaciones de dinero con tarjeta.

Ya sea casos de compras de productos a un precio muy rebajado, que el comprador nunca va a recibir o no va a tener nada que ver con el producto inicial ofertado.
Ya sea casos en los que un falso comprador solicitar al vendedor datos de su tarjeta (numeración, cvv y caducidad) para hacerle el pago y le pide que autentique las operaciones. Realmente lo que está autenticando el vendedor son pagos con cargo a su tarjeta.

Reservas de hotel en la que los ciberdelincuentes se hacen pasar por el establecimiento y contactan con el cliente, bien a través de correo Phishing o incluso llamada telefónica fraudulenta, en la que instan al comprador a realizar el pago de la operación si no quiere perder su reserva.

En cualquier caso...

¿Qué hacer en caso de detectar estás siendo objeto de alguna de todas las casuísticas descritas?

No facilites nunca tus claves a nadie, no piques en enlaces ni descargues una aplicación que pudiera haberte llegado a través de algún contacto que no sea de confianza.

No facilites datos de tus tarjetas a particulares.

Jamás autentiques una transacción que te indican debes validar para poder recibir el abono del artículo que tienes en venta. Una transacción de abono no requiere autenticación.

Desconfía cuando te indiquen debes pagar mediante operaciones de dinero, más cuando se trate de productos a un precio mucho más bajo del habitual.

Si te indican que no han recibido el cargo/abono y te piden repitas la transacción, comprueba tu B.E. antes de hacer nada.

Confirma la identidad del comercio o del comprador, antes de validar cualquier operación con tarjeta.

Usa el sentido común si recibes llamadas telefónicas o emails pidiéndote hacer alguna operación bancaria de forma urgente para no perder un producto o servicio. No tengas prisa, desconfía.

Si crees que puedes estar siendo objeto de un ciberataque o tienes alguna duda, contacta con nosotros a través de este formulario o llámanos al **914 23 00 29** o al número gratuito **900 15 10 10**.