CONSEJOS PARA PREVENIR EL FRAUDE EN OPERACIONES BANCARIAS

Iniciativa Educativa del Banco de España

Esta es una iniciativa del Banco de España destinada a divulgar conocimientos básicos de Educación Financiera entre la ciudadanía española. Por favor, tenga en cuenta que **la modificación de los contenidos no está autorizada**.

Gracias.

A. COLECTIVOS DESTINATARIOS: toda la población, a un nivel básico.

B. OBJETIVOS:

- Tomar conciencia del aumento del fraude en el entorno digital y en qué manera puede afectar a nuestro bolsillo
- Informar de los métodos más habituales que utilizan los estafadores para engañarnos
- Proponer consejos para protegernos contra el fraude
- Recalcar que el uso del sentido común es el arma más eficaz contra el fraude, habida cuenta de los nuevos métodos de fraude que van apareciendo

C. CONTENIDOS

0. Introducción

1. Datos

2. Tipos de fraude más habituales
   - 2.1. Sms o emails suplantando a los bancos
     - Smishing
     - Spoofing
   - 2.2. SMS o emails suplantando a empresas de mensajería
     - Phishing
   - 2.3. Falsos reembolsos de telefonía o electricidad
   - 2.4. Fraude en plataformas de segunda mano como Wallapop o Vinted
   - 2.5. Más tipos de fraude
     - Fraude del técnico informático
     - Vishing
     - Estafas a través de Bizum
     - Qrishing

3. Consejos para protegerte

---

0. Introducción:

La digitalización de los servicios y productos bancarios es una realidad cada vez más común y, como usuarios, nos es de utilidad conocer sus oportunidades y también los nuevos riesgos que pueden surgir.

En el año 2007 Apple lanzó al mercado el primer iPhone. Este hecho marcó el comienzo de la generalización de los smartphones en el mundo, que se culminó en la década de 2010 a 2020. Este hecho, junto con la crisis financiera global del año 2008, supusieron dos hitos que pueden marcar el punto de partida de la digitalización financiera (si bien esta ya había comenzado unos años atrás).

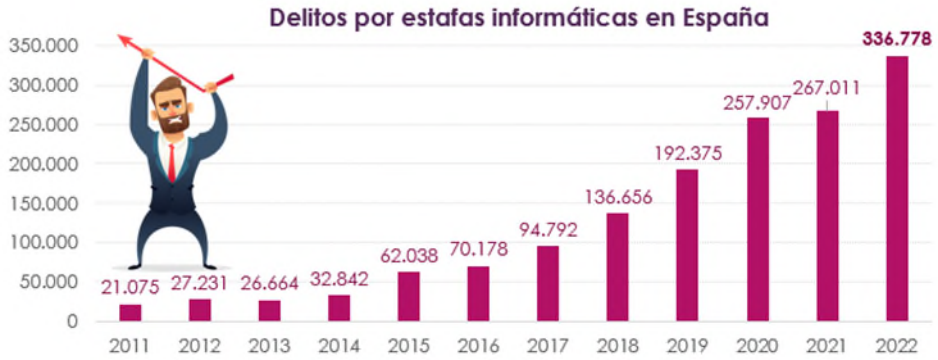
La digitalización fue acelerada con la pandemia de COVID-19. La pandemia también trajo una concienciación de los organismos internacionales y los gobiernos sobre la necesidad de centrarse en las finanzas de las personas y los hogares, para mejorar la resiliencia financiera y mejorar la preparación frente a diversas perturbaciones.

Como se indicaba anteriormente, la crisis de COVID-19 también aceleró el cambio hacia la digitalización en numerosos ámbitos: en servicios financieros, salud, comunicación, etc., con los con crecientes riesgos de exclusión digital.

Con carácter general, **una estafa financiera es una acción realizada por una persona o empresa que, mediante engaño y con ánimo de lucro, causa un perjuicio económico a un tercero**. Las consecuencias de este tipo de estafas pueden ser muy graves y provocar grandes pérdidas económicas. Existen muchos tipos de estafas financieras que en los últimos años se han visto incrementados debido a las posibilidades que permiten las nuevas tecnologías y las redes sociales.

1. Datos:

En esta diapositiva únicamente bastaría con comentar los datos que aparecen, para poner en contexto a los asistentes.



Fuentes:

1. INE
2. Fuente: INE
3. Fuente: Eurostat
4. Fuente: Balance de Criminalidad del Ministerio de Interior (4T 2022)

2. Tipos de fraude más habituales

2.1. SMS o emails suplantando a los bancos:

Seguramente hayáis recibido algún SMS o email procedente, supuestamente, de vuestro banco, en los que os solicitan que realicéis una determinada acción, como proporcionar datos (PIN, contraseña, clave online de banca digital, clave de firma, etc.).

Los ciberdelincuentes cada vez emplean técnicas más sofisticadas. No solo se hacen pasar por quienes no son, sino que también imitan y suplantan los canales habituales de contacto de los bancos.

El **smishing** es el envío de un SMS a tu móvil simulando ser tu banco con el objetivo de robarte información privada o hacerte un cargo económico, generalmente adjuntado un enlace a una página fraudulenta. Suelen ser más o menos fáciles de detectar.

No obstante, cabe la posibilidad de que estos SMS aparezcan en la misma sección donde con anterioridad habían llegado otros SMS reales de la entidad como los que te envían para las autorizaciones de pagos. ¿Cómo es eso posible? Cabe reemplazar el número de teléfono móvil desde el cual se envía el mensaje por un texto alfanumérico que aparenta ser la entidad, para que el destinatario, cuando lo reciba, no sospeche del emisor y acceda a realizar la operativa solicitada. Esta técnica, conocida como SMS **spoofing**, se realiza mediante diversas páginas web y aplicaciones móviles que permiten enviar SMS desde una fuente desconocida suplantando una identidad conocida con relativa facilidad.

Como puede apreciarse, en todos los ejemplos que se muestran en la pantalla, el mensaje nos alerta de algo supuestamente sospechoso, fraudulento o anómalo: acceso no autorizado a la banca online, operativa en la tarjeta limitada por razones de seguridad, caducidad de la tarjeta, etc.

En estos casos, los **consejos** a seguir son los siguientes:

- En el caso de los SMS, tanto iOS como Android incorporan por defecto detectores de spam y bloquean la entrada de este tipo de mensajes. Si aun así consiguen llegar a la bandeja de entrada, normalmente aparece un símbolo de advertencia. Si lo ves, sospecha.
- Aunque los recibes en el mismo sitio que el resto de mensajes de la entidad, fíjate en el formato o contenido, o si tienen faltas de ortografía.
- Fíjate en la URL a la que te invitan a pinchar. Siempre hay algo raro que te debe invitar a sospechar.
- Activa las notificaciones de la app de tu banco. Si hay algo que tu banco deba hacerte saber, lo hará a través de una notificación de la app.
- Siempre opera a través de la app del banco en lugar de utilizar el navegador de internet.
- En cualquier caso, recuerda que desde la entidad nunca te pedirán que les facilites contraseñas o claves completas.
- Si te llaman por teléfono haciéndose pasar por tu banco, usa el sentido común: coteja que lo que te dicen realmente es verdad, por ejemplo, si te llaman diciéndote que se ha hecho

una operación fraudulenta, accede a tu posición y verifica que es cierto. O si no te cuadra lo que te dicen, cuelgas y les llamas tú.

- Si no has realizado tú una operación, no tiene sentido que te llegue una clave temporal y mucho menos que el banco sea quien te la solicite verbalmente por teléfono. Y no, tu banco no necesita un código para anular esa supuesta operación fraudulenta.
- Nunca pinches en un enlace que provenga supuestamente de tu banco. Ante la más mínima duda, llama a tu entidad y pregunta.
- Si aun así pinchas en el enlace, te llevará a una página web que sea prácticamente idéntica a la de tu banco. En este caso, comprueba la url en la que estás, ya que será muy parecida a la de tu banco, pero no será la misma. Por ejemplo, en lugar de https://www.bancosantander.es/particulares será algo así como https://www.info.bancosantander.es/particulares, https://www.bancosantander.xyz
- Si has pinchado en el enlace, pincha en el icono del candado de tu navegador; si la página web es segura, se te indicará que la conexión es segura.

2.2. SMS o emails suplantando a empresas de mensajería:

Correos, FedEx, DHL, MRW… da igual la compañía, todas son utilizadas como gancho, usando las palabras mágicas “pedido de Amazon” como reclamo también.

Los ganchos de estos mensajes son variados: algunos te avisan que tienes que pagar tasas de aduana, otros te piden confirmar tus credenciales o devolverán el paquete, y otros simplemente te dan un enlace de seguimiento del paquete. Todos te llevan a una página de **phishing** que suplanta a la empresa de mensajería y te solicitan tus datos personales o te piden instalar una aplicación que es maliciosa.

Lo más común es que te pidan realizar un pequeño pago para “desbloquear” la situación de tu paquete. Tras pinchar en el enlace que te facilitan, y una vez dentro de la página web que suplanta a la empresa de mensajería, aparecerá un TPV virtual en el que te pedirán que introduzcas los números de tu tarjeta, la fecha de caducidad y el CVC (el número verificador que normalmente se encuentra en la parte trasera de la tarjeta). Con ello, ya tienen los datos de tu tarjeta.

En estos casos, los **consejos** a seguir son los siguientes:

- Aplicar la cautela, aún en los mensajes de organismos oficiales. Es muy sencillo fabricar un email o SMS falso que parezca real.
- Prestar atención al texto de mensaje. Las empresas reconocidas u organismos oficiales no envían correos electrónicos con un formato erróneo, faltas gramaticales o de ortografía.
- No abrir documentos adjuntos o hacer clic en enlaces de los correos electrónicos de los servicios de entrega, especialmente si el remitente insiste en ello. Es preferible acudir a la página web oficial e iniciar sesión desde allí.

- Si tienes dudas, llama tú a la empresa de mensajería y pide información. Seguramente, no seas el primero que llama por el mismo asunto, y la empresa de mensajería te dará orientaciones sobre cómo proceder.
- Utiliza un antivirus y mantén actualizado tu sistema operativo.

2.3. Falsos reembolsos de empresas de telefonía o electricidad:

Te llega un SMS haciéndose pasar por grandes empresas como Movistar o Iberdrola, donde te avisan que ya tienes disponible tu factura y que puedes reclamar un reembolso de X dinero. Después, te llevan a un enlace de phishing y tratan de robar tus datos allí.

Los **consejos** son los mismos que en las diapositivas anteriores. El principal es que, ante la más mínima duda, debes llamar tú mismo a la empresa de la que supuestamente estás recibiendo la comunicación sospechosa. Esta pequeña medida de cautela es siempre la más importante.

2.4. Fraude en plataformas de segunda mano como Wallapop o Vinted:

En la imagen de la izquierda, esta estafa en concreto nos propone desbloquear el chat donde queremos hablar pulsando sobre un enlace externo. Todo con la excusa de que el vendedor nos ha respondido (presunto defraudador) y que debemos entrar en el enlace para poder comenzar a hablar. A partir de ahí nos llevan a una supuesta app patrocinada que no existe, que suplanta el aspecto de Wallapop, y que ha sido diseñada para poder hacerse con nuestros datos bancarios, el objetivo final de toda acción fraudulenta de phishing. El mejor consejo que se puede dar a los usuarios de la app es que nunca abran un enlace externo dentro de la app, ya que no es ni mucho menos una acción amparada por la app.

En la imagen de la derecha, nos piden los datos bancarios para efectuar la transacción (también podrían pedirnos el número de tarjeta). El denominador común suele ser que el ciberdelincuente intenta convencer al afectado para hacer la transacción fuera del sistema de seguridad del que disponen Wallapop y Vinted, recurriendo a WhatsApp o apps similares de mensajería instantánea.

2.5. Más tipos de fraude:

- Fraude del técnico informático
- Vishing
- Estafas a través de Bizum
- Qrishing

3. Consejos para protegerte:

1. **Cuida tus claves personales.** Tu banco nunca te pedirá que facilites claves por correo electrónico o SMS. Utiliza contraseñas distintas para aquellas cuentas importantes y modifícalas periódicamente.
2. **Vigila SMS o mail sospechosos.** Comprueba la dirección electrónica de cualquier mensaje cuyo remitente sea desconocido. Si contienen enlaces, verifícalos con el cursor sin pinchar antes de acceder, y evita abrir archivos adjuntos
3. **Si aun así pinchas, atiende a la apariencia de la web, comprueba que tenga el candado al lado de la barra de exploración.**
4. **Mira a ver si hay faltas de ortografía o algo te parece raro.**
5. **Protege tus accesos electrónicos.** Accede a la banca electrónica mediante la APP de tu banco, instala un antivirus para mantener la seguridad de tu sistema operativo, y bloquea tu dispositivo mediante una contraseña.
6. **Utiliza tarjetas prepago en comercios online.** Pagar con este tipo de tarjetas te permite limitar la pérdida de dinero en caso de un posible fraude.
7. **Presta atención a los descubiertos.** Revisa si tu cuenta los permite o no. Ten en cuenta que en caso de fraude la posibilidad de incurrir en descubierto aumenta el posible impacto del fraude.
8. **Mantén un saldo apropiado en la cuenta que uses a diario.** Asocia tu tarjeta de débito a una cuenta que tenga un saldo ajustado a tus necesidades habituales y traslada el resto de ahorros a otros productos.
9. **Consulta los movimientos de tu cuenta corriente.** Revisa frecuentemente los movimientos de tu cuenta para tener controlados todos tus gastos.
10. **Y lo más importante de todo… El más importante. Usa el sentido común. El fraude suele producirse cuando tú recibes una llamada, un SMS o un email en el que te acaban pidiendo algo y metiéndote prisa. Nunca atiendas las peticiones de realizar ninguna acción en ese momento, y dirígete tú a tu entidad, o a la empresa de la que estás recibiendo una comunicación sospechosa, para asegurarte de con quien estás hablando.**

Recuerda que existe un apartado específico orientado a la prevención del fraude en el portal de cliente bancario donde hay muchos contenidos relacionados con los tipos de fraude y el mejor modo de evitarlos. También CNMV ha desarrollado contenidos para prevenir el fraude en las operaciones relativas a los productos de inversión.

Para ampliar información sobre medidas de ciberseguridad, no dejes de visitar la página web del Instituto Nacional de Ciberseguridad.