MOOC

INCLUSIÓN DIGITAL Y FINANCIERA PARA EL MUNDO RURAL

Módulo 6.
Utiliza la banca online de forma segura

DIPUTACIÓN DE CÁCERES

Módulo 6. Utiliza la banca online de forma segura

A pesar de todo lo visto ¿te da un poco de reparo eso de utilizar la banca en línea? ¿No tienes muy claro en qué debes fijarte para saber si un sitio es seguro?

No podíamos terminar esta formación de otra forma que dándote algunas claves para que puedas moverte en el mundo online con total seguridad. Normalmente, los sistemas informáticos que utiliza la banca en internet son muy seguros, pero si es verdad que debemos hacer un uso correcto de ellos.

Por eso es muy importante que conozcamos cómo pueden robarnos nuestros datos bancarios, o cómo pueden acceder a nuestras cuentas... y más importante todavía es saber qué podemos hacer para prevenirlo.

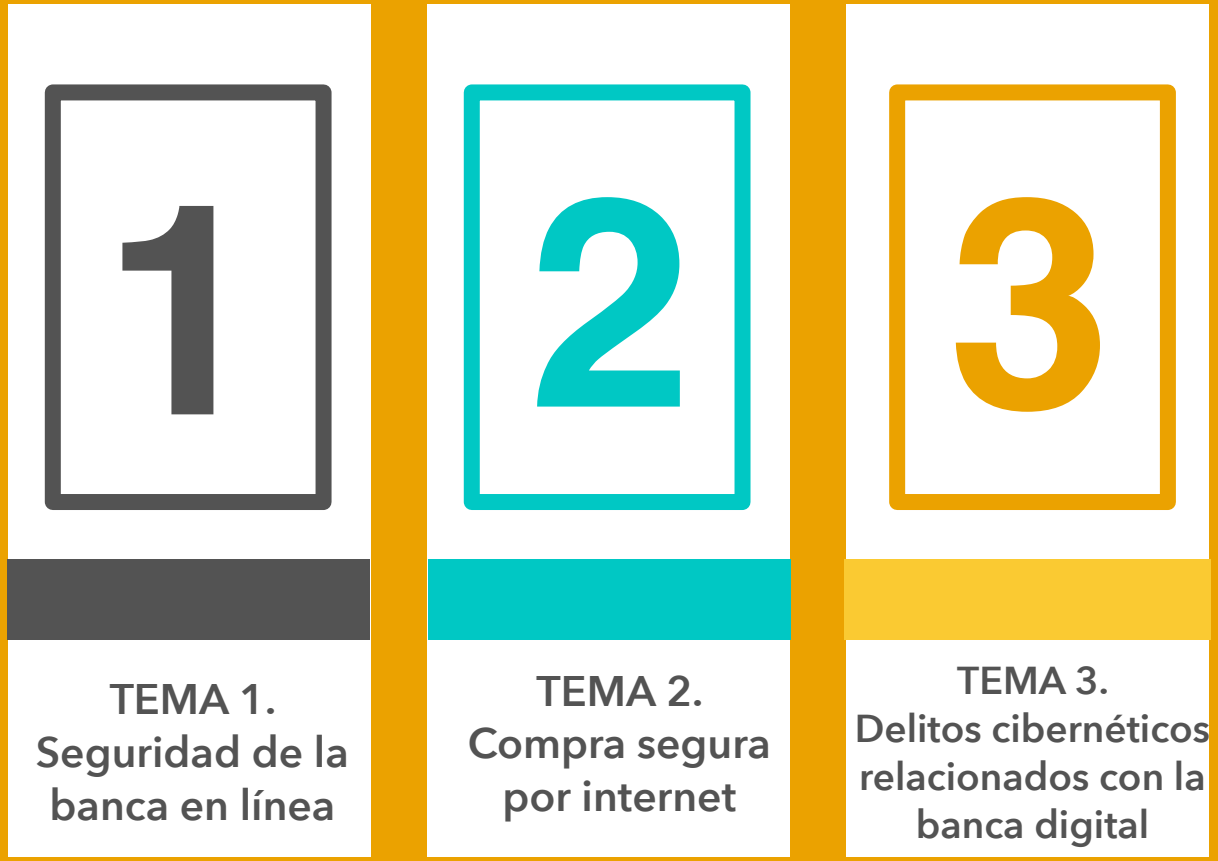
¿Qué aprenderemos?

- Cómo tener seguridad utilizando la banca en línea
- A realizar compras seguras por internet
- Identificar principales delitos cibernéticos relacionados con la banca digital

DIPUTACIÓN DE CÁCERES

Módulo 6. **Utiliza la banca online de forma segura**

MOOC **Inclusión digital y financiera para el mundo rural |**



Tema 1.

Seguridad de la banca en línea

En este tema vamos a:

- Detectar los principales tipos de fraude
- Conocer cómo prevenirlos

Entendiendo “eso” de la seguridad de la banca en línea

Debemos entender ...

Que la banca online es de gran utilidad y casi todas las entidades bancarias ya disponen de este servicio, por sus múltiples ventajas ya estudiadas.

Sin embargo **la desventaja más habitual es la desconfianza** que produce frente a la banca tradicional, sobre todo **en cuanto a términos de protección de datos y seguridad.**

Debemos entender ...

En general, los sistemas informáticos que utiliza la banca en Internet son seguros, pero tenemos que asegurarnos de hacer un correcto uso de ellos, ya que la mayoría de los problemas relacionados con la seguridad, tienen que ver con un error de la persona usuaria.

Por eso es muy importante conocer los riesgos que existen para estar seguros y seguras a la hora de su utilización y evitar problemas como el robo de nuestros datos bancarios o el acceso a nuestras cuentas bancarias o contraseñas.

Principales técnicas de fraude

A continuación, vamos a conocer las técnicas que más suelen emplearse para realizar fraudes, engaños y estafas a través de Internet.

- Phishing
- Pharming
- Spoofing
- Troyanos

Phishing

El "phishing" es una modalidad de estafa diseñada con la finalidad de **robar nuestra identidad.** Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico y ventanas emergentes.

Esta técnica consiste en el envío de un correo electrónico en el que, un/a ciberdelincuente (conocido como “phisher”), se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.

Phishing

A través de este correo electrónico, pretende hacernos creer que es nuestra entidad bancaria y a través de un enlace, **nos solicita información personal y bancaria, incluso nuestras claves de acceso a la cuenta**. En el caso de los bancos o entidades financieras se ha producido un incremento exponencial del número de ataques de phishing.

Dado que los mensajes y los sitios Web que envían desde la ciberdelincuencia parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos.

Phishing

Antiguamente, se enviaban aleatoriamente a todos los correos que se pudiese, esperando que por casualidad alguno de los receptores fuese usuario de esa entidad. **Actualmente, los estafadores han afinado mucho sus técnicas de forma que pueden incluso detectar cuál es la entidad con la que opera cada usuario y enviarle un correo "personalizado"**.

Un email de tipo phishing también puede llevar un archivo adjunto infectado con software malicioso. El objetivo de este programa maligno es infectar el equipo del usuario y robar su información confidencial.

Si recibimos estos mensajes...

- **No debemos responder nunca a solicitudes de información personal a través de correo electrónico. Las empresas nunca piden contraseñas, números de tarjeta de crédito u otro tipo de información personal por correo electrónico.**
- Para visitar sitios Web, debemos introducir la dirección URL en la barra de direcciones. Si sospechamos de la legitimidad de un mensaje de correo electrónico, que realmente no lo envía quien aparece como remitente, no debemos pinchar en los enlaces que tenga.

Si recibimos estos mensajes...

- Debemos comunicar los posibles delitos relacionados con nuestra información personal a las autoridades competentes. Si creemos que hemos sido víctima de "phishing", debemos informar inmediatamente a nuestro banco, dar de baja la tarjeta y bloquear el número de cuenta bancaria
- Si ya hemos sufrido alguna pérdida económica debemos ponerlo en conocimiento de la policía.

Pharming

El “pharming” (palabra compuesta por phishing y farming), es un paso más en las técnicas de phishing, que **consiste en manipular las direcciones de las páginas web que utilizamos**. La ciberdelincuencia redirecciona una página web de un supuesto sitio oficial, es decir, que nos envían sin quererlo a otra página web con el mismo aspecto que la oficial pero que ha sido creada por el/la hacker.

La página web falsa suele parecerse mucho a la real, por lo que, por lo general, las víctimas no sospechan que algo no va bien.

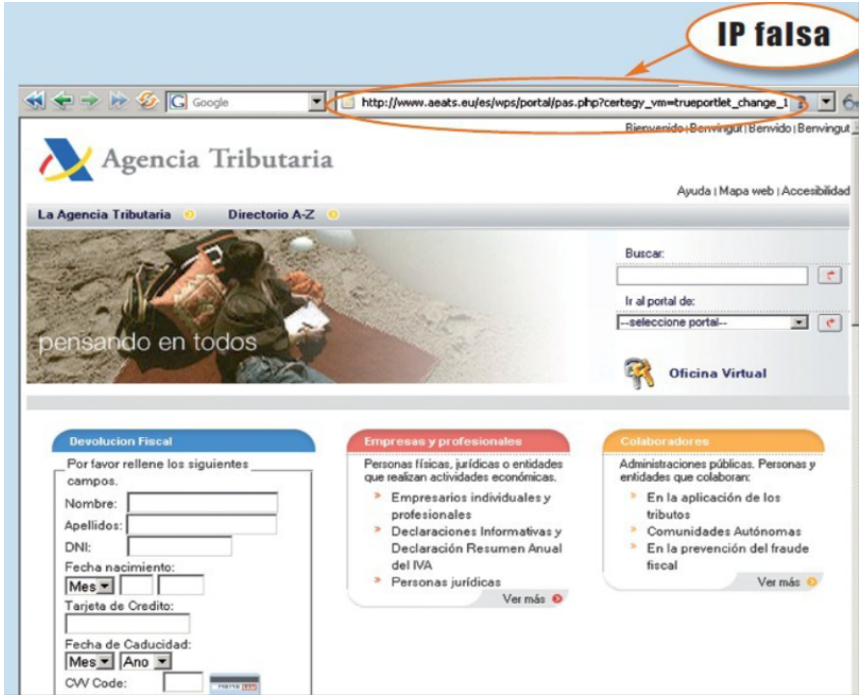
Pharming

Tanto los ataques de phishing como de pharming utilizan información fraudulenta que parece legítima y veraz para **engañar a las personas usuarias con el objetivo de que compartan información confidencial.** Se diferencian en que el phishing se lleva a cabo principalmente mediante el uso de correos electrónicos falsos, mientras que el pharming ocurre a través de páginas web falsas.

➡ En la siguiente imagen podemos ver un *ejemplo* de este tipo de estafa, cuyo diseño es muy similar a la página oficial y puede ser confundida fácilmente. Sin embargo, si nos fijamos en la barra de dirección, podemos ver de forma clara que no es una fuente oficial.

Ejemplo Pharming

En esta página web falsa, introduciremos nuestros datos confidenciales sin ningún temor, pensando que estamos actuando con la **Agencia Tributaria,** sin saber que los estamos remitiendo a un/a delincuente. Luego estos datos de tarjetas de crédito, cuentas y claves podrán ser utilizados maliciosamente para realizar movimientos de dinero con cargo a los fondos de o desde una tarjeta de crédito/débito.



Este fraude puede realizarse de diversas maneras

- Se puede crear un dominio con nombre muy similar al de la web que se quiere suplantar y se trata de confundir a la persona, que habitualmente no comprueba que es el nombre real. En el ejemplo anterior aparece “eaets”, jugando con las iniciales de la Agencia Estatal de la Administración Tributaria, para crear la ficción de que es real.
- Se puede crear un enlace falso que, a partir de otras webs, nos lleven a la web falsificada. Se puede combinar con el phishing añadiéndole el enlace falso al e-mail fraudulento.
- Los/las piratas informáticos/as intentan conseguir información personal para poder acceder a nuestras cuentas bancarias, robar la identidad o cometer otro tipo de fraudes con el nombre de la persona, de manera que los bancos y otros sitios financieros similares, son el objetivo de estos ataques.

Para evitar caer en esta trampa

- Debemos navegar por Internet con precaución. Si estamos consultando una página habitual debemos comprobar que el aspecto de la web es el habitual.
- Debemos fijarnos en que la web no tenga faltas de ortografías importantes, observar los logos, que no tenga logotipos falsificados, mirar bien la dirección URL …
- **Instalar en nuestro ordenador un software antimalware** (software que tiene como objetivo infiltrarse en su ordenador para recabar información), ya que el pharming suele estar causados por troyanos.

Para evitar caer en esta trampa

- Debemos seguir los consejos básicos sobre seguridad en Internet:
  - ✓ Utilizar un antivirus y mantenerlo actualizado.
  - ✓ Vigilar que la página web comience por https://
  - ✓ Comprobar que en las webs visitadas aparece el símbolo de navegación segura.
- Desconfiar de aplicaciones que prometen mostrarte quiénes te han eliminado de alguna red social.
- No fiarse de los regalos, concursos o promociones fáciles de obtener que nos llegan en Internet o al correo, ni responder a mensajes que solicitan datos en forma urgente.

Para evitar caer en esta trampa

- **No usar la opción “guardar contraseña” en las pantallas iniciales de sitios de Internet.**
- Desconfiar de los enlaces: verificar el dominio al cual apunta un enlace, antes de hacer clic o enviar datos a un mail.

Spoofing

El Spoofing (suplantación de identidad), consiste en diferentes técnicas que los/las hackers utilizan para la **suplantación de una tercera persona**: su página web, su correo o su identidad electrónica, **con la finalidad de obtener información** (sitios web visitados, claves personales, información privada del usuario, etc).

El Spoofing puede producirse también **con un reclamo en forma de recompensa**, mediante anuncios o enlaces a páginas web puestos en lugares no controlados como foros de Internet o enviados a directamente a nuestro correo electrónico.

En el entorno bancario, los principales tipos de Spoofing que se utilizan son el SMS Spoofing y el ID Spoofing (conocido como Spoofing telefónico).

SMS Spoofing

El **SMS SPOOFING** se trata de una suplantación de identidad por SMS que consiste en enviar un mensaje de texto (SMS) al teléfono de la víctima que simula ser de su banco con el objetivo de que le facilite la información necesaria para cometer la estafa o cualquier otro delito. Este SMS es modificado (cambiando el número de teléfono original que envió el SMS por otro, añadiendo el nombre de la entidad en el FROM del SMS, etc.) para que parezca ser un mensaje oficial de la entidad bancaria y que entre en el hilo de mensajes originales del banco recibidos por la persona.

Estos SMS falsos contendrán un enlace a una página web falsa parecida a una página web original del banco en cuestión.

ID Spoofing

El **ID SPOOFING** (conocido como Spoofing telefónico) trata de que la persona reciba indicaciones para llamar a un número de teléfono donde se le solicitará el usuario y la contraseña de su banca electrónica, el código que envía el banco al móvil para acceder o el número de tarjeta, fecha de caducidad y CVV/CVC (tres dígitos de la parte de atrás de la tarjeta).

Algunos consejos y advertencias

- **Recuerda que los bancos o entidades financieras nunca solicitarán a sus clientes a través de ningún medio como SMS, llamada telefónica, correo electrónico, etc. que proporcionen credenciales de la banca electrónica** (usuario y contraseña, código que envían al teléfono móvil), ni ninguna otra información como la numeración de la tarjeta, fecha de caducidad y los tres dígitos de control necesarios para efectuar compras online.
- Utiliza siempre un buen antivirus y mantenlo actualizado.
- Haz caso de los avisos que su navegador o servidor de correo electrónico acerca de la fiabilidad de sitios web visitados o seguridad de correos electrónicos recibidos.

Troyanos

Se le llama troyano a un **programa malicioso capaz de alojarse en los ordenadores y permitir el acceso a usuarios externos**, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente un ordenador.

Un troyano no es en sí un virus. Para que un programa sea un "troyano" sólo tiene que acceder y controlar el ordenador anfitrión sin ser advertido. Al contrario que un virus, que es destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Además, a diferencia de los virus y los gusanos informáticos, los troyanos no pueden multiplicarse.

Troyanos

Suelen ser programas alojados dentro de una aplicación o programa instalado en nuestro ordenador, **una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene.**

Habitualmente se utiliza para espiar a la persona usuaria:

- ✓ Lee contraseñas
- ✓ Registra las pulsaciones del teclado
- ✓ Elimina datos
- ✓ Bloquea datos
- ✓ Modifica datos
- ✓ Interrumpe el rendimiento de equipos informáticos

Troyanos

Se llama troyano por su cierto parecido a la historia del caballo de Troya, que suele llegar como un regalo (una imagen, un archivo de música, todo aparentemente inofensivo…) y una vez dentro lo que hace es abrir la puerta para que entre "lo malo". Al igual que en la historia del caballo de Troya, el troyano es inofensivo, lo que ataca es lo que lleva dentro.

Se conocen varios tipos de troyanos: Rootkit, Dropper, DDoS… y entre ellos se encuentran los troyanos bancarios.

Los troyanos bancarios son algunos de los troyanos informáticos más extendidos por la aceptación cada vez mayor de la banca en línea y por el mal uso de esta por parte de algunas personas. **Su objetivo es obtener las credenciales de acceso a las cuentas bancarias.**

Para evitar que se instalen troyanos en nuestro ordenador

- **Utilizar sólo la aplicación del banco correspondiente.**
- Nunca abrir archivos adjuntos si recibimos un correo electrónico de un remitente desconocido.
- No facilitar a todo el mundo la dirección de correo que se utiliza habitualmente.
- Utilizar una cuenta de correo para recibir y enviar cadenas de mensajes, inscribirse en foros y realizar otros trámites en Internet.

Para evitar que se instalen troyanos en nuestro ordenador

- Es recomendable que instalar algún programa de software anti troyanos.
- Manter siempre el antivirus actualizado.
- Evitar en lo posible el uso de redes P2P (red de pares que permiten conectarse entre sí, para compartir archivos) como eMule, Bit Torrent o Ares.
- Tener precaución cuando naveguemos por Internet y descarguemos archivos como música y fotos.

En resumen

Estos serían los pasos más importantes para prevenir un robo, pero sobre todo algo que queremos que quede muy clarito: jamás de los jamases, debemos enviar un correo con nuestras claves, numero de cuentas, etc.

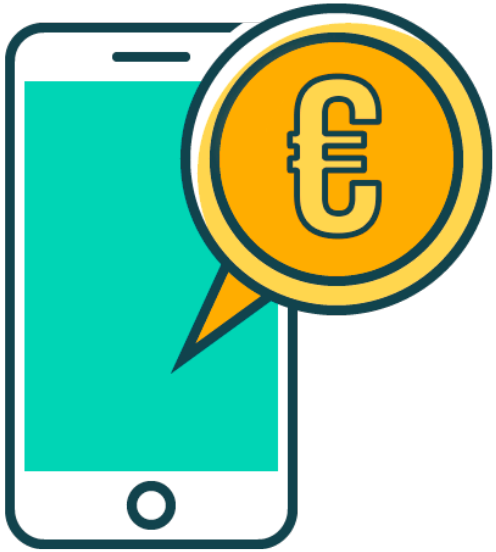
Recordad que éste tipo de datos son nuestros y solo nuestros y nunca una entidad oficial nos los va a pedir ni por correo electrónico, ni por teléfono. Siempre ante la duda es mejor no abrir correos electrónicos sospechosos y sobre todo no pinchar en los enlaces, sino llamamos y preguntamos a nuestro banco.

Tema 2.

Compra segura por internet

En este tema vamos a:

- Preparar nuestro dispositivo y contraseñas
- Comprobar si la web de la tienda es segura
- Conocer los diferentes tipos de pago

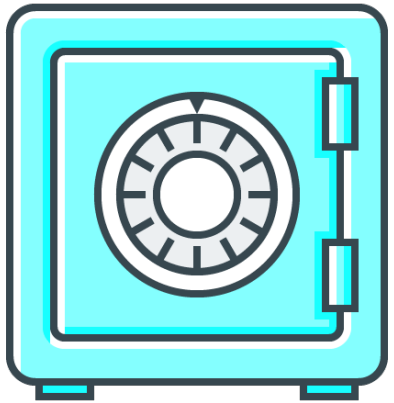


¿Cómo comprar de forma segura en internet?

Compra segura

El comercio electrónico es uno de los servicios que más ha crecido en los últimos años pero… ¿alguna vez has querido comprar algo por internet pero te ha dado un poquillo de miedo y no lo has hecho?

No te preocupes que después de este tema vas a deshacerte de esos miedos, ya que para realizar compras online lo primero y más necesario es que el dispositivo que uses esté debidamente configurado y protegido.



Antes de comenzar tus compras ¡Revisa tu dispositivo!

- ✓ Que tu dispositivo tenga instalado y actualizado, un antivirus que detecte posibles amenazas.
- ✓ Que el sistema operativo del dispositivo esté actualizado con la última versión para evitar un fallo de seguridad.
- ✓ Revisa los programas y aplicaciones que tienes instaladas y elimina aquellas que no utilices, así será más fácil que tu dispositivo se mantenga actualizado y protegido, y más difícil que puedas ser víctima de un fraude.
- ✓ Si el dispositivo lo utilizáis más de una persona, crea un usuario por cada una de las que vayan a utilizarlo.

Antes de comenzar tus compras ¡Revisa la conexión!

- ✓ Utiliza una conexión de Internet de confianza. No hagas compras utilizando una red pública. Hazlo siempre desde casa y revisa la configuración de tu red wifi para que esté bien configurada y no puedan acceder a ella otras personas.
- ✓ No emplees una red Wifi pública para este tipo de acciones. Para saber más de este tema puedes visitar la siguiente web a través del enlace: https://www.osi.es/es/wifi-publica.

Antes de comenzar tus compras ¡Revisa tu contraseña!

- ✓ No compartas tus contraseñas que utilices en tus tiendas on line. No las escribas en ningún sitio y crea siempre contraseñas robustas.
- ✓ Crea contraseñas que tengan:
  - mayúsculas (A, B, C…)
  - minúsculas (a, b, c…)
  - números (1, 2, 3…)
  - y caracteres especiales ($, &, #...)

Antes de comenzar tus compras ¡Revisa tu contraseña!

- ✓ No uses contraseñas que sean fáciles de adivinar: 123; abc; matricula de tu vehículo, fecha de nacimiento…
- ✓ Utiliza diferentes contraseñas, no utilices siempre la misma. Esto puede ser complicado cuando tienes muchas contraseñas, pero para evitar estos "olvidos" puedes utilizar un gestor de contraseñas. Un gestor de contraseñas es un programa que permite que las guardes de forma segura; y así solo tendrás que acordarte de una sola, que es la que te dará acceso a ver todas las demás.

Antes de comenzar tus compras ¡Revisa tu contraseña!

- ¿Cómo puedes recordar mejor tus contraseñas? Utiliza un patrón para crearlas:
  - Elige un símbolo (%,&,*…) que utilizarás siempre.
  - Piensa una frase que no se te olvide nunca, por ejemplo "La lluvia en Sevilla es una maravilla"
  - Escoge un número…
  - Y júntalo todo
  - %lleSeum2, ¡ya la tienes!

Antes de comenzar tus compras ¡Revisa tu contraseña!

- ¡Y cámbiala de vez en cuando! 😉
- Cuando termines de utilizar tu dispositivo cierra la sesión, sino cualquier persona que lo utilice con posterioridad podrá acceder a tus datos.

¿Tienda de confianza?

Como consumidor debes asegurarte en qué web o aplicación vas a realizar el pago de tus compras online. Realiza preferentemente las compras en páginas oficiales o con reputación y prestigio consolidado.

Lo primero **comprueba que la página web es segura.** Con esto evitarás no solo ser víctima de fraude o robo de tus datos o de dinero, sino también minimizar el riesgo de que la empresa en la que crees que esta comprando sea un fraude y también evitar comprar artículos falsificados.

¿Tienda de confianza?

Es importante conocer que las páginas web seguras siempre tienen el candado al principio y la letra "s" de seguridad en el dominio web "https".

¿Tienda de confianza?

Además, puedes comprobar también que tengan un apartado sobre los Términos de uso, Aviso legal o Política de privacidad, en la que te explican claramente cuales son todos estos elementos y como aplican si utilizas y navegas por su web.

Las tiendas online suelen tener un certificado válido, si una tienda online no dispone de certificado, o éste no es válido, te recomendamos no continuar con el proceso de compra y buscar otra web que cumpla con los requisitos mínimos de seguridad que te hemos comentado.

¿Tienda de confianza?

Utiliza tiendas que tenga sellos de confianza: los sellos de confianza son distintivos que se proporcionan a las tiendas online para demostrar su calidad y seguridad en la venta online. Para conseguirlo, éstas son auditadas o evaluadas para comprobar que cumplen criterios de seguridad en la compra y cumplimiento legal en materia de privacidad y protección de los consumidores.

Uno de los sellos de confianza más conocido en España es Confianza Online.

Es obligatorio que todos los comercios online faciliten en su web los siguientes datos:

- ✓ Nombre completo de la entidad (persona física, sociedad, fundación, etc.)
- ✓ Número de identificación fiscal (NIF, NIE o CIF)
- ✓ Datos de su inscripción en el registro mercantil
- ✓ Dirección postal
- ✓ Dirección electrónica
- ✓ Los términos legales de este servicio, en España se regulan en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Es obligatorio que todos los comercios online faciliten en su web los siguientes datos:

- ✓ Además, la directiva PSD2, que es una regulación europea sobre servicios de pagos electrónicos, pretende aumentar la seguridad en los pagos en Europa. Persigue disminuir el fraude en los nuevos medios de pago, adaptando los servicios bancarios a las nuevas tecnologías, por ejemplo, mediante la autenticación reforzada utilizando la huella dactilar, con códigos PIN, envíos de mensajes al smartphone.

Si quieres **ampliar tus conocimientos** puedes visitar el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Existen muchos motivos para desconfiar de una página web. Entre otros están:

- Que el diseño de la página web no sea homogéneo (por ejemplo, que tenga varios tipos de letra en la misma ventana).
- Que la foto de su portada puede encontrarse en otros lugares de internet.
- Si las imágenes son de baja calidad, están pixeladas o incluyen marcas de agua.
- Si aparecen textos mal traducidos. Por ejemplo, aparece traducida la sección “Home” como “Casa”, en vez de “Inicio”, que es lo correcto.

Métodos de pago aceptados

Una de las cosas que más suele preocupar a las personas a la hora de realizar compras online es el tipo de pago a utilizar, sobre todo por desconocimiento de las distintas alternativas disponibles y de las ventajas o inconvenientes de cada una de ellas.

Es importante que conozcas qué opciones hay disponibles para saber cuál es la que más te interesa y así, poder utilizar la más adecuada para cada tipo de compra y la que ofrece una mayor seguridad. Procura utilizar siempre el medio de pago que te resulte más sencillo y seguro para realizar tus operaciones. Si tienes duda sobre cómo hacer el pago no sigas adelante.

Descarta la compra si la web anuncia varias formas de pago, pero finalmente sólo acepta tarjeta de crédito.

Los medios de pago de uso común en el comercio online son:

- Contra reembolso
- Envíos de dinero en efectivo
- Pago con tarjeta
- Transferencia bancaria
- Pago a través de intermediarios

Contra reembolso

Es la modalidad de envío de paquetes, en la cual se paga en efectivo cuando se recibe el paquete. Para el comprador se trata de un método bastante fiable, ya que **se paga el producto cuando se recibe**.

Envíos de dinero en efectivo

Hay servicios que están diseñados para realizar transferencias de dinero, incluso de forma anónima. En estos casos es imposible identificar quién es el emisor y el receptor y, por tanto, no debes utilizarlos nunca para realizar compras online. **Si un operador de comercio online solicita el pago en dinero efectivo, renuncia a la compra, no sigas adelante.**

Pago con tarjeta

Es la modalidad más utilizada por las tiendas virtuales. Es un método sencillo de utilizar y la única información necesaria para realizar el pago son los datos de la propia tarjeta de crédito/débito.

Es muy importante saber que, **si han utilizado tu tarjeta y hecho una compra, y por tanto el importe ha sido cargado de forma fraudulenta o indebida, puedes exigir la inmediata anulación del cargo.**

Con este método de pago, a pesar de haber un intercambio de datos bancarios, que puede llevar un cierto riesgo, hoy en día, es un método bastante seguro. En las tiendas online oficiales, disponen de un sistema de seguridad o "pasarela de pago" con los bancos, que verifica los datos bancarios y protege la información de los usuarios.

Además, también **tienes la posibilidad de solicitar a tu banco una tarjeta de uso exclusivo para realizar pagos online** y activarla sólo cuando hagas uso de ella.

Transferencia bancaria

Este método de pago **permite enviar una cantidad de dinero desde una cuenta bancaria a otra sin que sea necesario introducir ningún dato en el sitio web.**

El vendedor tendrá que facilitarte los datos de su cuenta bancaria para que realices el ingreso del dinero correspondiente a tu compra. Ten en cuenta que, en el caso de que no te entreguen los productos adquiridos puedes reclamar contra el vendedor por incumplimiento del contrato.

Hoy en día muchas de las compras que hacemos las efectuamos a vendedores de otros países. Esto puede llevar algún riesgo de seguridad, ya que **en el caso de transferencias internacionales será más difícil recuperar el dinero una vez abonado** el importe en la cuenta del vendedor y, además, si el titular de la cuenta receptora del dinero no autoriza su devolución, tendrías que acudir a la vía judicial.

Pago a través de intermediarios

Esta forma de pago **utiliza a una tercera empresa de confianza (por ejemplo PayPal), para gestionar los datos bancarios del vendedor y del comprador**; y es esta empresa la que se encarga de formalizar los pagos. A través de este método, el vendedor y el comprador no conocen los datos el uno del otro.

Muchas tiendas online ofrecen este servicio, por la comodidad que supone no tener que introducir los datos bancarios cada vez que vas a realizar una compra, y porque algunas personas son reacias a facilitar sus datos bancarios.

Para poder usar esta forma de pago **necesitas darte de alta en este servicio,** disponer de una cuenta aquí y configurar en ella tu tarjeta de crédito. Recuerda siempre utilizar una buena contraseña para acceder a este servicio y no te olvides de consultar las condiciones de uso del servicio.

Posibles costes añadidos

Aunque la mayoría de los medios de pago son gratuitos, es importante que conozcas que **en ocasiones existen tarifas asociadas** a la prestación de servicios de pago por lo que **debemos estar atentos y evitar estos cobros.**

Estos posibles costes pueden provenir de transacciones, devoluciones, contrarrembolso, etc.

¡Importante! **La normativa restringe que los comercios cobren comisiones en función de los medios de pagos utilizados**, y también, prohíbe las dobles comisiones a los clientes.

Servicio de compraventa

En los últimos años han aparecido nuevos servicios de compras online que **facilitan la compra y venta de artículos y productos de segunda mano.**

Dichos servicios actúan como intermediarios entre el comprador y el vendedor. Permiten al vendedor la publicación de anuncios en los que describe las características del producto, el precio de venta, así como los mecanismos de contacto.

A pesar de que estos servicios ofrecen muchas ventajas, no están exentos de riesgos que debes conocer para evitar fraudes al comprar cualquier producto.

Servicios de compraventa: Algunos consejos para comprar

- Busca información del vendedor antes de realizar la compra: haz búsquedas por el nombre, ver los comentarios de otros compradores, las valoraciones de otros usuarios, etc.

- Descarta los anuncios que tengan fotos genéricas del artículo en venta, o cuya redacción no esté cuidada; aquellos en los que aparezcan traducciones automáticas o cuya descripción no coincida con el artículo en venta.

Servicios de compraventa: Algunos consejos para comprar

- Si el vendedor se encuentra en el extranjero y utiliza este hecho como excusa para que la gestión de los trámites se ejecute de una forma determinada, no continues con la compra.
- No aceptes nunca como método de pago para este tipo de compras servicios tipo Western Union o Money Gram.
- Y siempre cancela el proceso de compra en caso de dudas.

Servicios de compraventa: Algunos consejos para vender

- Infórmate sobre quién es el comprador antes de realizar el envío.
- Desconfía si te ofrecen más dinero del que pides en el anuncio.
- Utiliza un método de pago conocido que garantice que la compra está bajo tu control.

Servicios de compraventa: Algunos consejos para vender

- No adelantes dinero. Por ejemplo, en algunas estafas, el comprador utiliza como excusa que su banco no le permite hacer transferencias inferiores a una cantidad de dinero que, casualmente, es siempre mayor que el precio del artículo en venta. El objetivo es intentar engañar al vendedor para que abone por adelantado la diferencia de dinero para compensar los costes totales.
- Y como siempre, ante cualquier duda cancela el proceso de venta.

Compras a través de APPS

En el caso de compras online a través de aplicaciones, **tienes que configurar previamente la aplicación de compra con tus datos privados y bancarios.** Así que, debes tener la precaución de que nadie realice compras en tu nombre si, por algún motivo, tienen acceso físico al terminal móvil donde está configurada.

Para evitar cualquier riesgo, por ejemplo, puedes establecer un bloqueo de pantalla del dispositivo para restringir el acceso a las funcionalidades (incluyendo las apps) y **configurar un patrón, PIN o contraseña.**

En resumen

Como norma general y para cualquier tipo de compra que hagas en la red, toma siempre una serie de precauciones:

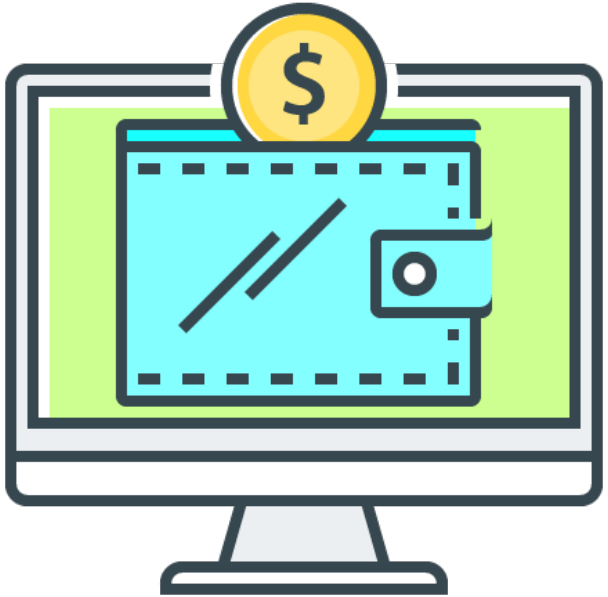
- ✓ Averigua cuales son las formas de pago que te permiten.
- ✓ Comprueba siempre el precio final a pagar. A veces el precio aparece sin tasas, impuestos, gastos de envío, etc.
- ✓ Consulta en la red las opiniones de otros compradores. Existen algunas páginas específicas que te pueden ayudar en la búsqueda de referencias sobre los vendedores.
- ✓ No te olvides de verificar cual es la política de devolución tanto del producto como del dinero y las condiciones de los envíos (plazos, costes asociados, envíos exprés…)

Tema 3.

Principales delitos cibernéticos relacionados con la banca digital

En este tema vamos a:

- Conocer los principales delitos para saber identificarlos y prevenirlos
- Qué hacer ante un fraude cibernético



¿Qué tipos de delitos existen?

Principales delitos cibernéticos relacionados con la banca digital

Los delitos cibernéticos hacen referencia a los delitos informáticos, que son todas aquellas **acciones ilegales, delictivas, antiéticas o no autorizadas que, haciendo uso de dispositivos electrónicos e internet, vulneran o dañan los bienes de terceras personas o entidades.**

El término **ciberseguridad hace referencia a todas las medidas para prevenir delitos cibernéticos,** en este caso, relacionados con el mundo digital. Hace referencia a la forma en la que te proteges a ti, a tu dinero y a tus datos confidenciales de los piratas y sus ataques cibernéticos.

Tipos de delitos cibernéticos

España, en septiembre de 2010 ratificó el **«Convenio de la Ciberdelincuencia"**, que es aceptado internacionalmente por los países que lo firman y que define una clasificación y tipología para los delitos informáticos, en cuatro bloques:

- Título 1: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- Título 2: delitos informáticos
- Título 3: delitos relacionados con el contenido
- Título 4: delitos relacionados con infracciones de la propiedad intelectual y derechos afines como los derechos de autor

Principales delitos cibernéticos relacionados con la banca digital

Si quieres conocer más sobre este tema puedes visitar el siguiente enlace: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

Ten siempre presenta que la digitalización de los servicios y productos bancarios es una realidad cada vez más común y, por tanto, también es mayor el número de ataques cibernéticos en este campo.

Vamos a conocer algunos de los delitos más habituales.

Tipos de delitos cibernéticos

Podemos agruparlos en diferentes categorías atendiendo a distintas circunstancias, así:

Punto de compromiso

Es el lugar físico o virtual en el que se produce la sustracción de los datos, ya sea número de tarjeta, chip, banda magnética, caducidad, etc. Para ello pueden clonar el chip de la tarjeta (método Shimming) o manipulando el hardware y software de los cajeros automáticos.

Punto de uso

Es el lugar físico o virtual donde se lleva a cabo el fraude derivado de las tarjetas comprometidas. Estos fraudes se materializan no solo con tarjetas clonadas sino también chip. En Internet encontramos venta de tarjetas fraudulentas creadas por cibercriminales con los datos de tarjeta legítima, y el software necesario para volver la información robada y posterior utilización.

Exposición de información relativa a tarjetas

Es decir, uso ilegítimo de tarjetas bancarias pertenecientes a otras personas con el fin de obtener bienes cometiendo fraude con ellas.

Vishing

Consiste en **llamadas telefónicas no deseadas y fraudulentas que se realizan a través de Internet.** Este fraude tiene unas características muy similares al phishing (que ya desarrollamos al comienzo), pero en vez de enviar e-mails se realizan llamadas telefónicas por Internet solicitando los números de las tarjetas de crédito, claves secretas, etc.

El delincuente informático configura lo que se llama un "war dialing". A través de esta técnica hace llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún otro ordenador para llamar a números telefónicos en una determinada región.

Algunos ejemplos de Vishing:

- **Tarjeta utilizada de forma fraudulenta:** contestas la llamada, suena una grabación y te alerta de que tu tarjeta de crédito está siendo utilizada de forma fraudulenta y debes llamar al número que sigue inmediatamente. El número puede ser incluso, un número gratuito. Cuando llamas a este número, te contesta una voz computarizada que te indica que tu cuenta necesita ser verificada y te requiere que ingreses los 16 dígitos de su tarjeta de crédito. La llamada puede ser también utilizada para obtener detalles adicionales como el PIN de seguridad, la fecha de expiración, el número de cuenta u otra información importante que después utilizarán para cometer el delito.

Algunos ejemplos de Vishing:

- **Supuesto empleado de una entidad bancaria:** te llaman y te avisan de que se está realizando una operación fraudulenta (y ficticia) con tu tarjeta y solicitan datos de la tarjeta. Mientras hablan contigo, realizan compras en línea reales y te piden las claves OTP recibidas por SMS haciéndote creer que son códigos para cancelar la operación falsa.

- **Un falso comercial de una compañía telefónica:** te llama para comunicarte que te han cobrado de más por error en la factura y te solicita tus datos bancarios para abonar la diferencia.

Con el fin de que puedas evitar estos delitos:

- No facilites a nadie los datos de tu cuenta o tarjeta por teléfono. No des información tuya ni respondas a solicitudes que no hayas iniciado.
- Cuando contestes al teléfono y suene una grabación, recuerda que puede ser un fraude.
- Las compañías legítimas ya disponen de tu información personal, no necesitan pedírtela de nuevo y mucho menos por teléfono.
- Ante cualquier llamada que te resulte sospechosa, cuelga el teléfono
- Si se han identificado como alguna compañía, y te surgen dudas, busca el número oficial y contacta tú para comprobar que sucede.

Vishing

Si quieres conocer más sobre este tema visita el siguiente enlace: https://clientebancario.bde.es/pcb/es/blog/consejos-de-la-policia-para-evitar-el-vishing.html

Smishing

Es otra variante del Phishing y de las más utilizadas para el **robo de información suplantando la identidad de otra persona** o entidad. La operativa de este fraude es muy similar a la del phishing convencional, pero en este caso, se lleva a cabo mediante mensajes de texto (SMS). Actualmente también se reciben a través de mensajería instantánea como WhatsApp.

Recibes mensajes de texto que te inducen a llamar a líneas de tarificación adicional, a acceder a un enlace de una web falsa bajo un pretexto o a realizar transferencias bancarias con distintos reclamos. El sistema emisor de estos mensajes de texto o intentará suplantar la identidad de alguna persona conocida entre nuestros contactos o incluso una empresa de confianza.

Ejemplos de Smishing:

- Las víctimas reciben mensajes SMS o mensaje instantáneos de WhatsApp, Line… con líneas similares a estás:

"Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 euros al día a menos que cancele su petición: www.?????.com."

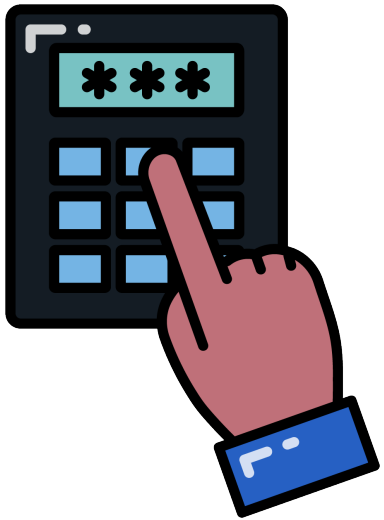
Cuando visitamos la dirección web, las víctimas son incitadas o incluso forzadas a descargar algún programa que en su mayoría suele ser un Troyano.

Para no caer en este fraude:

- Aunque en el mensaje te digan que pertenecen a una entidad de confianza, siempre comprueba el remitente de este. Si no aparece el nombre de la empresa y solo ves un número de teléfono, lo más probable es que se trate de un fraude.
- No te fíes de los mensajes que te informan de que recibirás un regalo en tu cuenta.
- No llames al teléfono que se le indica en el mensaje ni visite la web que contiene.
- También es importante leer detenidamente el mensaje para detectar errores ortográficos y gramaticales o fallos en la traducción.
- Si crees que puedes estar ante un mensaje de texto fraudulento, lo mejor que puedes hacer es ignorarlo y eliminarlo. Además, ten mucho cuidado de no hacer clic en ningún enlace o adjunto sospechoso para descargar.

Fraude en Paypal

En el caso de los **fraudes con suplantación de la entidad Paypal,** los correos se hacen pasar por un representante de Paypal, informando de que debes renovar tu contraseña, actualizar tu cuenta o alguna acción similar. Te dicen que de lo contrario te sería suspendida la cuenta. El correo incluye un link a una web falsa, el cual aparentemente te redirige a Paypal pero en realidad el link te redirige a otra web fraudulenta que robará tu información para cometer el delito.



Para no caer en este fraude:

- No visites el enlace que contiene el e-mail si sospecha que el mensaje es un fraude.
- Entra siempre en tu cuenta de Paypal a través de su página habitual y revisa que todo es correcto.
- Si tienes dudas póngase en contacto con la empresa y pregunte sobre el estado de tu cuenta.
- Conoce las direcciones oficiales del servicio (la dirección de correo electrónico principal de PayPal es paypal@mail.paypal.com y PayPal envía los recibos a través de service@paypal.com.)

Cartas nigerianas

Las conocidas como cartas nigerianas, también conocidas como fraude 419, son una **estafa que consiste en convencer a la víctima de un adelanto de dinero** mediante diferentes engaños.

El envío de estas comunicaciones o cartas puede hacer por correo electrónico y el remitente pone a disposición del destinatario ofertas "falsas" para participar en negocios supuestamente muy rentables, o con la intención de involucrar a la víctima en cualquier otra situación engañosa, procurando que transfiera una cantidad de dinero para llevar a cabo la operación.

Algunos ejemplos son:

- **Estafa de la lotería:** te informan de que el receptor ha ganado la lotería o un sorteo y te piden ayuda para evadir capitales ofreciendo una cuantiosa recompensa.
- **Estafa de las mascotas:** las mascotas de alto valor y escasas se anuncian como cebo en sitios web de publicidad en línea. Cuando la víctima decide adoptar o comprar la mascota, se debe utilizar un servicio de mensajería que en realidad es parte de la estafa. Si se trata de una mascota adoptada, normalmente se espera que la víctima pague alguna tarifa como seguro, comida o envío.
- **Estafa de ofertas de trabajo falsas:** anuncian trabajos con compañías reales y ofrecen salarios y condiciones muy buenas, fingiendo ser agentes de recursos humanos encargados de la contratación. Incluso te realizan una entrevista telefónica falsa, y después de un tiempo te informa que eres el candidato seleccionado, pero para asegurarte el puesto, te piden que envíes dinero para el pago de algún trámite necesario para poder contratarte.

Para no caer en este fraude:

A pesar de no ser técnicamente muy complejo, se trata de uno de los fraudes que más daño causa a sus víctimas. Además, es muy difícil recuperar el dinero estafado ya que usualmente se envía por giros postales a países con escasa seguridad jurídica donde ya se pierde la vista del dinero sustraído. Inicialmente los estafadores se hacían pasar por ciudadanos nigerianos lo que dio origen al término en cuestión.

- Desconfía de ofertas de trabajo que se alejan de la realidad y que provienen de empresas o negocios dudosos, otros países, remitentes desconocidos… o investigue sobre la empresa.

SCAM

Se trata de una estafa que combina el phishing con las cartas nigerianas. En primer lugar, **los estafadores ofrecen trabajos con alta remuneración por foros** u otros lugares visitados por los internautas, solicitándoles el nombre y cuenta corriente para contratarlos.

Posteriormente se obtienen las claves de otros usuarios mediante el fraude llamado phishing y se realizan transferencias a otra persona llamada "mulero". Esta persona cree estar contratada para la para gestión de cobros y lo que hace es enviar las cantidades recibidas por medio de giros a otros países, quedándose una pequeña cantidad en concepto de comisión.

Consejos y advertencias para no ser víctima de este fraude:

- Utilizar el sentido común. El "dinero fácil" siempre es una trampa.
- Consulta la web http://scamomatic.com para asegurarte si se trata de un correo scam o no.

Virus de la policia nacional

Esta es una de las maneras más peligrosas de estafa en internet porque **suplanta la identidad de la Policía Nacional**. Es fácil caer en él porque hace creer a quien lo recibe que es un mensaje real, y esto por la supuesta procedencia. Como funciona es haciéndote creer que has cometido alguna actividad ilegal, y que es la policía quien se comunica contigo.

Mediante un virus informático (llamado Ukash) tu ordenador infectado emite un mensaje que simula ser de la policía y en el que te comunican que has cometido un delito por el acceso a páginas de Internet que contienen pornografía, pornografía infantil, zoofilia o elementos de violencia sobre los menores. Además, te informan también que tu PC ha sido bloqueado para evitar que sigas cometiendo "acciones ilegales".

Virus de la policia nacional

Después, el mismo mensaje del virus te dará «una solución», que es pagar una supuesta multa y te detallan las instrucciones a seguir para el pago de esta supuesta multa, que generalmente asciende a 100 euros. Las supuestas multas se pagan a través de un sistema prepago llamado Ukash que para muchos puede ser poco conocido.

Si alguna vez te encuentras esta situación **de inmediato denúncialo.** Debes tener siempre en cuenta que la policía nunca actúa de esta manera y que ninguna institución oficial solicita pagos a través de sistemas de este tipo.

Domiciliaciones fraudulentas

Consiste en el **cargo a tu cuenta de pagos periódicos por gastos que no son realizados** o servicios que tu no has contratado. Estas domiciliaciones realizadas en tu cuenta bancaria han podido ser realizadas obteniendo tus datos mediante algunos de los fraudes anteriormente comentados.

Si no revisas periódicamente tus cuentas puedes ser víctimas de este tipo de fraude durante mucho tiempo, ya que las domiciliaciones se producen de forma periódica.

Si detectas que te pasan gastos que no has realizado, debes dar parte a tu banco para cancelar el cobro y denegar futuros pagos, diciendo expresamente al empleado de la sucursal que no los carguen de aquí en adelante.

Para no caer en estos fraudes, conviene que:

- Revises periódicamente tus cuentas bancarias.
- Recuerda que dispones de 13 meses para devolver cualquier recibo cargado no autorizado, y de 8 semanas si este sí se autorizó, pero aun así quieres retroceder el pago.
- Solicita a tu banco que se no se realicen futuros pagos de recibos que provengan de estas compañías sospechosas.

Fraude de tarjetas caducadas y brushing

Uno de los últimos fraudes detectados son las **tarjetas de crédito caducadas para realizar compras por Internet.** Es importante conocer que las tarjetas de crédito que se usan en grandes tiendas virtuales (Market Place), aunque estén caducadas es posible siguen siendo medios de pago válidos y se puede realizar compras con ellas. Y esto es porque existen determinados acuerdos entre algunos bancos y las grandes tiendas online mundiales, que permiten que puedas realizar compras con una tarjeta caducada si así se ha acordado previamente entre ambas partes.

Una vez que han realizado la compra, eligen el envío del paquete a la dirección del titular de la tarjeta, pero antes de que sea entregado en su destino interceptan el paquete.

Fraude de tarjetas caducadas y brushing

➡ Para no caer en estos fraudes, conviene que revises periódicamente tu cuenta bancaria y los movimientos de tus tarjetas.

En el caso del llamado **"Brushing", el vendedor ubicado en el Market Place externo de una tienda online, compra sus propios productos por medio de cuentas de falsas.** Los pedidos son enviados a una dirección real. La finalidad es que este vendedor reciba una puntuación positiva sobre los productos que vende para impulsar su clasificación en la plataforma online y así poder engañar a otros usuarios con otras técnicas utilizando su buena reputación.

Cómo reclamar los abusos en medios de pago

En primer lugar, las empresas tienen obligación de informar al consumidor sobre las vías que tienen para reclamar sus derechos. Las vías que existen son tres:

- ✓Servicio de atención al cliente.
- ✓Sistema arbitral de consumo.
- ✓Organismos de supervisión.

Si como consumidor tienes algún tipo de problema (robo de datos, estafa, mal funcionamiento de la aplicación, incorrecta prestación de servicios, …) tienes derecho a acudir al servicio de atención al cliente del proveedor del servicio de pago.

Para poder realizar una reclamación debes incluir:

- Tu nombre, apellidos, dirección postal y DNI en el encabezamiento.
- Seguidamente, exponer los motivos por los que se presenta la reclamación, aportando todo tipo de datos y documentos que se precisen (contrato, copia de cuentas, recibos…).
- Por último, solicitar que se resuelva el problema ocasionado.

Cómo reclamar los abusos en medios de pago

Los proveedores de servicios de pago, no sólo bancos sino cualquier operador en este ámbito, deben establecer procedimientos para resolver las reclamaciones de sus clientes.

Tu servicio de atención al cliente debe de resolver las quejas en un plazo máximo de 15 días hábiles y la respuesta deberá remitirse al cliente en papel o en otro soporte duradero si así lo acuerdan la empresa y el cliente. Si bien es cierto que, ante situaciones excepcionales ese plazo se alarga hasta 35 días hábiles, debiendo en tal caso aclarar la razón del retraso en la resolución de la queja y cuándo remitirá la respuesta final.

Cómo reclamar los abusos en medios de pago

Si tienes una respuesta insatisfactoria puedes dirigirte al organismo supervisor que, en este caso, es el **Banco de España según la normativa de medios de pago**. Cabe destacar que tiene un periodo de 3 meses para contestar y su resolución no es vinculante para el proveedor del servicio de pago.

Como consumidor puedes presentar estas reclamaciones de forma presencial, vía email o carta certificada con acuse de recibo. Si prefieres presentarla en la oficina del proveedor de pago, tienes que entregar una copia y quedarte con otra sellada que justifique la entrega de dicha reclamación. Por otro lado, si elijes enviarla por email o correo certificado con acuse de recibo, te va a quedar constancia de que esa reclamación fue enviada, a efectos de que no recibas contestación, o te tengas que dirigir al órgano supervisor.

Si has sufrido un fraude en tu tarjeta bancaria:

Lo primero y más urgente es que lo notifiques a tu entidad financiera o emisora para que la tarjeta sea inmediatamente cancelada. Puedes acudir a la sucursal de tu banco más cercana o llamar por teléfono.

En caso de no conocer el teléfono de tu sucursal habitual puedes llamar al número de la red de cajeros a la que la entidad emisora de tu tarjeta está asociada:

Teléfono 4B: 91 362 62 00 y 902 114 400

Teléfono Euro 6000: 902 206 000

Teléfono Servired: 902 19 21 00

Si has sufrido un fraude en tu tarjeta bancaria:

Después, denúncialo ante la policía, ya que es el primer paso para posteriormente poder reclamar a la entidad financiera. La denuncia deberá incluirse como documentación adicional (juntamente con el contrato de la tarjeta, etc.) al escrito de reclamación a la entidad.

Ten en cuenta...

- La rapidez a la hora de denunciar un fraude y de dar de baja tu tarjeta es fundamental, cuanto más tiempo pase, más dinero pueden utilizar los estafadores sin tu consentimiento.
- Si la entidad te pone problemas, puedes realizar una reclamación ante el Defensor del Cliente y si este no te diera la razón, ante el Banco de España aportando siempre una copia de tu denuncia ante la Policía.
- En caso de que hubiera alguna otra parte implicada (alguien con quien no tengas relación pero que te reclame una deuda como, por ejemplo, un comercio donde supuestamente hayas realizado alguna compra) ponte en contacto con ellos para informarles de la situación.
- Si avisas a la entidad y ya se ha producido la extracción de dinero por el estafador, tu respondes por 50 euros, el resto lo asume el Banco.
- Si avisas del robo de la tarjeta a tu entidad, es el banco el que tiene que responder.

Si has sido víctima de un fraude informático:

La Legislación obliga en estos casos a que la denuncia sea de forma presencial, con personación del denunciante o su representante legal. No es posible, pues, hacer la denuncia de forma telemática.

Debes acudir al Juzgado, al Cuartel de la Guardia Civil o a la Comisaría de Policía más cercana para presentar una denuncia. Allí tendrás que acreditar tu identidad con el DNI, NIE o Pasaporte y cumplimentar las diligencias de trámite.

El grupo de delitos telemáticos de la Guardia Civil ofrece un modelo de denuncia que puedes descargar en su página web, con objeto de agilizar los trámites y una vez relleno y cumplimentado, acudas con él al Juzgado, Comisaría de la Policía o Cuartel de la Guardia Civil más próximo.

Autoridades en materia de ciberseguridad, consumo y protección de datos:

Autoridades y entidades Europeas de Ciberseguridad

EUROPOL

Autoridades Europeas de Consumo

Organismos europeos para la Resolución alternativa de litigios (RAL)

Autoridades y Entidades nacionales de Ciberseguridad

Policía Nacional - Brigada de Investigación Tecnológica (BIT)

Guardia Civil - Grupo de Delitos Telemáticos (GDT)

Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)

Instituto Nacional de Ciberseguridad (INCIBE) y el CERT de Seguridad e Industria (CERTSI)

Centro Criptológico Nacional (CCN-CERT)

En resumen

Es importante estar alerta y poner en práctica todo lo aprendido, no obstante recuerda que siempre puedes pedir ayuda, a tu entorno más cercano, al propio banco o empresa para confirmar si te han enviado ese correo o ese mensaje o incluso acudir a la policía.

Con éstos consejillos generales hemos llegado al final, esperamos que te haya quedado claro clarinete y te hayan servido de ayuda para pisar sobre seguro en la "nueva era de las finanzas digitales".

Como dijo el escritor francés Albert Camus *"Nos hacemos siempre una idea exagerada de lo que no conocemos"*... ¿Te ha pasado alguna vez? ;)