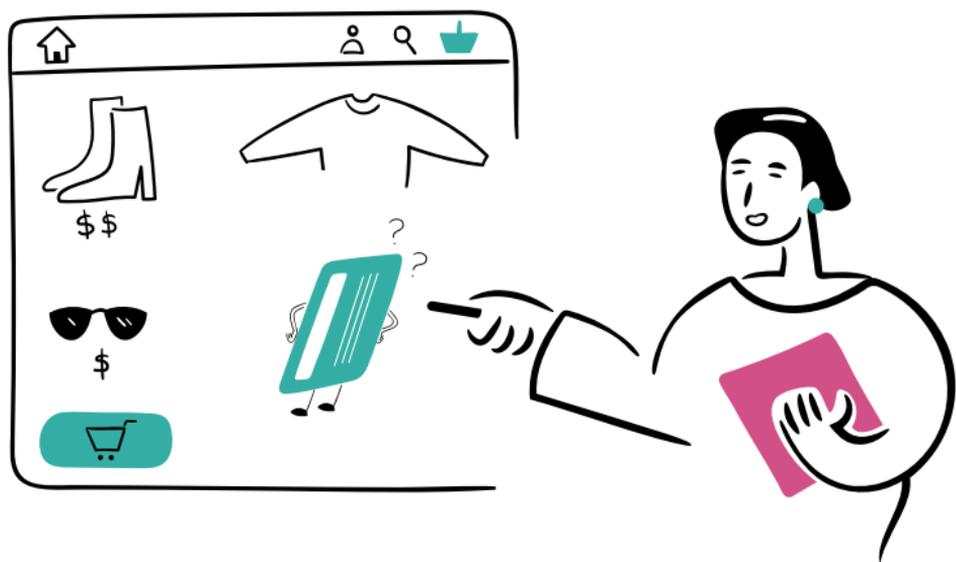


# 3. COMERCIO Y PAGO ELECTRÓNICO



**S!LBO**  
*Tu Ayuda Digital*

## INICIO

El comercio electrónico, (conocido popularmente como e-commerce) es la compraventa y distribución de bienes y servicios a través de internet u otras redes informáticas.



Imagínate ya no usar billetes y monedas sino simplemente tarjeta, móvil, etc... donde esté representado el valor del dinero y poder efectuar compras y aceptación en los establecimientos que uses.

El Dinero Electrónico o Digital viene a ser un sistema para adquirir créditos de dinero en cantidades relativamente reducidas. Este dinero electrónico se almacena en la computadora y se transmiten a través de redes electrónicas para ser gastado al hacer compras electrónicas.

**Sobre tu privacidad.** Las ventajas y desventajas del dinero electrónico son parte de un debate que se está produciendo en la actualidad debido a la aparición de múltiples medios tecnológicos para efectuar o recibir pagos.

Cada compra, cada intercambio económico o viaje, quedaría registrado en el sistema.

Aunque no se trate de ningún hecho delictivo, a muchas personas no les convence ese control absoluto sobre su vida.



## TIENDAS ON-LINE

Una tienda en línea (tienda virtual o tienda electrónica) se refiere a un tipo de comercio que usa como medio principal para realizar sus transacciones un sitio web o una aplicación (**APP**)! conectada a Internet. Constituye la herramienta principal del comercio electrónico.

La inmensa mayoría de tiendas on-line requieren la creación de un usuario en el sitio web a partir de datos como nombre, dirección y correo electrónico. Este último, a veces es utilizado como medio de validación.

## SEGURIDAD EN LAS PÁGINAS WEB

Cuando entras a una web puedes encontrarte que tienes que aceptar la Cookies;! pulsar en sitios donde no esperabas, como publicidad engañosa o confirmar que eres un humano.

Para evitar el **SPAM**! muchas páginas web nos ponen un código **CAPTCHA**! hay que tener paciencia, requiere muchos clicks. En realidad lo que estamos haciendo es enseñar a un ordenador en la nube (**IA**).!

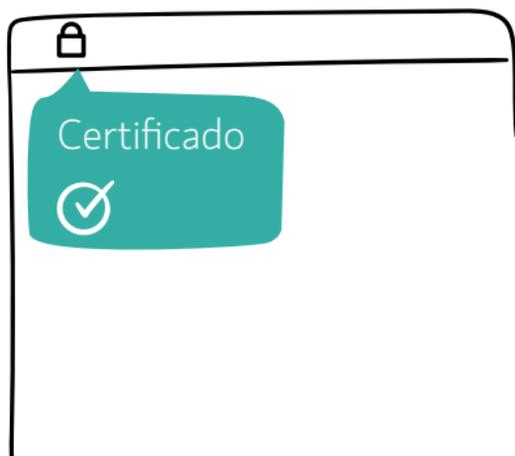
## PAGO SEGURO

Debido a las amenazas a la privacidad de los datos en Internet y la amenaza de robo de identidad, es muy importante hacer compras en línea solamente en sitios reconocidos y de buena reputación. Igualmente es recomendable no proporcionar datos personales ni de tarjeta de crédito si no se está utilizando una conexión segura.

Sólo tienes que tomar algunas precauciones y optar por la forma de pago más adecuada en cada caso. Para que tus datos no sean copiados por terceras personas lo mejor es utilizar conexión

### **https**

Comprueba que la web dispone de certificado de seguridad. Si lo tiene, el navegador mostrará un icono con forma de candado y la URL empezará por **https** en lugar de http.



## ¿HAS COMPRADO ALGUNA VEZ POR INTERNET?

Identificar donde puedes comprar o no y hacer una buena búsqueda del producto que quieres adquirir, muchas veces puede ser engorroso y lleva su tiempo. Evita páginas con excesiva publicidad.

Verifica a quién le compras en Internet, comprueba que la página donde realizas la transacción económica tenga herramientas de seguridad para realizar tu pago y no te dejes engañar con precios falsos, ni publicidad engañosa.

Muchos de los comercios que ya conoces ofrecen servicios de venta on-line. No es lo mismo un comercio que una plataforma de venta. **Amazon**, **Apple**, **Google** o **Facebook** son plataformas donde otros vendedores pueden poner a la venta sus productos.

## FORMAS DE PAGO

- ✓ *Paypal / Stripe / Otras*
- ✓ Tarjetas de crédito / débito / virtuales de tu propio banco
- ✓ Pago por **NFC**
- ✓ Pagos a través de Apps de terceros.
- ✓ *Bizum / Twyp / Verse / Yaap*
- ✓ Tarjetas virtuales prepago de terceros
- ✓ Transferencia bancaria o contra reembolso
- ✓ Monedas virtuales

### ¿QUÉ ES PAYPAL?

Es una empresa que nos da un servicio que te permite pagar, enviar dinero y aceptar pagos sin tener que introducir tus datos financieros continuamente. Está muy extendida.

# APPS BANCARIAS

Es una aplicación o serie de aplicaciones que tiene el servicio proporcionado por tu banco, te permite realizar transacciones como envío de dinero, pagos, entre otras cosas, de manera 100% digital.

## CONECTAR A TU BANCO

A menudo tu banco te va a pedir que verifiques que eres tú, mediante diferentes métodos. Siempre a través de tu móvil o e-mail.



### Verificación de doble factor.

Los bancos usan métodos para verificar los pagos online, mediante una doble verificación, ya sea por SMS (mediante un código) o en la propia aplicación bancaria.

### Autenticación Reforzada.

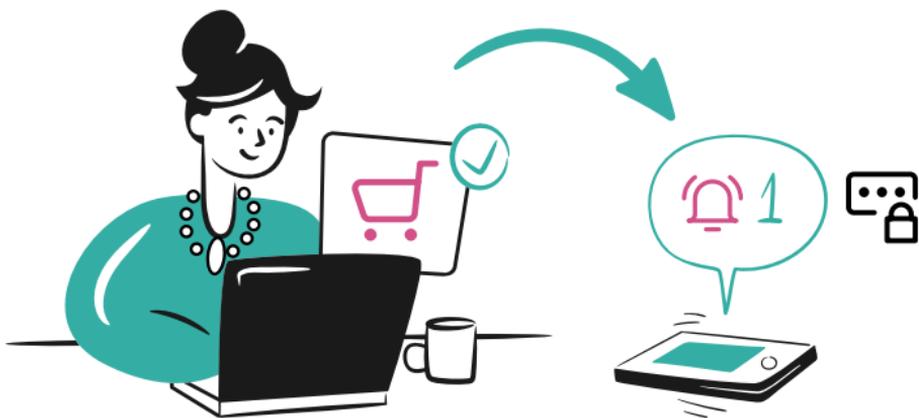
Para poder efectuar pagos en línea (PSD2)! Ahora incluso tendrás que verificar la identidad con otra aplicación (APP) del banco solo hecha para firmar.

## ¿CONECTAR CON UNA APP O WEB?

Algunos bancos no tienen sincronizado los servicios que te ofrecen entre la web bancaria y la APP. Por lo que es diferente conectarte desde el móvil o desde un dispositivo de escritorio como una tablet o un ordenador.

### **Seguridad extra.**

Evita llevar a cabo operaciones en ordenadores públicos y a través de **wifis** públicas. Recuerda que los bancos nunca solicitan información personal a través del correo ni teléfono.



# OTRAS TRANSACCIONES

## ENVIAR Y RECIBIR DINERO

Desde tu móvil puedes enviar y recibir dinero, mediante transferencias bancarias (a través de la **APP** bancaria) o mediante **APPs** de servicios como **BIZUM** o **TWYP**.

Para tener estos servicios debes hablar con tu entidad bancaria antes.

## TARJETAS BANCARIAS EN EL MÓVIL

NFC es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles. Tipo al **bluetooth**, pero mucho más corta, con esta tecnología puedes tener tu tarjeta de crédito en el móvil o en el reloj.

## Tarjetas almacenadas en grandes plataformas

Google, Amazon, Apple disponen de los sistemas necesarios para poder almacenar tarjetas bancarias. Esto los convierte en potenciales medios de pago.



## Pagos desde los mercados de Aplicaciones

**(Apps).** Cuando te registras en los mercados de apps. Se puede pagar servicios al instalarse una app, que puede contener una suscripción o un extra que se te cobrará en la tarjeta de crédito que hayas proporcionado al hacer la cuenta de en Android o iOS.

## Compras de suscripción a servicios.

Muchas empresas o plataformas ofrecen pagos por suscripción mensual, trimestral o anual. Pueden ser automáticos o manuales, por ejemplo un periódico, una plataforma de música como **Spotify** o de series como **Netflix**. Casi nunca dejan usar un número de cuenta y requiere una tarjeta de crédito, de débito o virtual.

# FRAUDES

Objetos, trabajos, préstamos o servicios... cualquier búsqueda en Internet te da resultados diversos. Si quieres establecer una relación comercial con esa página, recuerda siempre que detrás hay una empresa o institución.

- ✓ Evita el uso de redes wifi públicas para realizar transacciones online.
- ✓ Comprueba la información legal del comercio en los apartados “aviso legal”, “términos de uso” o “política de privacidad”.
- ✓ No te recomiendo utilizar servicios de un comercio que no identifica correctamente los siguientes datos: Nombre de la entidad, CIF y dirección postal.
- ✓ Revisa los sellos de confianza. Hay tiendas con sello de calidad obtenidos previa evaluación y auditoría. En España, el sello de confianza más conocido es “Confianza Online”.



## Phishing

Se suplanta la identidad de páginas de tus servicios a través de las que se solicitan contraseñas, datos personales o bancarios.

Para evitarlo:

- ✓ Debes desconfiar de mensajes alarmistas al descargar ficheros o entrar en enlaces.
- ✓ No debes responder a mensajes que solicitan datos personales o bancarios sin esperarlos.

## Carding

Esto es la utilización fraudulenta de la numeración de las tarjetas de créditos para efectuar compras por internet.

Para ello, se debe:

- ✓ Revisar periódicamente los movimientos de las cuentas asociadas a tarjetas.
- ✓ Anular las tarjetas en caso de pérdida o sustracción.
- ✓ Denunciar y reclamar si se advierte haber sido víctima de esta práctica.

## El hackeo inexistente

Al igual que las falsas alertas de seguridad, se realiza principalmente (aunque hay excepciones) a través de email, y trata de generar miedo en los usuarios para conseguir su objetivo.

Por lo general, los usuarios reciben un email en el que un hacker afirma haber infectado el ordenador con un virus. Y supuestamente, gracias a ese virus han obtenido acceso a la webcam del ordenador, al historial de navegación, o a diversos tipos de información comprometedor.

Ignora completamente el email y asegurate de que ese e-mail no vuelva a llegarte enviándolo al correo no deseado o SPAM.



Los *Hackers*:

Son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección.

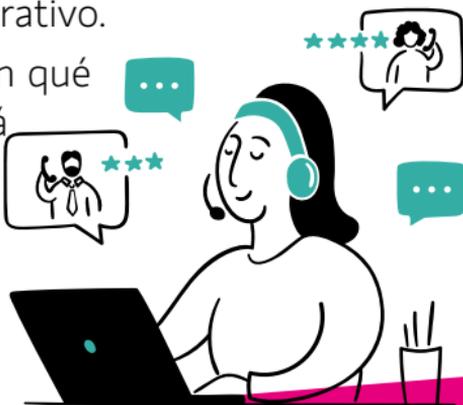
## Actualización de APPs.

Mantén actualizadas las aplicaciones de tu banco, suelen actualizarse cada poco tiempo por seguridad.



## Recuerda... antes de instalar Apps.

- ✓ Verificar que la app es compatible con el sistema operativo.
- ✓ Revisa con atención qué información te está solicitando la app.
- ✓ Lee reseñas y comentarios de [nuestr@s](#) [voluntari@s](#).



- ! Existe un diccionario en papel y en línea que explica las palabras o frases marcadas.

# MANUALES S!LBO



1. Identidad digital y seguridad
2. Administración electrónica
3. Comercio y dinero electrónico
4. Información digital
5. Socialización digital



Fundación  
**PEM**

En colaboración con:



—La Universidad Permanente—

ENTIDAD DECLARADA  
DE UTILIDAD PÚBLICA

Con el apoyo:



tuayudadigital.net