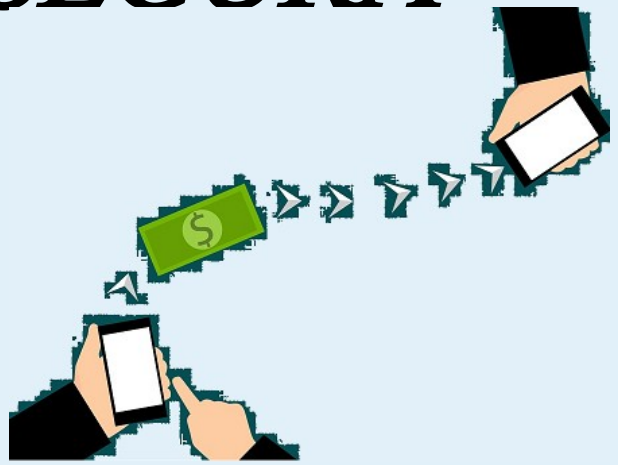
GUÍA DE CONSEJOS PARA

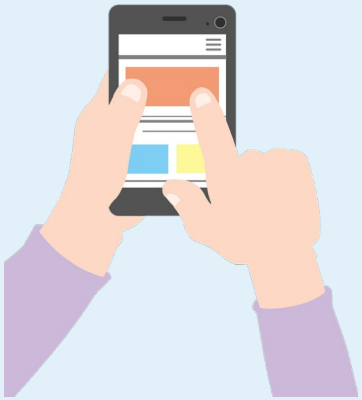
USAR DE FORMA SEGURA



LA BANCA ONLINE

Durante los últimos años se ha venido popularizando el uso de la banca online, bien a través de las propias páginas webs de las entidades financieras, bien a través de las apps creadas para su utilización a través de nuestro dispositivo móvil.

Desde la OMIC del Ayuntamiento de Talavera de la Reina editamos esta guía de consejos prácticos para aumentar la seguridad de nuestros datos bancarios y mantenerlos a buen recaudo, dificultando el acceso no permitido a los mismos.



A pesar de los esfuerzos de las entidades por reforzar la seguridad de sus servicios y aplicaciones, la posibilidad de ser objeto de un fraude o un ataque hacker está muy presente en el día a día. La utilización de estos servicios no está exenta de un cierto nivel de riesgo de que nuestra identidad y datos bancarios queden expuestos.

1 Utiliza nombres de usuarios y claves únicas.

Solemos utilizar los mismos usuarios y claves de acceso para todos los servicios online de los que somos usuarios. Anteponemos nuestra comodidad a la seguridad que nos proporciona individualizar esas claves para cada uno de los servicios a los que accedemos de forma habitual. Además, mantenemos estas claves durante grandes periodos de tiempo, lo que debilita las medidas de seguridad que las entidades financieras implementan en sus servicios y aplicaciones, facilitando a los hackers la obtención de la llave de entrada a nuestros datos financieros.

También es aconsejable la utilización de contraseñas fuertes y seguras, evitando utilizar en su confección datos personales o fácilmente deducibles.

Si lo crees necesario, utiliza administradores de contraseñas para facilitar su recuerdo y cuidado.

2 Accede a tu cuenta desde una red segura.

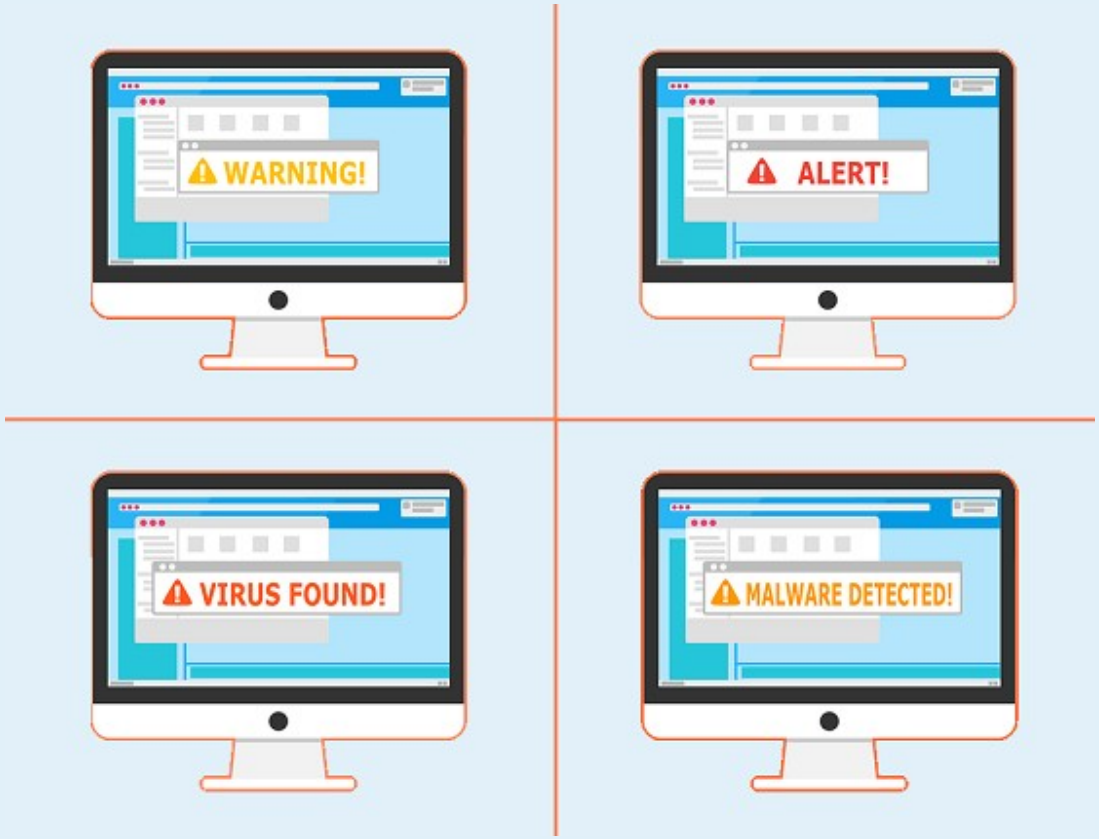
Evita acceder a tu banca online utilizando un Wi-Fi público, ya que en algunas ocasiones no proporciona una conexión segura a Internet, dejando nuestros datos de acceso al descubierto y fácilmente visibles para terceros.

El uso de páginas webs encriptadas puede salvarnos de esas miradas ajenas e indiscretas. Procura utilizar páginas seguras, verificando la URL de la página de acceso para que comience por **https//** y no **http.** La **s** indica que la página es segura de usar.

Pero aún si una página tiene cifrado, es mejor evitar por completo la conexión Wi-Fi pública. Usar una red privada virtual (Virtual Private Network), o usar tu red móvil para acceder a Internet es mucho más seguro cuando se trata de banca en línea. Si realmente quieres acceder de forma segura, hazlo desde el Wi-Fi de tu propia casa.

3 Utiliza un antivirus.

Usar un buen antivirus nos ayuda a mantener protegidos nuestros datos de las miradas ajenas, pero no sólo debemos hacer uso del antivirus en nuestro PC o portátil, también debemos instalarlo en nuestro dispositivo móvil, tablet, etc.



Mantener protegidos todos los dispositivos con los que accedemos a internet es importante para no dejar al descubierto nuestros datos personales y de acceso a los diferentes servicios bancarios de los que seamos usuarios.

Los rápidos avances que se esperimentan en materia de virus y troyanos bancarios, malware etc, aconseja que tengamos permanentemente actualizado nuestro software antivirus y programas antimalware para poder detectar más fácilmente estas amenazas.

También, procura mantener actualizados todos los sistemas operativos de tus dispositivos, ya que lanzan parches y correcciones que ayudan a proteger las vulnerabilidades descubiertas que estos programas maliciosos suelen aprovechar.

4 Accede a páginas webs de confianza.

Asegurate de acceder a la web oficial de tu entidad financiera y que la misma cuenta con un protocolo de cifrado adecuado (**https//**).

Las páginas webs de los bancos incluyen, obligatoriamente, las políticas de privacidad y avisos legales en cumplimiento de la normativa de protección de datos. Debes comprobar que cumplan todos esos requisitos y te indiquen qué tipo de datos recogen, cómo los recopilan y para qué los van a utilizar. También deben darte la opción de ejercer tus derechos de acceso, rectificación, cancelación, oposición y portabilidad respecto a tus datos personales.

5 Desactiva el bluetooth de tu dispositivo.

El Bluetooth es una tecnología inalámbrica diseñada para conectar distintos dispositivos entre sí. Con el Bluetooth activado podemos conectarnos al manos libres del coche, a otros dispositivos (móvil, portátil, Smart TV, tablet), altavoces y auriculares, etc.

La funcionalidad de esta tecnología es la propia comunicación entre los diferentes dispositivos y el trasvase de datos. El tener activado el Bluetooth facilita la conectividad y, por lo tanto, la posibilidad de sufrir ataques de piratería o phising.

Esta facilidad aconseja que, en el momento de operar con nuestra entidad financiera de forma on line, desactivemos la funcionalidad del bluetooth del dispositivo para evitar que nuestra conexión se pueda monitorizar y acceder a nuestro datos sin autorización.

Este proceso de acceso a nuestra conexión a través de la funcionalidad bluetooth se conoce como ***bluesnarfing***, y la única manera de protegernos frente a sus ataques es la desactivación del Bluetooth.

6 Monitoriza los movimientos de tu cuenta.

Accede con frecuencia a tus cuentas para verificar que los movimientos se adecúan a la actividad realizada.

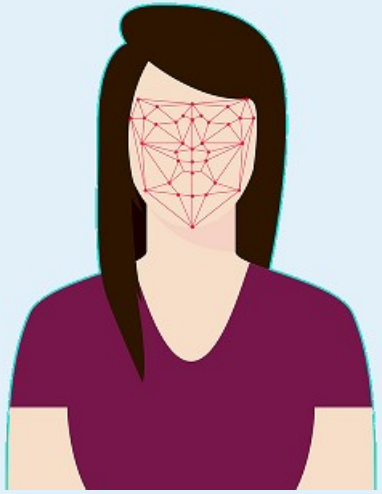
Un control periódico de los movimientos de nuestras cuentas nos permitirá detectar la existencia de actividades no autorizadas o fraudulentas. La rápidez a la hora de actuar en el caso de observar operaciones no autorizadas aumentará las posibilidades de recuperar nuestro dinero.

Los bancos ofrecen la posibilidad de recibir alertas (por sms o correo electrónico) cuando se produce algún tipo de actividad en tu cuenta. Es aconsejable suscribirse a estos servicios de alerta, incluso si somos nosotros mismos los que estamos haciendo la actividad.

Estos servicios de alerta son aprovechados por los piratas y estafadores, remitiendo una falsa alerta de actividad legítima al usuario bancario y ofreciendo un enlace externo para verificar el movimiento en cuestión, enlace que aprovechan para acceder a tus datos de acceso. Nunca utilices enlaces, accede directamente, desde otra ventana del navegador, a tu cuenta, para comprobar la veracidad de la actividad.

7 Pin o identificación de huella dactilar.

Los bancos, preocupados por los ataques fraudulentos y accesos ilegítimos a las cuentas de sus clientes, vienen implementando mayores medidas de seguridad para acceder al servicio online. Entre esas medidas se encuentra el acceso a la cuenta mediante un PIN o identificación de huella dáctilar. El uso de estos servicios de seguridad nos protegerá en los casos de pérdida o robo de nuestro dispositivo y nos proporcionará una barrera más de seguridad, complicando el acceso a nuestros datios bancarios a los piratas informáticos.



En ocasiones nos ofrecen los inicio de sesión biométricos, mediante huella dactilar y/o reconocimiento facial. La utilización de estos servicios aumentan las garantías de seguridad de nuestra cuenta, impidiendo el acceso ilegítimo a nuestros datos y protegiendonos de ataques y robos de identidad.

Esta guía informativa ha sido elaborada por la OMIC de Talavera de la Reina. (C/ San Francisco, 12 / Tfno. 925 810 000 / omic@talavera.org). La información que se facilita sólo proporciona una orientación de carácter general y no sustituye en ningún caso a la legislación aplicable.

Fuentes:

.- Ministerio de Consumo (www.consumo.gob.es)
.- Banco de España (www.clientebancario.bde.es)
.- Instituto Nacional de Ciberseguridad (www.incibe.es)