# Ciberseguridad y finanzas digitales: Aspectos clave

15 de octubre de 2024

**Autor: Manuel Jurado**
Manuel Jurado es graduado en Ingeniería de Telecomunicaciones, posee un máster en Ciberseguridad y certificaciones en seguridad de la información. Actualmente trabaja como especialista de Ciberseguridad en Unicaja.

---

En un contexto de creciente digitalización y ante un mayor uso de la banca digital y la realización de operaciones financieras por Internet, resulta fundamental para el ciudadano conocer aquellos aspectos de ciberseguridad que le permitan realizar su actividad digital de la manera más segura posible. La educación

financiera debe, por tanto, contemplar también la concienciación en seguridad para prevenir el ciberfraude y las estafas informáticas en la medida de lo posible.

En el presente artículo se desarrollan algunos de estos conceptos clave para asegurar nuestra actividad *online* y financiera.

**¿Cuáles son las amenazas informáticas a las que nos podemos enfrentar?**

Dado que la práctica totalidad de la población española entre 16 y 74 años utiliza habitualmente Internet, se ha de tener especial precaución a la hora de realizar nuestra actividad *online*. Esto incluye la realización de compras por Internet, pero también la actividad en redes sociales, los sitios web que visitamos, las aplicaciones o programas que instalamos, etc.

En todas estas situaciones pueden darse numerosas amenazas, entre las que destacan:

- *Malware*: se trata de virus o programas maliciosos que pueden entrar a nuestros dispositivos por visitar sitios web poco fiables o por descargar e instalar aplicaciones no confiables. De esta forma, se pueden "aprovechar" vulnerabilidades en los dispositivos que utilizamos para obtener información sensible de éstos (por ejemplo, para obtener nuestro número de tarjeta o conseguir acceso a nuestra cuenta bancaria).
- *Phishing*: se trata de una técnica de ingeniería social, esto es, que recurre al engaño de una víctima para que realice alguna acción, de forma que los ciberdelincuentes puedan acceder a nuestros sistemas u obtener información confidencial (por ejemplo, convenciéndonos para que hagamos clic en un enlace malicioso). El phishing puede darse a través de correo electrónico, pero también a través de SMS, aplicaciones de mensajería instantánea, a través de llamadas, etc.
- Suplantación de identidad: nuestra identidad digital podría ser robada por los ciberdelincuentes con el objetivo de suplantarnos y conseguir así algún tipo de beneficio a nuestra costa. Dado que la identidad digital es todo aquello que nos identifica en el entorno *online* (tanto los datos personales que utilizamos como nombre, correo, alias o contraseña, como la actividad que llevamos a cabo en redes sociales, blogs, etc.), es muy importante ser consciente de toda la información que estamos compartiendo.

A través de las técnicas anteriores, los ciberdelincuentes pueden cometer actividades delictivas con fines económicos, como estafas. Por ejemplo, pueden solicitarnos dinero haciéndose pasar por algún amigo o familiar, conseguir acceder a nuestra cuenta bancaria mediante portales de acceso falsos que simulan ser nuestro banco, solicitar transferencias en portales de compra-venta de productos, conseguir acceso a nuestra cuentas de redes sociales, etc.

Por todo ello, resulta imprescindible ser precavido y conocer estos riesgos para estar lo más preparado posible para afrontar estas situaciones.

**¿Por qué a mí? ¿Qué probabilidad hay de que algo así me ocurra?**

Si os estáis preguntando por qué motivo sois en concreto objetivo de los ciberdelincuentes, la respuesta es que en la mayoría de los casos no tiene por qué existir ningún motivo en especial. Si bien en ocasiones se realizan ataques dirigidos a personas específicas con un fin muy concreto, en la mayoría de los casos los ciberdelincuentes realizan campañas masivas en las que intentan obtener el máximo beneficio total posible y, por tanto, cualquier persona es realmente susceptible de ser suplantada o engañada por el mero de hecho

de estar conectada y realizar actividades a través de Internet.

Pero esta situación no debería preocuparnos en exceso, ya que no se trata ni de vivir con miedo ni de ignorar la situación, sino de estar lo mejor informados y preparados.

**¿Cómo me puedo proteger ante estas amenazas?**

Podemos realizar varias acciones para estar mucho más protegidos y preparados ante posibles estafas o intentos de suplantación de identidad, entre las que se encuentran:

- **Revisar nuestros registros en los sitios web** más relevantes (como aquellos en los que se almacenen información de pago como tarjetas de crédito) y dar de baja nuestra cuenta en aquellos que ya no utilicemos.
- **Utilizar métodos de pago seguros** como tarjetas prepago o tarjetas virtuales de un solo uso, como también considerar el no utilizar la misma cuenta bancaria para ahorro y compras por internet.
- **Ser precavido ante mensajes o llamadas inesperadas** que tienen un carácter urgente o que parecen suponer consecuencias graves si no actúas con rapidez.
- **Nunca pinchar en enlaces o ficheros adjuntos si no se está completamente seguro**, así como verificar siempre el remitente (el dominio de correo o llamada de número desconocido).
- **Descargar aplicaciones en nuestros dispositivos que provengan sólo de páginas web o tiendas oficiales**. En otro caso, existe un riesgo de que éstas incluyan algún *malware* oculto.
- **Mantener el sistema actualizado** en nuestros dispositivos.
- **Utilizar contraseñas robustas y diferentes** para cada sitio web donde nos registramos. De esta forma, si robaran tus credenciales, el impacto sería mucho menor.
- Para hacer más fácil el punto anterior, es recomendable **utilizar gestores de contraseñas**. Se trata de aplicaciones que nos permiten generar contraseñas robustas y aleatorias para cada sitio, teniendo sólo que memorizar una única contraseña o huella.
- **Configurar el doble factor de autenticación** en los servicios más importantes, como el acceso al correo electrónico o las redes sociales. De esta forma, nuestra cuenta estará protegida incluso si adivinaran nuestra contraseña.

Aplicando todos los puntos anteriores, estarás mucho más preparado ante posibles imprevistos, pero si todo lo anterior fallara y detectaras algún cargo desconocido en tu cuenta bancaria, contacta con tu entidad lo más rápido posible para que puedan actuar (por ejemplo, bloqueando la tarjeta o modificando tus claves de acceso a la banca electrónica).

Los ciberdelincuentes utilizarán métodos cada vez más sofisticados, pero recuerda que siempre puedes tomar el control y ponérselo un poco más difícil.