

CONSEJOS PARA PREVENIR SER UNA VÍCTIMA DEL PHISHING



1. **Verifica el remitente** de los correos electrónicos recibidos (descarta directamente los sospechosos. Sé incrédulo).
2. **Desconfía por completo de mensajes en los que te soliciten datos confidenciales.** Recuerda que las instituciones responsables nunca te piden este tipo de información por este medio.
3. **Introduce tu información personal únicamente en webs seguras** (las que empiezan por **https://** y en las que aparece un pequeño candado cerrado en la barra de estado del navegador).

[https:// es el protocolo destinado a la transferencia segura de datos de hipertexto que utiliza un sistema de cifrado]



4. **No accedas a tu banca virtual a través de enlaces incluidos en correos electrónicos** (las entidades bancarias nunca solicitan información a través de e-mail). Escribe directamente la dirección del banco o tienda on-line de confianza en la barra de tu navegador.
5. En la medida de lo posible, **evita transacciones bancarias o comerciales desde equipos públicos o que no sean de confianza.**
6. **Revisa periódicamente tus movimientos bancarios,** con el fin de detectar transacciones irregulares.
7. **Refuerza la seguridad de tu ordenador:** actualiza el antivirus, aplica parches de seguridad y analiza periódicamente tu pc.
8. Con frecuencia, el phishing se propaga por correo basura, por lo que **reducir o evitar el spam** te ayudará a protegerte frente a esta amenaza.
9. **Ante la más mínima duda, es mejor que te abstengas de facilitar información confidencial/personal.**



ACTÚA CON PRUDENCIA Y HAZ DE LA PREVENCIÓN UN HÁBITO

Más sobre la actualidad del phishing



<http://portal-seguridad>