

# Phishing

Los ataques de "phishing" usan la ingeniería social para **adquirir fraudulentamente información personal** de los usuarios. Mediante correos electrónicos que aparentan ser fiables y que suelen derivar en páginas web falsas, intentan **engañar a los usuarios** para que faciliten **datos de carácter personal** (datos de cuentas bancarias, contraseñas, números de seguridad social, etc.)



## Cómo evitar ser víctima del phishing

-  Compruebe el **dominio del correo remitente** y que su nombre coincide con su cuenta de correo electrónico (nombre y dominio).
-  **Desconfíe** de los correos electrónicos cuyo texto esté mal redactado o con faltas de ortografía.
-  Evite abrir **archivos adjuntos** si se desconoce al remitente o no se espera el documento.
-  Preste atención a la **sintaxis de los enlaces a páginas web** que le lleguen por correo electrónico. Una letra puede marcar la diferencia.
-  Si accede a páginas web a través de buscadores, antes de introducir datos personales, **compruebe siempre que se trata de la página web oficial y no una página secundaria** que recaba la información de su interés.
-  Si observa alguna anomalía en un correo electrónico, **contacte con el remitente a través de otro canal** (ej. Teléfono) para comprobar la autenticidad del mensaje.
-  Habilite el **segundo factor de autenticación** en todos los medios digitales que dispongan de él (aplicaciones bancarias, redes sociales, correo electrónico, etc.).
-  No introduzca datos personales en páginas web cuyo **enlace haya llegado acortado** (cort.as, bit.ly, etc.).
-  Utilice un navegador para las **gestiones bancarias y oficiales**, y otro **distinto** para la navegación habitual.
-  Mantenga **actualizado** el navegador, así como sus extensiones y complementos (Flash, Java, etc.).