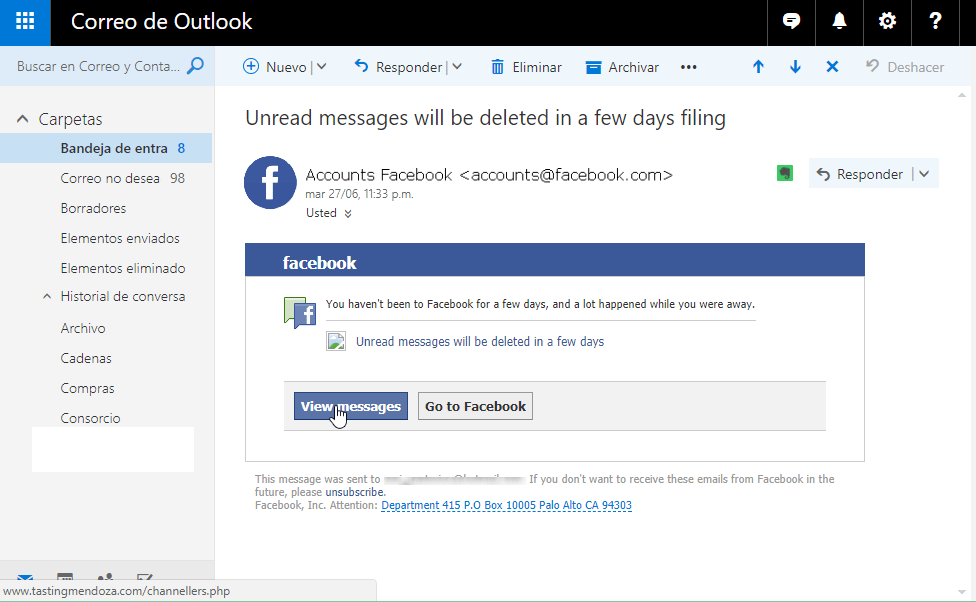
**Estafas en Internet: averigua si eres capaz de no caer en el engaño**

Averigua si eres el perfil de usuario que puede ser fácilmente engañado por los cibercriminales.



**EMPEZAR**

1. **¿Cómo se llama la técnica utilizada en el siguiente mensaje para engañar a los usuarios?**



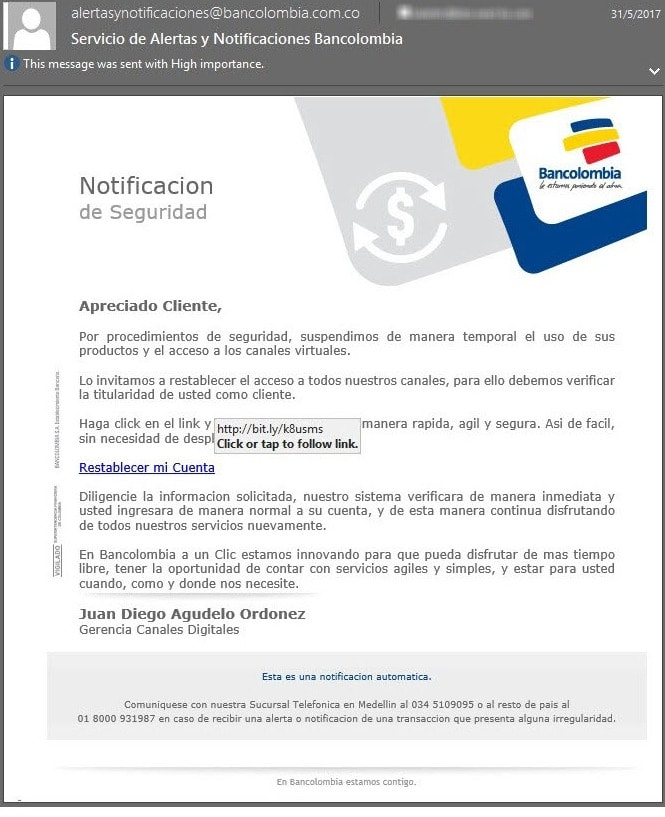
* Spoofing
* Ataque Homográfico
* Spearphising
* BlackHat SEO

**2)¿Cuál de los siguientes links se trata de un Ataque Homográfico?**



* Coto (1)
* Adidas (2)
* Nike (3)
* Ninguno

1. **¿Se trata de una notificación real?**



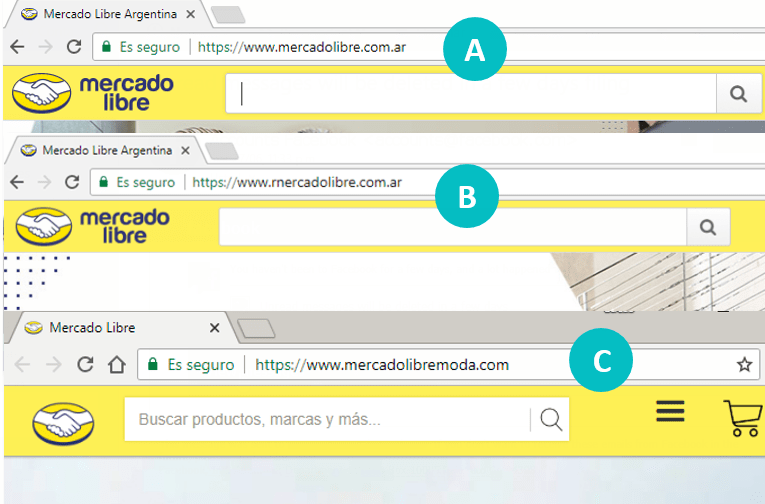
* Si, ya que el remitente pertenece a un dominio real de la institución
* Si, que no solicita datos personales
* No, ya que el link real está oculto mediante un acortador
* No, ya que el correo es despersonalizado y tiene errores de ortografía

1. **¿Qué información nos permite confiar 100% en este sitio?**



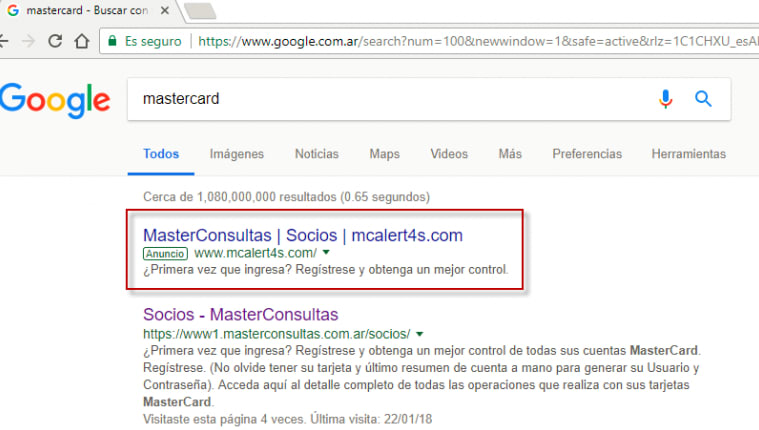
* Es un sitio seguro, que tiene HTTPS y un candado
* El certificado lleva el nombre de la compañía
* La URL está escrita correctamente
* Ninguna de las anteriores

**5) ¿Cuál es el sitio auténtico?**



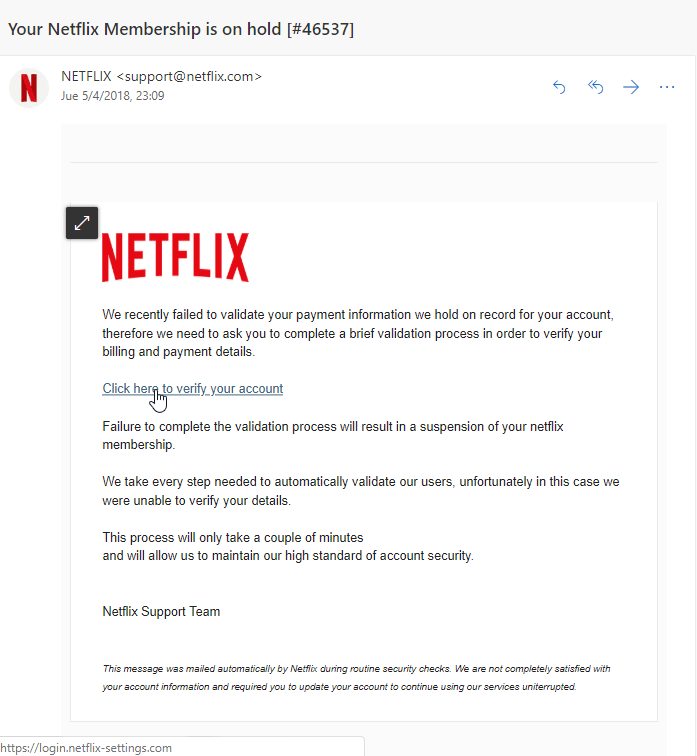
* El primero (A)
* El segundo (B)
* El tercero (C)
* El primero (A) y el tercero (C)

**6) ¿Cómo se llama la técnica que utiliza el cibercriminal para que sus víctimas ingresen al sitio fraudulento?**



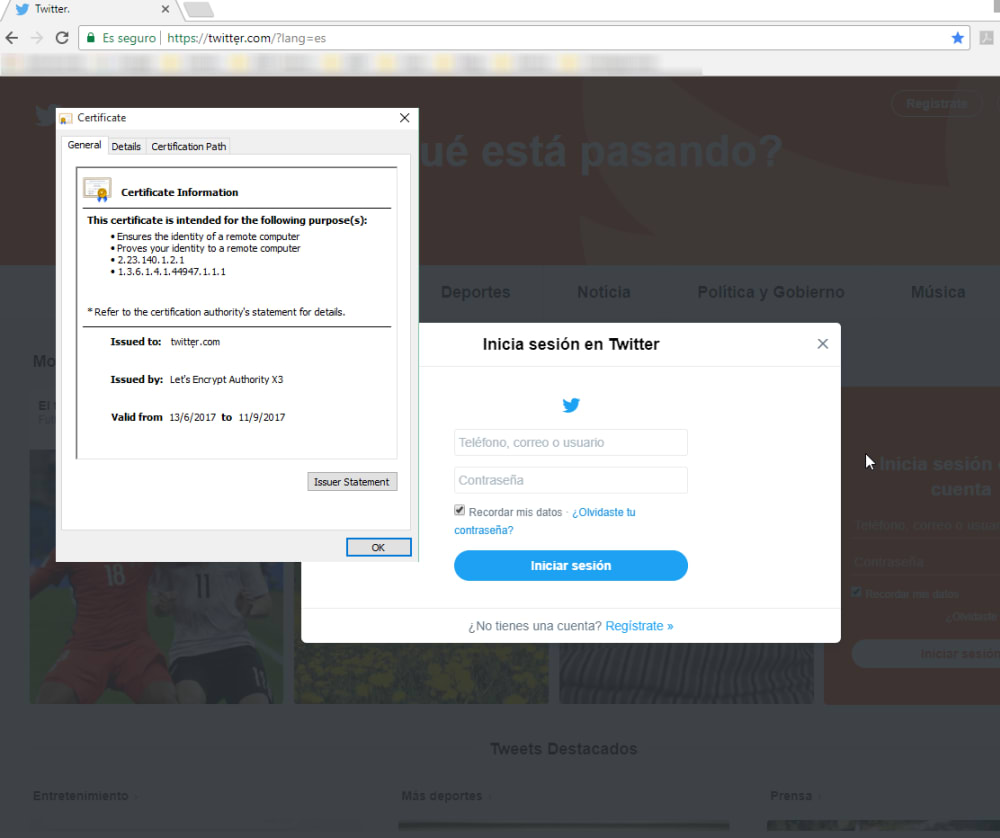
* Spoofing
* BlackHat SEO**:** contenido oculto, contenido duplicado, cloaking, doorway page (o gateway page), linkfarm, Private Blog Networks (PBN), Links pagos, Blog SPAM y SEO negativo.
* Malvertising
* Ataque Homográfico

**7) ¿Cómo se comprueba que se trata de un aviso real?**



* Está enviado desde una dirección de dominio de Netflix
* El link corresponde al dominio de Netflix
* Ambas anteriores
* Se trata un de correo fraudulento

**8) ¿Se trata del sitio real de Twitter?**



* Si, ya que es HTTPS y el certificado es válido
* Sí, ya que la URL está escrita correctamente
* No, ya que el certificado no es válido
* No, se trata de un ataque homográfico.