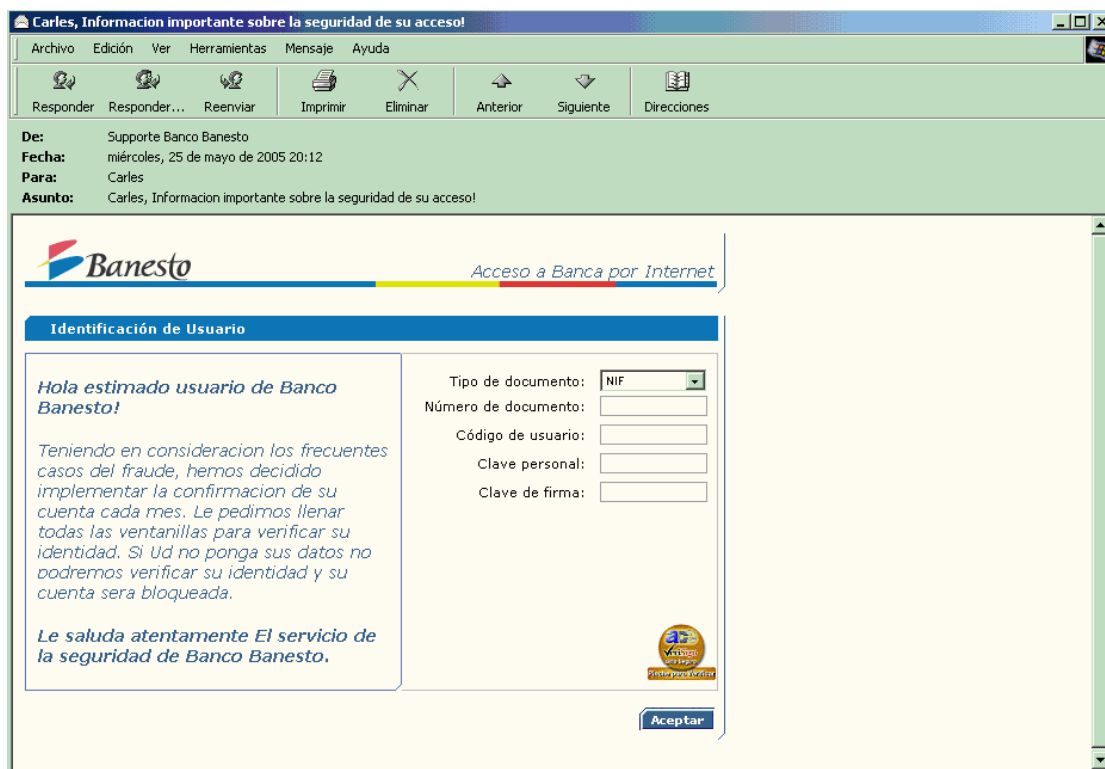


# PISHING

El Pishing es una estafa que se inicia con la recepción de un supuesto e-mail de tu banco o de una entidad comercial como PayPal, Ebay, etc. En dicho e-mail se expone una incidencia (actualización de servicios, verificación de su identidad, etc.). Una vez introducimos los datos estos son enviados a los estafadores y tienen luz verde para entrar en nuestra cuenta y robarnos todo el dinero que tenemos. A continuación muestro un ejemplo que he recibido:




Ejemplo de Pishing (Se trata de un email recibido a mi cuenta de correo)

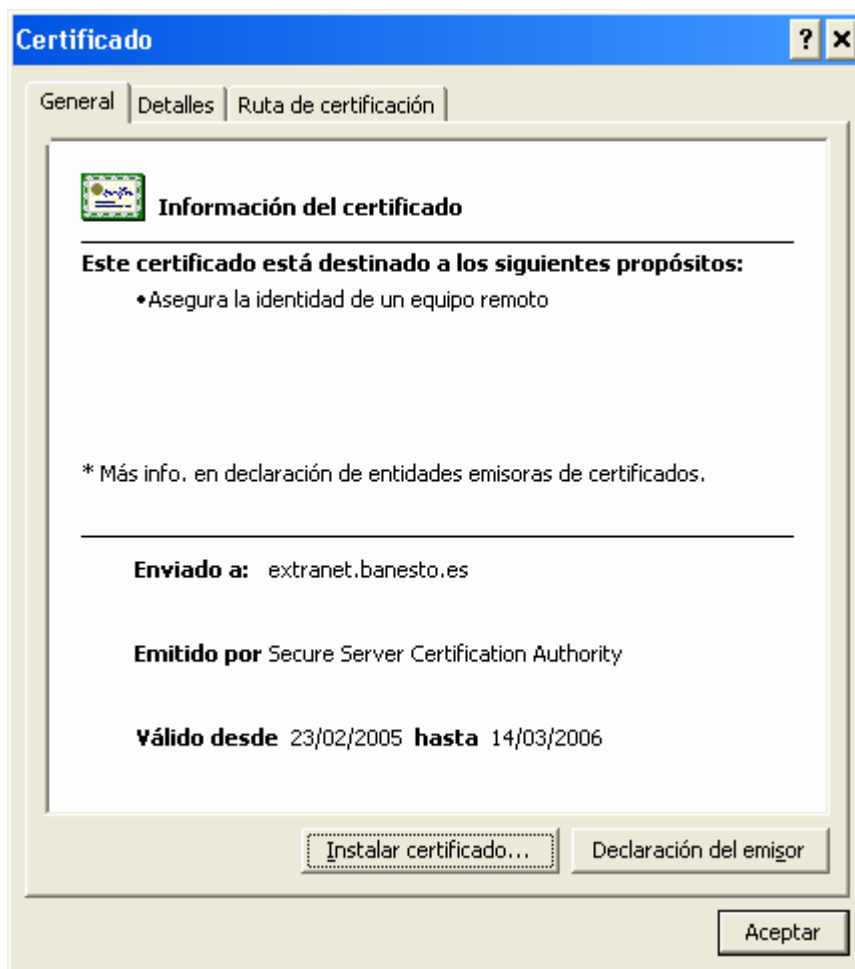


Página web REAL del banco (se parece al email recibido, ¿verdad?)

## WEBS SEGURAS (Protocolo SSL)

Se trata de páginas web que utilizan el protocolo SSL para encriptar la conexión a dicha web. Este tipo de conexiones son fácilmente reconocibles puesto que su dirección empieza por https: y aparece un candado en la esquina inferior derecha del navegador . Dicho protocolo crea un “túnel” entre tu ordenador y el servidor del banco, y la protege con una clave de 128 bits.

Si hacemos doble clic en el candado nos aparece la información del certificado usado para la conexión:



Para que esto funcione es necesario que un organismo independiente garantice que el ordenador al que nos conectamos es realmente el de nuestra entidad bancaria. Esta tarea la realizan las autoridades certificadoras (son como los notarios electrónicos reconocidos por los gobiernos de los distintos países), por ejemplo: **ACE** (Agencia Certificación Española), **VeriSign** o **Thawte** (a nivel Internacional)

### 6.- Certificación ACE / Verisign

El Servidor del Grupo Banesto ha sido certificado por **ACE / Verisign** lo que garantiza que las comunicaciones se realizan de forma cifrada.

Si desea consultar el estado del certificado del servidor de Banesto, pulse [aquí](#) (se accede a una página en inglés).



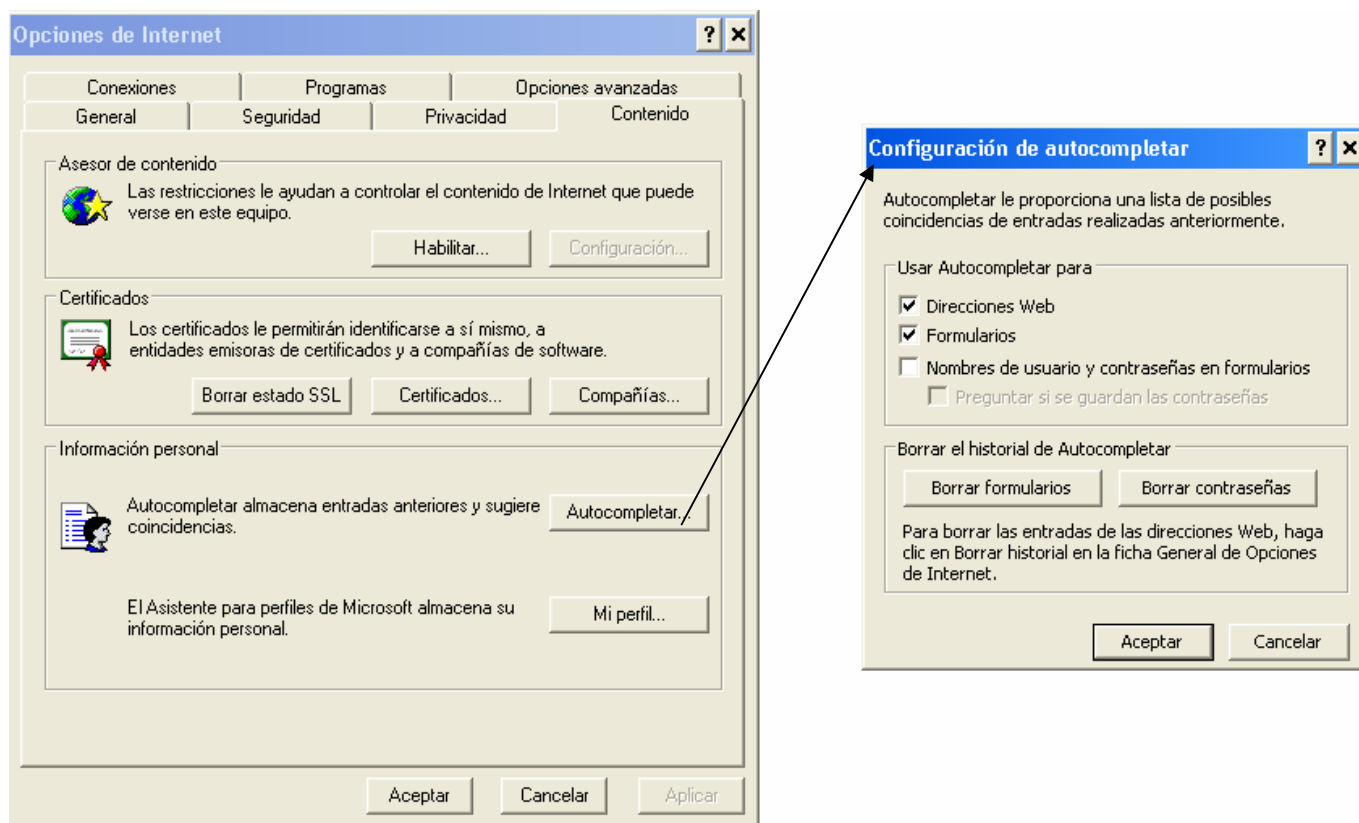
es la entidad externa del máximo prestigio a nivel mundial en la provisión de Infraestructuras de Clave Pública y en la emisión de Certificados.

En la web de la entidad bancaria aparece este mensaje indicándonos que ACE y VeriSign verifican que las comunicaciones con dicha web de la entidad se realizan de forma cifrada

## AUTOCOMPLETAR CONTRASEÑAS


Se trata de una opción que llevan los navegadores para recordarnos el nombre de usuario y su contraseña cada vez que accedemos a una web que nos pida dichos datos. Esta opción, aunque parezca que va muy bien, es un auténtico peligro, pues dicha información se almacena en un fichero de texto de nuestro ordenador (fácilmente accesible para cualquier troyano), por lo que la seguridad de dichos datos se ve claramente comprometida.

Para cambiar esta configuración debemos entrar en las opciones del navegador (Herramientas-Opciones de Internet) e ir a la pestaña de **Contenido**



Pulsando el botón Autocompletar nos aparece la ventana de la derecha. Es recomendable tenerlo como en la pantalla, de esta manera los nombres de usuario y las contraseñas no las guarda. Si queremos borrar toda la información que pudiéramos tener almacenada pulsamos en los dos botones de Borrar formularios y Borrar contraseñas

## CONSIDERACIONES A TENER EN CUENTA

- Los bancos JAMÁS enviarán nada por email (además solo entrar en la página REAL de nuestro banco encontramos un mensaje que nos lo dice)
- El símbolo del candado en la barra de estado (en la parte inferior del navegador)  nos está indicando que se trata de una página web segura. También lo podemos ver en la barra de direcciones, vemos que la dirección web ha cambiado y empieza por **https://** en lugar de **http://** que sería lo normal para las páginas web
- Buscar el sello de ACE, VeriSign u otra autoridad certificadora en las webs que requieren el uso de datos confidenciales
- Al terminar la sesión, desconectarse de la cuenta bancaria antes de abandonar la web o de cerrar el navegador
- No enviar ningún dato bancario por correo electrónico (aunque el destinatario sea de confianza), pues esta información viaja en texto plano (es decir, sin cifrar) y puede ser captada
- Como medida de seguridad es más que recomendable cambiar periódicamente las claves de acceso a nuestra cuenta
- Borrar periódicamente las cookies y los ficheros temporales que se almacenan en el ordenador
- Consultar los consejos de seguridad que aparecen en la página web de tu banco
- Evitar conectarse a páginas web de contenido privado en ordenadores públicos (cibercafés, universidad, etc.)
- No utilizar la opción “Autocompletar contraseñas” de los navegadores. No hay que guardar las claves en ningún fichero

## ¿ES SEGURO COMPRAR POR INTERNET?

La primera regla para la seguridad online es bien sencilla: Tenemos que estar bien protegidos. Esto se consigue primeramente por tener un buen antivirus actualizado (McAfee, Kaspersky, Trandmicro o Norton, por ejemplo) y si puede ser disponer de algún Cortafuegos (Firewall), por ejemplo McAfee o Norton Internet Security, Zone Alarm, Kaspersky, etc. También tenemos que estar seguros que no tenemos ningún troyano ni nada parecido en nuestro ordenador, esto lo podemos hacer usando un programa antispyware como Ad-Aware o SpyBot (hay un documento que he hecho donde hablo de este tema)

A partir de aquí y teniendo muy presente las recomendaciones mencionadas anteriormente es totalmente seguro comprar por internet, subastas online, acceder a nuestras cuentas bancarias, hacer transferencias, comprar acciones, etc.

## PAYPAL

Cuando vamos a realizar una compra en cualquier comercio online, este nos pide los datos de nuestra tarjeta bancaria (por supuesto, antes de dar ningún dato debemos tener bien presente las recomendaciones que he mencionado antes), una vez damos dichos datos y el comercio nos cobre el producto adquirido, debemos confiar en la honestidad del comercio para que solo utilice dichos datos en la compra y no para fines maléficis

Para evitar este problema surgió **PayPal**, una forma de pago gratuita que asocia una tarjeta bancaria a una dirección de email. Cuando pagas con PayPal el comercio no recibe ningún dato bancario, mediante email ordenas a PayPal que pague al comercio.

PayPal es aceptado por la mayoría de los comercios y es el sistema más usado en los pagos entre particulares (subastas, segunda mano, etc.)

## ENLACES DE INTERÉS

[www.antiphishing.org](http://www.antiphishing.org)

[www.ace.es](http://www.ace.es)

[www.verisign.es](http://www.verisign.es)

[www.paypal.es](http://www.paypal.es)

[www.delitosinformaticos.com/](http://www.delitosinformaticos.com/)

[www.seguridadenlared.org](http://www.seguridadenlared.org)

[www.hispasec.com/](http://www.hispasec.com/)

[www.aui.es](http://www.aui.es)

[www.internautas.org/](http://www.internautas.org/)

[www.noticias.com](http://www.noticias.com)