



## **PHISHING: FRAUDE EN INTERNET**

### **1. INTRODUCCION:**

Cada día surgen en Internet nuevas amenazas que provocan que estemos al día en todo lo referente a actualizaciones, parches, vulnerabilidades del sistema, virus, etc. Pero ahora la nueva moda de delitos por internet se denomina Phishing. La gran diferencia con lo anteriormente citado es que esta vez nadie intenta acceder a tu sistema con intenciones maliciosas, o tratan de introducirte un virus que puede provocar el mal funcionamiento de tu computadora. Con un phishing, es el propio usuario quien envía información personal y confidencial de forma voluntaria; eso si, animado mediante técnicas de engaño.

### **2. ¿QUÉ ES?**

El PHISHING no es más que la suplantación de sitios de internet. Se tratan de correos electrónicos engañosos y páginas Web fraudulentas que aparentan proceder de instituciones de confianza (bancos, entidades financieras, etc.), pero que en realidad están diseñados para embaucar al destinatario y conseguir que divulgue información confidencial.

El término phishing significa "pescar", en inglés, ya que en realidad tiene cierta similitud con la pesca. Se lanza un cebo y se espera a que alguien "pique". La recompensa no puede ser más sabrosa: datos personales y claves de acceso a tus cuentas bancarias.

### **3. ¿COMO FUNCIONA?**

A través de un mensaje electrónico, simulando proceder de una fuente fiable (por ejemplo, de tu banco), se intentan recoger los datos necesarios para estafar al usuario. En realidad se trata de mensajes masivos. Los estafadores no saben cuál es tu banco y por ello crean un mail con la apariencia corporativa del banco escogido y se envía masivamente. La realidad es que alguno de esos mensajes llegará a alguien que pertenezca a ese banco.

Normalmente se trata mensajes con textos como: "Por motivos de seguridad...", o "Su cuenta se debe confirmar...", o "Usuarios del banco advierten", indicando al usuario que se están realizando cambios y que por seguridad debe introducir sus datos personales y códigos bancarios pinchando en un link que ellos te indican. Al pinchar se redirecciona a una página con gran similitud a la de tu banco habitual. La verdad es que esa página pertenece al estafador, quien no tiene más que copiar los datos que el usuario rellena. Al finalizar te confirma la operación y te quedas tranquilo pensando que esos datos los ha recogido tu banco sin menor problema.

Otras veces el mismo mail te pide que rellenes los datos y pulses "enviar", sin necesidad de redireccionarte a otra página.

La sorpresa en ambos casos llegará cuando encuentres que tu cuenta bancaria está a cero, y tu banco te informe que has sido víctima de una estafa denominada "phishing".



#### 4. ¿COMO EVITARLO?

El fenómeno del phishing ha adquirido gran importancia a nivel mundial, tanto a nivel de usuarios como a nivel de empresas, incluido los propios bancos, que observan como no pueden hacer nada al respecto mientras sus clientes son estafados y además pierden confianza en la "banca online".

Actualmente, la única forma de evitar este tipo de estafas consiste en estar informados y concienciados. Por desgracia, ningún antivirus ni ningún sistema de seguridad pueden impedir estos ataques. A continuación exponemos unos consejos que nos podrán ayudar a reconocer este tipo de mensajes:

1. En primer lugar, y tal vez lo más importante, es que debemos recordar que en España los bancos o cajas se comunican siempre por correo tradicional. Nunca le pedirán que introduzca datos personales o bancarios en un e-mail
2. En España se están empezando a dar casos de este tipo de estafa a bancos españoles, pero por el momento son escasos y los mail que están recibiendo los usuarios están escritos en inglés. Es lógico pensar que un banco español no te enviará comunicados en inglés.
3. Siempre que recibamos un e-mail desconocido o de dudosa procedencia, es aconsejable llamar inmediatamente al banco para confirmar la veracidad del mensaje.
4. Observar si la dirección comienza con https: en lugar de solo http: (La "S" indica que la página está albergada en un servidor seguro.)

**ATENCIÓN:** Las técnicas de Phishing están aprendiendo rápidamente de este tipo de errores y los están perfeccionando. Consiste en crear una ventana emergente justo en la posición donde aparece la URL en la barra de dirección de Internet Explorer, de forma que se superpone y oculta la dirección real del servidor Web del atacante donde realmente se encuentra el usuario, mostrando en su lugar la URL de la entidad bancaria. El mensaje incluye un enlace que supuestamente le dirige a la Web de la entidad. Si el usuario pincha en el enlace, puede observar como aparece la Web de la entidad y que en la barra de direcciones de Internet Explorer aparece la URL correcta, incluyendo el prefijo https:// como si estuviera en una conexión segura.

5. Si tienes alguna duda, puedes pasar el cursor por encima del enlace que lleva adjunto el correo. Muchas veces la dirección no es la misma que aparece en el mensaje.
6. Otra manera de reconocer estos mensajes es que no van personalizados. Normalmente llevan el titular de: "Estimado cliente".
7. Procure no dirigirse a sus webs financieras de confianza a través de enlaces facilitados o direcciones de Internet cuyo origen es desconocido.
8. También puedes confirmar que en la parte baja del navegador se vea un candado entero (no roto). Este símbolo indica un certificado de autenticidad y si pinchamos sobre él, se mostrarán los datos del certificado. Podremos comprobar que no esté caducado y que el propietario del mismo corresponde a la página que estás viendo.



Queremos recordarle que el phishing no es algo nuevo y que no se extiende únicamente a entidades financieras. En general debemos ser cautelosos y sospechar ante cualquier ventana emergente que nos pida datos bancarios. Otros fraudes con mensajes engañosos se pueden encontrar en falsas ventanas o e-mails enviados a usuarios de Hotmail. Otro de los sectores más perjudicados es el de subastas y ventas on-line.

My MSN | Hotmail | Shopping | Money | People & Chat | Search

## Hotmail Account Update

### Provide your billing information

**Billing information**

Type your name as it appears on your payment method.

**First name**

**Last name**

**Payment method** Debit card

**Debit card type**

**Name on debit card**

**Debit card number**

**Expiration date**

**Civ/Cvv2**  Last 3 digits located on the back of your card

**Card PIN Number**  Your 4 digit number used in ATM transactions

**Billing address**

Type your address exactly as it appears on the billing statement for your payment method.

**Address Line 1**

**Address Line 2 (optional)**

**City**

**State**

**ZIP/Postal code**

**Country/Region**

**Area code & phone number**   Ext.

\*Your debit card will not be charged.

Microsoft Internet Explorer

PLEASE READ CAREFULLY

Welcome to MSN's Billing Center!

Our current records indicate that your account may be suspended. However, you have to provide us new billing information. Valid billing details are required to maintain availability of your account.

Please have the following:

- Your last Billing Statement.
- Your current debit card(s).
- Any relevant information.

## Please Sign In [Need Help?](#)

For security reasons please re-enter your user ID and password.

**eBay User ID**

[Forgot your User ID?](#)

**Password**

[Forgot your password?](#)

Copyright © 1995-2004 eBay Inc. All Rights Reserved.  
Designated trademarks and brands are the property of their respective owners.  
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



## 5. REPERCUSION DEL PHISHING

En la actualidad, los casos más graves de phishing se han producido en Estados Unidos, aunque las mafias se han dado cuenta de su gran potencial, por lo que su expansión se está produciendo a nivel mundial, sobre todo en los países de habla inglesa donde se encuentra ahora más concentrado. En España se han dado, por el momento, casos en Banco Pastor, Banco Popular y Banesto, los cuales analizaremos más adelante.

La empresa Gartner ha analizado el problema del Phishing y realizó un interesante estudio sobre este fenómeno en Estados Unidos. A continuación exponemos las conclusiones más relevantes:

Los intentos de fraude contra consumidores en Internet, mejor conocidos como *phishing*, se han vuelto tan comunes que se estima que 57 millones de estadounidenses han recibido algún tipo de correo fraudulento, de acuerdo con un nuevo estudio presentado por Gartner. Las pérdidas directas del fraude de identidad contra estas víctimas relacionadas con ataques tipo *phishing*, costaron a los bancos y compañías de tarjetas de crédito alrededor de 1,200 millones de dólares el año pasado.

Basados en una encuesta aplicada a 5,000 adultos que usan Internet, los analistas de Gartner estiman que aproximadamente 30 millones de adultos usuarios de la Web creen que definitivamente han experimentado un ataque *phishing*, mientras que otros 27 millones creen que han observado lo que parece ser un intento de fraude.

Los intentos de ataques *phishing* no son nuevos, pero se han vuelto más comunes en los últimos 12 meses. De acuerdo con la encuesta de la firma consultora, 76% de los ataques sospechosos ocurrieron en los últimos seis meses (desde octubre del 2003) y otro 16% ocurrió hace seis meses o antes. Por lo tanto, los resultados combinados sugieren que 92% de los intentos de fraude han tenido lugar en el último año.

“Las instituciones financieras, proveedores de servicios de Internet y otros proveedores de servicios deben de tomar en cuenta seriamente este tipo de fraudes”, dijo Avivah Litan, vicepresidente y director de investigación de la firma. “Estos proveedores de servicio deben tomar acciones y aplicar soluciones que dramáticamente minimicen o erradiquen la amenaza, incluso si los proveedores de servicios no son blancos directos. Eventualmente, todos los involucrados en el comercio electrónico en Internet se verán afectados por una falta de confianza del consumidor en sus transacciones si los fraudes no son reducidos en forma significativa de los niveles en que actualmente se encuentran”.

El ataque tipo *phishing* ocurre cuando un ciberpirata manda un correo electrónico que contiene una liga a un sitio de red fraudulento donde se le solicita al usuario que provea información sobre su cuenta personal. El correo electrónico y el sitio de red están típicamente disfrazados simulando ser el de uno de los proveedores de servicios de confianza, institución financiera o comercio en línea de los usuarios.

La encuesta de Gartner, completada en abril, mostró un alto grado de éxito por parte de los defraudadores. Basándose en los resultados de la encuesta, Gartner estima que alrededor del 19% de los atacados o casi 11 millones de estadounidenses adultos que usan Internet, han dado clic a un correo de intento de fraude. Peor aún, 3% de los atacados o un estimado de 1.78 millones de adultos, reportan haber dado a los defraudadores su información financiera o personal.



Los datos indican que "las víctimas de fraudes tipo *phishing* son casi tres veces tan propensas a identificar un fraude, como lo son otros consumidores en línea", mencionó Litan. "De cualquier forma en que se vea, los ladrones están logrando sus objetivos fraudulentos. Los proveedores de servicios no tienen más opción que combatir dichos correos, si es que quieren que la computación en línea se vuelva más confiable como un canal para las transacciones con clientes".

Las soluciones en contra de los fraudes tipo *phishing*, desde correos con firma electrónica digital hasta servicios *anti-phishing* administrados, son algunas de las tecnologías que discutirán en notas de investigación futuras de Gartner.

## 6. LUCHANDO CONTRA EL PHISHING

### 6.1 ANTI-PHISHING WORKING GROUP" (APWG)

La rápida proliferación de esta nueva estafa se ha convertido en una de las principales causas de lucha de las empresas contra los delitos on-line. En Estados Unidos se ha creado la "**Anti-Phishing Working Group**"(APWG). Se trata de una asociación de industrias cuyo principal objetivo es acabar con el robo de identidad y fraudes resultantes del creciente problema del phishing en correos electrónicos fraudulentos. Si quieres ampliar información sobre esta organización, puedes visitar su página Web: <http://www.antiphishing.org>; y en caso que detectes un caso de estafa sobre phishing, puedes denunciarlo y enviarles un email a [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org)

Anti-Phishing Working Group  
**APWG**
register

## Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

[report phishing - click here](#)

- [Home](#)
- [Phishing Archive](#)
- [Report Phishing](#)
- [Events](#)
- [APWG News](#)
- [Resources](#)
- [Membership](#)
- [APWG Member Site](#)
- [Contact Us](#)
- [JOIN THE APWG](#)

**PARTNER EVENT:**

Spam Compliance  
  
**inbox**  
 THE EMAIL EVENT

### What is Phishing?

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

#### Unique Phishing Attack Trends May 2004 - July 2004

Date	Cumulative Phishing Attacks	Weekly Phishing Attacks
5/1/2004	215	215
5/8/2004	279	268
5/15/2004	321	374
5/22/2004	310	305
5/29/2004	224	327
6/5/2004	315	358
6/12/2004	339	392
6/19/2004	303	423
6/26/2004	324	455
7/3/2004	424	479
7/10/2004	418	438
7/17/2004	419	381
7/24/2004	395	421
7/31/2004	504	475

**News and Events:**

- 30-Aug-04 - New Phishing Trends Report Available!  
[Phishing Attack Trends Report - July 2004](#)

**Anti-Phishing Working Group**  
The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity and fraud that result from the growing problem of phishing and email spam.

**APWG Members**

- Over 636 members
- Over 407 companies
- 8 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 100 technology vendors
- Law enforcement from Australia, Canada, UK, USA

**APWG Working Groups**

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Sizing the Problem
- Solution Evaluation/Trial
- Law Enforcement

**APWG SPONSORS:**

Esta organización realiza un informe mensual analizando todos los ataques de phishing denunciados a APWG. Su último informe publicado corresponde a Julio de 2004 y lo podemos encontrar en su página Web (en inglés). A continuación os reproducimos los datos más relevantes del informe.



## 6.2 DATOS

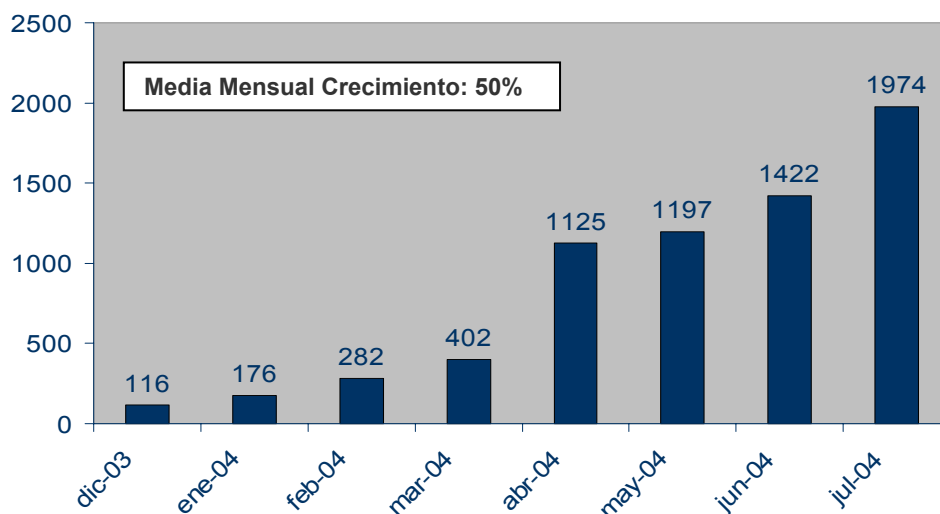
- ▶ Número de ataques únicos de phishing\* reportados durante Julio: **1974 ataques**
- ▶ Media mensual del ratio de crecimiento: **50%**
- ▶ Organización más atacada durante Julio: **Citibank (682)**
- ▶ País con mayor número de Webs alojadas de phishing: **USA (35%)**

\*Un "ataque único de phishing" se define en este análisis como un solo envío masivo de correos electrónicos enviados de una vez, destinados a una compañía u organización, y escritos en una misma línea de texto.

### ▶ **NÚMERO DE ATAQUES ÚNICOS DE PHISHING**

En Julio, se produjeron 1974 nuevos y únicos ataques de phishing denunciados a la APWG. Esto significa un aumento de un 39% sobre el número de ataques registrados en el mes de Junio (1422). La media de números de ataques diarios registrados en Julio fue de 63.7 (dato muy significativo considerando que en Junio la media fue de 47.6). La última semana de Julio fue la peor al registrarse más cerca de 500 ataques.

### Gráfica de ataques únicos mensuales



Fuente: Anti-Phishing Working Group



► **¿QUE ORGANIZACIONES O COMPAÑIAS ESTAN SIENDO MÁS ATACADAS POR PHISHING?**

Cuando hablamos de organizaciones más atacadas, queremos hacer referencia a los correos electrónicos fraudulentos que simulan provenir de una organización concreta. Obviamente, los más atacados y realmente perjudicados son los usuarios y clientes de esa organización.

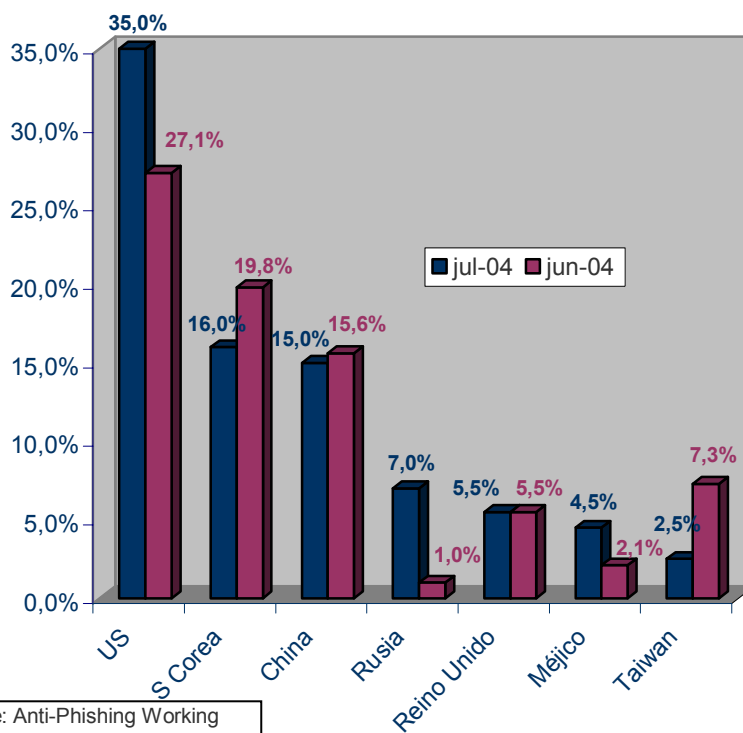
Empresa "Blanco"	Jul-04	Jun-04	May-04	Abr-04	Mar-04	Feb-04	Ene-04
Citibank	682	492	370	475	98	58	34
U.S.Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
Lloyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9

Fuente: Anti-Phishing Working Group

► **PAISES CON MAYOR NÚMERO DE WEBS ALOJADAS DE PHISHING**

Estados Unidos es una vez más el país "líder" en número de alojamiento de webs con phishing. Otros países, incluyendo Rusia, Reino Unido y Méjico han mostrado un incremento significativo en el alojamiento de estas páginas.

**Países con mayor número de webs alojadas de phishing**



Fuente: Anti-Phishing Working Group



### **6.3 CICLO DE VIDA DE WEBS PHISHING**

La media de "vida" de este tipo de Webs fraudulentas, medidas según el tiempo que estén hasta que se deje de responder a su engaño, es de 6.1 días.

Hasta la fecha, la web phishing más duradera conocida fue de 31 días (en otras palabras, esta web estuvo funcionando durante un mes completo)

## **7. INTENTOS DE ESTAFA A BANCOS ESPAÑOLES**

Como hemos señalado con anterioridad, las estafas de phishing están creciendo sobre todo en los países de habla inglesa. Pero en España se han dado casos de phishing utilizando las mismas técnicas: envío masivo de correos electrónicos pidiendo al usuario información privada. Analizaremos los casos de Banesto y de Banco Pastor.

### **CASO BANESTO:**

El mensaje solicita a los clientes se dirijan a una dirección del sitio web de Banesto para reactivar la cuenta con un nuevo sistema de seguridad que evitará las estafas. El remite falso del mensaje aparece con el nombre de "Banesto Banca" con dirección <[serv.atencion@banesto.es](mailto:serv.atencion@banesto.es)>, y en el campo de asunto el texto "Banesto Banca: Estimado cliente!". El cuerpo del e-mail, en formato HTML, incluye una cabecera gráfica con el logotipo y elementos gráficos de la imagen corporativa de Banesto, en un intento de hacer más creíble el engaño.

Sin embargo, en la redacción del texto del mensaje pueden observarse varias faltas de ortografías e incoherencias, no propias de un comunicado serio de cualquier entidad, y que deben hacer sospechar a los usuarios. Este extremo también apuntaría al origen extranjero de la estafa.

En cuanto al apartado técnico, todos los elementos gráficos del mensaje son descargados desde el servidor <http://www.tedfahn.com/>, donde también pueden encontrarse numerosos logs de otros ataques. El formulario falso, donde se solicita al cliente de Banesto sus datos, se encuentra hospedado en el servidor: <http://www.fischers.nu/>.

En ambos casos es más que probable que se traten de servidores webs legítimos que han sido comprometidos y utilizados por los atacantes para llevar a cabo la estafa. En el mensaje la URL de la web de Banesto aparece a simple vista correctamente escrita, en un gráfico, que al ser pinchado redirige realmente a la web <http://www.fischers.nu/> donde se encuentra el formulario falso.

El enlace que utilizan internamente para la falsificación se encuentra ofuscado en el código HTML como:

<http://extranet.banesto.es.npage.loginParticulares.htm%01@www.%66%69%73%63%68%65%72%73%2E%6E%75>

Con este formato los atacantes intentan aprovechar una vulnerabilidad de Internet Explorer para que el usuario visualice una URL concreta en la barra de direcciones, cuando en realidad está visitando un sitio web diferente. Esta vulnerabilidad ya fue corregida en un parche de Microsoft en febrero de este año, y los usuarios con Internet Explorer actualizado no se encuentran afectados ni podrán ser víctimas de la estafa en esta ocasión.



### **CASO BANCO POPULAR:**

(Observen la cantidad de faltas de ortografía en el texto del mensaje)

El email que han recibido los posibles afectados es el siguiente:

De: Banco Pastor [mailto:support@bancopastor.es]

Enviado el: jueves, 27 de mayo de 2004 12:29

Asunto: Importante informacion sobre la cuenta de Banco Pastor ¡Querido y apreciado usuario de Banco Pastor!

Como parte nuestro servicio de proteccion de su cuenta y reduccion de fraudes en nuestro sitio web, estamos pasando un periodo de revision de nuestras cuentas de usuario. Le rogamos visite nuestro sitio siguiendo link dado abajo. Esto es requerido para que podamos continuar freciendole un entorno seguro y libre de riesgos para enviar y recibir dinero en linea, manteniendo la experincia de Banco Pastor.Despues del periodo de verificacion, sera redireccionado a la pagina principa de Banco Pastor. Gracias.

[https://pastornetparticulares.bancopastor.es/BEPBEBEPA\\_F.jsp](https://pastornetparticulares.bancopastor.es/BEPBEBEPA_F.jsp)

El enlace ofrecido en dicho email está redireccionado a la dirección <http://ebay.dasmarket.biz/pastor/bepe.html>, página en la que se reproduce la portada de la web del banco Pastor, y en la que se solicita por parte del usuario la inclusión del NIF o CIF y la identificación y clave de acceso a la interfaz banca electrónica.

El banco Pastor ha indicado que sus comunicaciones con sus clientes no son a través del correo electrónico.

## **BIBLIOGRAFIA**

### Revistas:

- ▶ Personal Computer: Octubre 2004. Nº 21
- ▶ PC Pro: Nº 51 2004

### Internet:

- ▶ [www.hispasec.com/unaaldia/2163](http://www.hispasec.com/unaaldia/2163)
- ▶ [www.vnunet.es/Actualidad/Noticias/Seguridad/Privacidad/20040927017](http://www.vnunet.es/Actualidad/Noticias/Seguridad/Privacidad/20040927017)
- ▶ [www.el-mundo.es/navegante/2004/09/27/seguridad/1096287700.html](http://www.el-mundo.es/navegante/2004/09/27/seguridad/1096287700.html)
- ▶ <http://www.antiphishing.org/>

### Informes:

- ▶ Anti-Phishing Working Group. "Phishing Attack Trends Report - July 2004." Julio 2004