

Seguridad en la red

Fernando Tricas García
ftricas@unizar.es

Dpto. de Informática e Ingeniería de Sistemas del Centro Politécnico Superior
Universidad de Zaragoza, España

<http://www.cps.unizar.es/~ftricas/>

Curso 'Educación del Consumidor'

9 de noviembre de 2006

Índice

- ▶ Algunas definiciones
- ▶ Modos de atacar la seguridad y la privacidad
- ▶ Algunas reglas de autoprotección
- ▶ Confidencialidad y autenticidad
- ▶ Para saber más
- ▶ Conclusiones

Algunas definiciones

ESPASA:

PRIVADO, DA adj: Que se ejecuta a la vista de pocos, familiar y doméesticamente, sin formalidad ni ceremonia alguna || Particular y personal de cada uno.

INTIMIDAD: Parte personalísima, comúnmente reservada, de los asuntos, designios, o afecciones de un sujeto o de una familia.

Algunas definiciones

Oxford English Dictionary:

PRIVACY (from private) The state or quality of being private. The state or condition of being withdrawn from the society of others, or from public interest; seclusion. || The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. Also attrib. designating that which affords a privacy of this kind. 'one's right to privacy'.

Privacidad vs. Seguridad Pública

Algunas objeciones

- ▶ Existen herramientas para ayudarnos a proteger nuestra privacidad.
- ▶ Esas herramientas, ¿no serán una ayuda para que gente con pocos escrúpulos cometa sus 'fechorías'?

Privacidad vs. Seguridad Pública

Pero ...

- ▶ También se puede comprometer esa seguridad con otras tecnologías (teléfono, cartas, anuncios en la prensa, ...)
- ▶ La tecnología está disponible, prohibirla no impide su uso.
- ▶ Nosotros también podemos necesitar protegernos.

¿Todos somos espías?



(Casi) todo el mundo lleva una cámara en el bolsillo, hay un montón de cámaras por las calles, ...

¡hasta Google!

Ataques a la privacidad/seguridad

- ▶ La mayoría de los usuarios son gente común '*como nosotros*'.
- ▶ ¿A quién pueden interesar mis datos?
- ▶ ¿Quién puede querer hacerme daño?

Ataques a la privacidad/seguridad

Ojo!!

- ▶ Puedo tener acceso a información importante.
- ▶ Alguien puede utilizarme como intermediario (o herramienta).
- ▶ Romper sólo porque es posible (y fácil a veces).

¿Con qué debo tener cuidado?

- ▶ Acceso físico a los recursos

¿Quién tiene acceso?

- ▶ Conocidos.
- ▶ Desconocidos.
- ▶ Computadores compartidos.
- ▶ Servicios de mantenimiento.

¿Dónde están?

- ▶ En un despacho cerrado
- ▶ En un laboratorio común
- ▶ En ...

¿Con qué debo tener cuidado?

- ▶ Técnicas de ingeniería social
 - ▶ Cuidado con gente muy 'amistosa'.
 - ▶ Si en la calle no se lo dirías, ¿en la red si?.
 - ▶ Si normalmente se hace de una manera, ¿por qué cambió?.
 - ▶ ¿Qué datos puede pedirme un técnico?

Ingeniería social

- ▶ Un poco + otro poco + varios pocos = mucha información
 - ▶ Primera llamada: nombre del jefe.
 - ▶ Con el nombre del jefe: localización de un recurso.
 - ▶ Con el nombre del jefe y la localización del recurso ...

Confidencialidad de los datos

- ▶ La prudencia nos ayuda a disminuir los peligros
- ▶ Pero queremos comunicarnos!!!

Además

... ¿Cómo viaja la información por la red?

¿Cómo viaja la información por la red?

¿Entonces?

- ▶ Objetivo: transmisión de información, fiabilidad y robustez, no seguridad.
- ▶ No sabemos por dónde viaja nuestra información (ni tenemos control sobre ello).

Puertos (sin mar)

- ▶ Habitualmente, una sola conexión (dirección)
- ▶ Muchos servicios (mail, web, compartir archivos, ...)
- ▶ Solución: asignarles diferentes números (como a los buzones de una oficina)
- ▶ Conexión \longrightarrow dirección + servicio

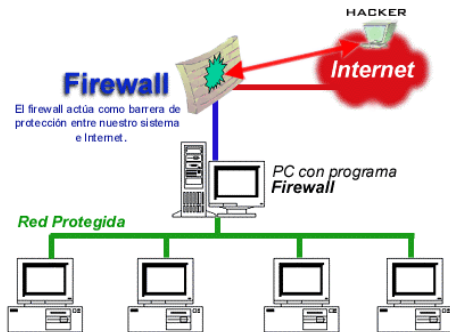
¿Y?

Puertos (¿Y?)

- ▶ Si no damos los servicios, es mejor que no estén abiertos los puertos correspondientes.
- ▶ ¡Usar un cortafuegos!
- ▶ Uno, general (a la entrada de la red)
- ▶ Uno, personal (en cada PC)

<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=2>

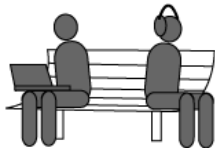
El cortafuegos



Redes inalámbricas



La información se transmite por el aire (radio)



What is wireless fidelity?

Wi-Fi, or Wireless Fidelity, connects computers with radio signals. The technology enables users to network PCs and laptops without running any additional cables or drilling holes in walls and floors. It also lets users share a single high-speed Internet connection and files as well as peripheral devices such as printers and external drives — all at the same time.

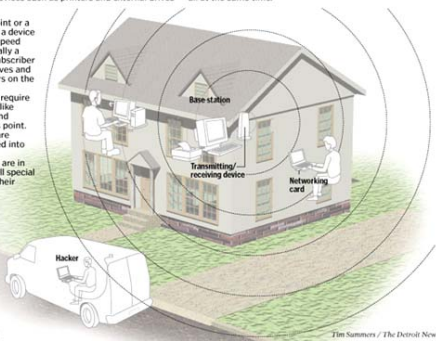
How it works

Wi-Fi requires an access point or a base station. It's essentially a device that's plugged into a high-speed Internet connection — usually a cable modem or a digital subscriber line (DSL). The device receives and transmits data to computers on the network.

Computers on the network require special adapters that work like antennae to receive from and transmit data to the access point. They're usually cards that are installed into PCs or inserted into laptops.

Once the network adapters are in place, users must then install special software to connect all of their computers.

Since Wi-Fi uses radio signals to send and receive data, it's fairly easy for hackers — also called "war drivers" — with the right tools and software to tap into wireless home networks and access users' Internet connections and information stored on their computers.



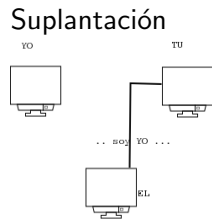
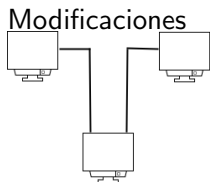
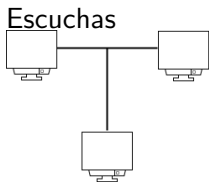
Source: The Detroit News research

Tim Summers / The Detroit News

Precauciones WiFi

- ▶ Cuidado con las claves
- ▶ Control de acceso con autenticación bidireccional
- ▶ Configuración WEP (128 bits). Mejor WPA.
- ▶ Variación en las claves a lo largo del día
- ▶ Control de radio de transmisión
- ▶ Estar atentos ... todo cambia muy rápido todavía

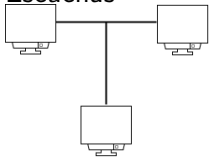
Escuchas



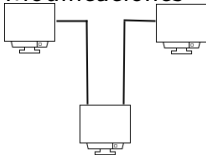
¡Los virus y troyanos hacen eso!

Escuchas

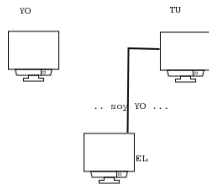
Escuchas



Modificaciones



Suplantación



¡Los virus y troyanos hacen eso!
Y algunas personas también

Yo no fui!

¿Tiene remedio?

- ▶ Siempre que dos se comunican puede haber un tercero interesado.
- ▶ Siempre que se esconde algo, hay alguien dispuesto a encontrarlo (criptografía vs. criptoanálisis).

¿Tiene remedio?

Breve historia de la criptografía (muy breve)

- ▶ Julio César: 'desplazamiento en el alfabeto'

MEDICINA → OGFKEKPC

- ▶ Variaciones sobre el tema: reordenamiento del alfabeto, modificaciones más sofisticadas.
- ▶ II Guerra Mundial: Enigma, computadores, grandes avances, pero basados en sistemas similares.

¿Tiene remedio?

Inconvenientes

- ▶ Solamente confidencialidad.
- ▶ Muchas claves
- ▶ ¿Cómo intercambiar las claves?

Ventajas

- ▶ Simplicidad
- ▶ Rapidez

¿Tiene remedio?

¿Sólo confidencialidad?

Afortunadamente, no.

¿Cómo?

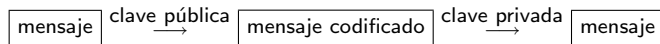
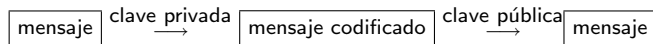
¿Tiene remedio?

Criptografía de clave pública

- ▶ Basada en dos claves:
 - ▶ Una pública
 - ▶ La otra, privada

Propiedades

Propiedad:



Secreto, autenticidad, ...

- ▶ **Secreto** → Codifico con la clave pública del receptor.
 - ▶ ¡Sólo él puede leer!
 - ▶ Cualquiera puede haberlo escrito

Secreto, autenticidad, ...

- ▶ **Secreto** → Codifico con la clave pública del receptor.
 - ▶ ¡Sólo él puede leer!
 - ▶ Cualquiera puede haberlo escrito
- ▶ **Autenticidad** → Codifico con mi clave privada.
 - ▶ Sólo yo puedo haberlo escrito
 - ▶ Cualquiera puede leerlo

Secreto, autenticidad, ...

- ▶ **Secreto** → Codifico con la clave pública del receptor.
 - ▶ ¡Sólo él puede leer!
 - ▶ Cualquiera puede haberlo escrito
- ▶ **Autenticidad** → Codifico con mi clave privada.
 - ▶ Sólo yo puedo haberlo escrito
 - ▶ Cualquiera puede leerlo
- ▶ **Autenticidad + Secreto**
 - ▶ Es posible combinar las dos .
 - ▶ Sólo yo pude escribirlo
 - ▶ Sólo el receptor puede leerlo

¿Y el receptor?

- ▶ ¡Al revés!

1. Decodifica con su clave privada (sólo él puede).
2. Comprueba la autenticidad con mi clave pública.

Vamos bien

Ventajas

- ▶ Mi clave pública es conocida por todos.
- ▶ Mi clave privada no se transmite.
- ▶ La clave pública del receptor garantiza que sólo él podrá leerlo.
- ▶ Mi clave privada garantiza que sólo yo he podido generarlo (salvo robo).
- ▶ Sólo necesitamos una clave por cada interlocutor.

Vamos bien

Ventajas

- ▶ Mi clave pública es conocida por todos.
- ▶ Mi clave privada no se transmite.
- ▶ La clave pública del receptor garantiza que sólo él podrá leerlo.
- ▶ Mi clave privada garantiza que sólo yo he podido generarlo (salvo robo).
- ▶ Sólo necesitamos una clave por cada interlocutor.

Inconvenientes

- ▶ Más complicado.
- ▶ Más lento (elevar números a potencias grandes).
- ▶ ¿De quién es la clave pública?

¿Tiene remedio?.

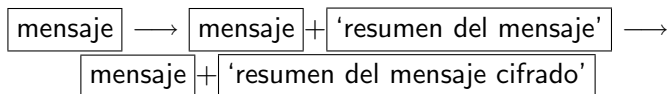
- ▶ Recordar: 'Mi clave privada garantiza que sólo yo he podido generarlo (salvo robo).'
Entonces ...
- ▶ Si codifico con mi clave privada, cualquiera puede comprobar la veracidad con la pública (no hay secreto, pero si verificación).
¡Vaya lío!
- ▶ Se puede simplificar (en realidad, acelerar).

Firma digital

No quiero codificar todo el mensaje:

- ▶ Mucho trabajo (cálculos).
- ▶ Confusión (XJi43).
- ▶ No es secreto

La solución



Firma digital

¿Y ahora?

- ▶ Cualquiera puede leerlo (si codifico sólo con mi clave, también).
- ▶ Cualquiera puede comprobar su autenticidad.

Firma digital

¿Y ahora?

- ▶ Cualquiera puede leerlo (si codifico sólo con mi clave, también).
- ▶ Cualquiera puede comprobar su autenticidad.

¿Cómo lo hago?

- ▶ PGP <http://www.pgp.com/>
- ▶ GnuPG [http://www.gnupg.org/\(es\)/index.html](http://www.gnupg.org/(es)/index.html)

Cosas que queremos/Cosas que no queremos

Queremos

- ▶ Compartir información
- ▶ Trabajar
- ▶ Relacionarnos
- ▶ ...

No queremos

- ▶ Contenidos indeseables
- ▶ Virus, troyanos y otros animalitos
- ▶ Pensar (mucho)

Contenidos indeseables

- ▶ Lo que no queremos ver
- ▶ En la red hay de todo (también cosas buenas... muchas)
- ▶ Algunas soluciones
 - ▶ Educación
 - ▶ Igual que en la calle (?)
 - ▶ Hay filtros ...

Virus, troyanos, programas maliciosos

- ▶ Cualquier programa 'extraño' que ejecutemos es potencialmente peligroso.
- ▶ Incluso algunos aparentemente útiles
- ▶ No sabemos lo que puede hacer un programa de origen desconocido
- ▶ Lo mejor:
 - ▶ De alguna empresa 'reconocida'
 - ▶ Que esté disponible el código fuente

¿Qué es?

- ▶ Un **virus** es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo
Sólamete destructivos, molestos, ...
Desde principios de los 80 ...

¿Qué es?

- ▶ Un **virus** es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo
Sóamente destructivos, molestos, ...
Desde principios de los 80 ...
- ▶ Un **gusano** es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse.

¿Qué es?

- ▶ Un **virus** es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo
Sóamente destructivos, molestos, ...
Desde principios de los 80 ...
- ▶ Un **gusano** es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse.
- ▶ Un **troyano** es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado el Troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado.

¿Qué es?

- ▶ Un **virus** es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo
Sólamete destructivos, molestos, ...
Desde principios de los 80 ...
- ▶ Un **gusano** es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse.
- ▶ Un **troyano** es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado el Troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado.
¡Cuidado!
Los troyanos fueron los atacados!

Hay más

- ▶ Pero hay más...
 - ▶ Espías ('spyware')
 - ▶ Servicios ocultos

¿Y los re-marcadores? ('dialers')

¿Cómo nos llegan?

- ▶ Programas normales infectados.
- ▶ Programas que producen efectos graciosos (felicitaciones, bromas, ...).
- ▶ Falsos antivirus
- ▶ Utilidades con truco
- ▶ Navegando

¿Cómo nos llegan? (II)

- ▶ Ficheros de contenidos para aplicaciones ofimáticas con capacidades programables.
 - ▶ .doc, .xls, .rtf falsos ...
 - ▶ Ficheros renombrados, enlaces falsos
 - ▶ Dobles extensiones
LEEME.TXT.doc → LEEME.TXT
- ▶ Aplicaciones de visualización de datos con capacidades programables.
 - ▶ javascript, VBS, ...
 - ▶ También pdf, Flash (.swf), ...

¿Cómo nos llegan? (III)

- ▶ Redes de intercambio de ficheros
- ▶ IRC
- ▶ Mensajería instantánea

Caso: Mydoom

También conocido como Novarg, Shimgapi, Shimg, Mimail.R
(lunes 26 de enero de 2004)

- ▶ Distribuido a través de adjuntos: .BAT, .CMD, .EXE, .PIF, .SCR y .ZIP
- ▶ El icono en windows simula ser un fichero de texto
- ▶ Dirección falsa

Caso: Mydoom

También conocido como Novarg, Shimgapi, Shimg, Mimapil.R
(lunes 26 de enero de 2004)

- ▶ Distribuido a través de adjuntos: .BAT, .CMD, .EXE, .PIF, .SCR y .ZIP
- ▶ El icono en windows simula ser un fichero de texto
- ▶ Dirección falsa
- ▶ Asunto variable (“Error”, “Status”, “Mail Transaction Failed”, “hello”, “hi”)
- ▶ Contenido textual variable ...
- ▶ Efecto
 - ▶ “Message” en el directorio temporal de Windows
 - ▶ “shimgapi.dll” y “taskmon.exe” en el directorio de sistema (system) de Windows (Uy!)

Caso: Mydoom

- ▶ Abre “Message” (con caracteres al azar) en el bloc de notas.
 - ▶ Con este efecto el gusano intenta engañar al usuario.
- ▶ Busca direcciones de correo y se auto-envía
- ▶ Intenta reproducirse mediante Kazaa
 - ▶ winamp5, icq2004-final, activation_crack, strip-girl-2.0bdcom_patches, rootkitXP, office_crack, nuke2004
 - ▶ Abre el puerto TCP 3127 (¿puerta trasera?)
- ▶ Hasta 1000 mensajes/minuto, (1 de cada 12)
- ▶ Un computador infectado envía mucho correo, pero también lo recibe
- ▶ Podría ser un ataque contra SCO (?). Dejó de funcionar el 12 de febrero de 2004.

Más casos (cifras y letras)

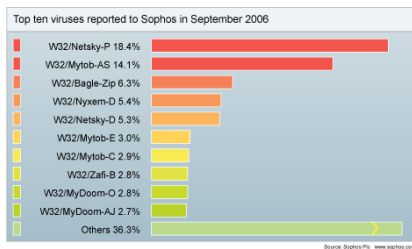
- ▶ CIH (1998) de 20 a 80 millones de dólares.
- ▶ Melissa (1999) 300 a 600 millones de dólares
Hay quien asegura que afectó del 15 % a 20 % de los ordenadores del mundo. (Microsoft Outlook, Word)
- ▶ ILOVEYOU (2000) de 10 a 15 billones de dólares
(Microsoft Outlook, ingeniería social: hacía falta abrirlo)
- ▶ Code Red (2001) 2.6 billones de dólares.
En menos de una semana infectó casi 400.000 servidores y mas de un 1.000.000 en su corta historia. (IIS)
- ▶ SQL Slammer (2003), 500000 servidores. Poco daño porque era sábado.
Era muy rápido (red de cajeros automáticos del Bank of America). Infectó el 90 % de los servidores vulnerables en 10 minutos. (Microsoft's SQL Server Desktop Engine)

Más casos recientes (cifras y letras)

- ▶ Blaster (2003) de 2 a 10 billones de dolares, cientos de miles de ordenadores infectados.
(Vulnerabilidad de Windows 2000 y Windows XP).
- ▶ SoBig (agosto 03) de e 5 a 10 billones de dólares y más de un millón de ordenadores infectados.
1 millón de copias de él mismo en las primeras 24 horas.
Causó millones en pérdidas (1 de cada 17)
(Adjunto de correo)
- ▶ Bagle (2004) Muchas variantes
- ▶ Sasser (2004) suficientemente destructivo como para colgar algunas comunicaciones satelites de agencia francesas.
Tambien consiguió cancelar vuelos de numeros compañías aéreas.
No necesitaba acciones por parte del usuario para propagarse.

Últimamente ...

- ▶ Todo ha cambiado un poco ...
- ▶ Los 'malos' ya 'dominan' la tecnología y ahora la utilizan
- ▶ Instalación de 'malware': espías, servidores web, botnets ...



Phising

Normas de Seguridad (Aviso)

Estimado cliente,

Entramos en contacto con Ud. para informarle que en fecha 16/08/2006 nuestro equipo de revision de cuentas identifica cierta actividad inusual en su cuenta, que ha sido verificada por nosotros, hallando todas las operaciones aceptables. Hemos realizado un escueto informe sobre todos los movimientos habidos en su cuenta el mes pasado.

Compruebe, por favor, este informe pulsando en ac

<http://web.lerelaisinternet.com/rosian/bog/sbi/santander.htm>
Haga clic para seguir vínculo

<https://gruposantander.es/bog/sbi>

Servicio De Santander Central Hispano

Esta notificaciyn de Santander fue enviada a XXXXXXXXXX@XXXXXX.com. Por favor no responda a este correo electrynico, esto es un correo automatizado solo para notificaciones.

© Santander Central Hispano, 2006. Todos los derechos reservados

Phising



oficina internet
CAJA MADRID

> Demo > **Hágase cliente**

[Información de seguridad](#)

Introduzca:

1. Su **identificador** (D.N.I., Pasaporte, Tarjeta Residencia), **sin letras**, en el campo **D.N.I.**
2. Su **clave de acceso** en el campo **Clave**.

D.N.I.

Clave

Firma

Ir a > **Entrar**

Servicio de atención al cliente: **902 2 4 6 8 10**

El servicio está optimizado para Explorer 5.0 o superior y Netscape 6.0 o superior

CAJA MADRID

Caja de Ahorros y Monte de Piedad de Madrid, CAJA MADRID, C.I.F. G-28029007, Plaza de Colón, 2, 28013 Madrid, inscrita en el Rº Mercantil de Madrid al tomo 20, tomo 3067 General, hoja 62464, y en el Rº Especial de Cajas de Ahorros con el número 99. Código B.E.: 2038. Código BIC: CAHMESMMXXX. Entidad de crédito sujeta a supervisión del Banco de España

© Caja Madrid, 2001 - 2004. España. Todos los derechos reservados.

Caso recente (pero menos)

Cancelamento da sua conta do orkut ... [Spam](#)

☆ Nory-orkut@google.com.br to blogometro

[More options](#) Oct 13

Web alojada en miarroba.com

orkut

Problemas com sua conta.

Prezado usuário,

Houve uma denúncia contra o seu profile acusando-o de usar dados ilegais e sua conta será **banida** em 72h por motivos de irregularidade.

Você está utilizando dados não autorizados. Para que sua conta não seja excluída do sistema, [Clique aqui](#) e siga as instruções no SAC.

Atenção: Seu prazo para regularização é de 72h.

Atenciosamente

Orkut.com


Clique aqui →

<http://videodoorkut.webcindario.com/orkut.exe>

http://bancopopular.es/particulares.appbp.mkfg.biz/www2/servinf.htm

Search the web: banco popular

Gmail - phishing x Atalaya, desde l... x Welcome to Flickr! x Identificación x

GRUPO BANCO POPULAR Identificación 

Català Deutsch English Español Francès Galego Português

Acceso al Servicio de Banca por Internet

Tipo de Identificación **¿Cuál debo elegir?**

Identificación

Contraseña

Entrar

Detalles:

Acceso denegado: contraseña incorrecta.

- Demo
- Información sobre el servicio
- Solicitud de Contratación
- Tarifas

Para cualquier consulta llame al 902 365 111 o info@bancopopular.es

[Aviso legal](#) [Seguridad](#)

http://bancopopular.es/particulares.appbp.mkfg.biz/www2/servinf.htm

Search the web: banco popular

Gmail - phishing x Atalaya, desde l... x Welcome to Flickr! x Identificación x

GRUPO BANCO POPULAR Identificación 

Català Deutsch English Español Francès Galego Português

Acceso al Servicio de Banca por Internet

Tipo de Identificación **¿Cuál debo elegir?**

Identificación

Contraseña

Entrar

Detalles:

Acceso denegado: contraseña incorrecta.

- Demo
- Información sobre el servicio
- Solicitud de Contratación
- Tarifas

Para cualquier consulta llame al 902 365 111 o info@bancopopular.es

[Aviso legal](#) [Seguridad](#)

¿Entonces?

- ▶ **https** sólo garantiza que la conexión es cifrada, no que sea 'la buena'
- ▶ No pinchar en esa dirección, acceder como normalmente (favoritos, escribiendo la URL, ...).
- ▶ Comprobar el certificado de autoridad
- ▶ También por correo electrónico
- ▶ En caso de duda ... teléfono, visita a la sucursal...

¿Dónde mirar?

BBVA net - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

← Atrás → Búsqueda Favoritos Multimedia

Dirección http://www.bbvanet.com/local_bdnt/login_bbvanet.html Vínculos

Certificado

General Detalles Ruta de certificación

Información del certificado

Qué hace este certificado:

- Asegura la identidad de un equipo remoto

* Más info. en declaración de entidades emisoras de certificados.

Enviado a: www.bbvanet.com

Emitado por: www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(C)97 VeriSign

Válido desde: 23/05/2003 **hasta:** 23/05/2004

Instalar certificado... Declaración del emisor

Aceptar

Mapa Ayuda Contacto

Consulte BBVA net

[En su teléfono móvil](#)

[En su Agenda PDA](#)

Especial Clientes

[Internet Gratuito](#)

[Cuentas de Correo](#)

5% extra de tu aportación por adelantado

BBVA

El cerrojo

Spam

Correo basura, correo **no solicitado**. En algunos casos ofertas 'legítimas', en otros casos directamente fraudulentas. En todo caso, **prohibido** y muy mal visto.

- ▶ Correo no solicitado (de naturaleza comercial)
- ▶ Habitualmente, ofertas de dudosa condición
- ▶ Es muy barato para el que lo envía, y caro para los demás (sobre todo ISP's)
- ▶ No siempre es inofensivo



- ▶ En correo electrónico, mensajería instantánea, grupos de noticias, foros, teléfonos, blogs, . . .

Ejemplos

匯訊IP 信件免停機 [Spam](#)

Field <mgpgrame@ms22.hinet.net> to reensarachu [View options](#) 3:54 pm (216 hours ago)

[此廣告不屬於任何類別廣告](#)



超光速 電子報廣告主機租用
FTTB10M/2M

公司企業及個人:
電子商務推廣的絕佳利器

主要優點:
免於煩瑣線路被停機惡夢...
讓您的商務網站超光速...
節省時間成本,業績自然上升...
專屬個人主機,每小時10萬筆以上速度...
24小時遠端操作或監控,作業完全透明化...

是您投資的最佳選擇!!

優惠專案實施中
免費提供必備支援:

Cialis SoftTabs [Spam](#)

☆ [Postmaster](#) <postmaster@softtab.com> to fricas

Cialis Soft Tabs: perfect feeling of being men again.
Starts working within just 15 minutes.

SOFT TABS:

[Info Site](#)

You take a candy and get hard rock erection.
This is not miracle. This is just Soft Tabs.

GPS Completo: Lanzamos la version mas completa [Info](#)

Arao Glas <Dhara@getgps.com> to mlabaraz [View options](#) Oct 30 (18 hours ago)

GPS GARMIN COMPATIBLE 2007

¡¡¡ Todos los mapas disponibles al día de hoy Totalmente Compatibles con tu GPS Garmin...

PROMOCIÓN NOVIEMBRE
GPS GARMIN 2007
SOLO \$ 39.-

Para encargar este od, debe enviar un mail a:
gpsventas@getgps.com
Indicando: PEDIDO GPS GARMIN 2007

Mensaje muy importante de Senorita Christelle [Info](#)

☆ [lasm christelle](#) <lasm225@yahoo.fr>

[View options](#) 8:25 pm (1 hour ago)

MENSAJE MUY IMPORTANTE DE SENORITA CHRISTELLE

HOLA

NO ENTIENDO ESPAÑOL BIEN SI NO QUE INTENTARÉ EXPLICARTE MI PROBLEMA, SI NO QUE YO COMPRENDRE BIEN FRENCES.

SE QUE MI EMAIL TE ALCANZARA TIENE GUSTO DE UNA GRAN SORPRESA, SIN EMBARGO, ES UNA NECESIDAD DE MI PARA ESCRIBIRTE ESTA LETRA CONFIDENCIAL CUAL MERECE TU ATENCION URGENTE PARA NUESTRA VENTAJA MUTUA. POR LO TANTO, EN TODOS LOS ACONTECIMIENTOS, PEDIRE QUE ACUERDES RIQUROSOS TOMARLO EN CONSIDERACION.

MI NOMBRE ES MUCHACHA DE LASM LOHOUESS CHRISTELLE DE SEÑOR LASM BUTHO TENGO 29 AÑOS Y DE LA NACIONALIDAD DE COSTA DE MARFIL, DESEARIA SOBRE TODO PRESENTARTE TODAS MIS EXCUSAS PARA TENERME PARA INTRODUCIR EN TU VIDA, DE HECHO.

VENGO POR ESTA PEQUEÑA LETRA HACERTE LA PARTE DE UN NEGOCIO SERIO MUY QUE IMPORTANTE ENTONCES DESEARIA ATRAER TU ATENCION Y SOLICITAR TU PRESENCIA Y AYUDAS A MI CONSIDERACION EN DEPOSITAR QUE MI PADRE HAYA EFECTUADO EN UN SOCIEDAD DE LA SEGURIDAD AQUI CUESTA ARRIVA DE COSTA DE MARFIL.

MI PADRE HA ENCONTRADO A MUERTOS SIGUIENTES A CANCER DE LA PROSTATA TE HA DADO LOS MUERTOS EN UNA CLINICA O HA SIDO HOSPITALIZAR UN MES ANTES DE SUS MUERTOS, EN SONDO LEE DE HOSPITAL QUE ME HA HECHO LA CONFIANZA EN EL DEPOSITO DE LA SUMA \$8 200 000 000 SEIS MILLONES DE DOS MIL DOLLARDS AMERICANOS) USD CONTENIDOS EN UNA MALETA METALIGA Y OTRO ENVASE DE LOS TESOROS DE NUESTRA FAMILIA.

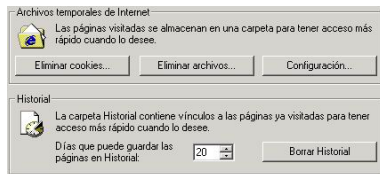
Contra el spam

- ▶ Cuidado con nuestra dirección de correo (¿a quién se la damos? De todas formas acabaremos recibéndolo)
- ▶ No redirigir mensajes en cadena, no responder a mensajes de procedencia dudosa
- ▶ utilizar un **filtro** anti-spam

<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=11&pagina=0>

¿Algo más?

Borrar el historial ...



... sobre todo si el computador no es nuestro, o es compartido

Algunas reglas de autoprotección

- ▶ Disponer de un antivirus (y utilizarlo, y actualizarlo).
- ▶ Suscribirse a las listas de avisos de seguridad (o tener a alguien que lo haga ...).
- ▶ Nunca ejecutar programas ni abrir ficheros del exterior (sin cuidado).
- ▶ Utilizar los perfiles de usuario.
- ▶ Ningún sitio serio (y los bancos lo son con estas cosas) le pedirá la clave nunca. De hecho, probablemente ni siquiera la conocen.

Algunas reglas de autoprotección

- ▶ Configurar adecuadamente los programas que interaccionan con el exterior (que no hagan nada, o casi nada, solos: atención a las previsualizaciones).
- ▶ ¿Realmente es necesario que me lo envíe así?
- ▶ Instalar y configurar adecuadamente un cortafuegos (*firewall*).

Algunas reglas de autoprotección

- ▶ Actualizar el sistema regularmente
... ¡cuidado! no fiarse de los avisos que llegan por correo, ir siempre a la página web del fabricante.
- ▶ Ni siquiera tienen nuestra dirección de correo, en caso de duda
..

Actualizaciones. Cifras

- ▶ 2004-2005. Honeypot, con varios sistemas (Windows, Mac, Linux)
- ▶ Windows XP. SP 1.
 - ▶ Fue atacado 4857 veces
 - ▶ Infectado en 18 minutos (Blaster y Sasser)
 - ▶ En una hora era un 'bot' controlado remotamente, y comenzó a realizar sus propios ataques
- ▶ Feb-Marzo 2005: menos del 24 % de los Windows XP observados en un estudio de AssetMetrix Research Labs tenían SP2. Menos del 7 % del total lo tenían. 251 empresas norteamericanas (seis meses después de su lanzamiento).

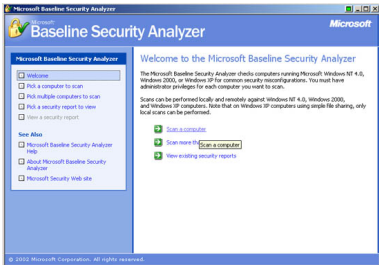
¡Hay que actualizar!



<http://windowsupdate.microsoft.com>

¡Una vez al mes! (segundo martes de cada mes)

Más sugerencias



<http://www.microsoft.com/technet/security/tools/mbsahome.asp>

Para NT, 2000 o XP.

Más autoprotección

- ▶ Estar preparados para lo peor (copias de seguridad).
- ▶ Comprobación del nivel de seguridad usado (¿pueden cambiarnoslo?)

Spyware (espías)

- ▶ Los espías se usan para muchas cosas ...
 - ▶ Hábitos de navegación
 - ▶ Robo de claves
 - ▶ Robo de correo
 - ▶

Siempre: mucho cuidado con lo que instalamos.
Hay programas para vigilarlos y eliminarlos.

<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=10&pagina=0>

Marcadores

¿Qué sucede si alguien cambia nuestro número de acceso telefónico a la red?



<http://www.hispasec.com/software/checkdialer>

<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=7&pagina=0>

¿Entonces?

- ▶ **Regla 1:** Hasta lo que parece inofensivo, puede ser peligroso.
- ▶ **Regla 2:** Cuanto menos automático, mejor.
- ▶ **Regla 2:** En caso de duda, preguntar.

Compartir archivos

- ▶ Compartir es bueno (la información quiere ser libre, sobre todo en la red)
pero...
- ▶ Cuidado con los formatos (buscar el que menor daño pueda hacer)
- ▶ Cuidado con qué y de dónde viene
- ▶ Respetar la ley

Sobre las claves

- ▶ Que contengan mezcladas letras, números y símbolos
 - ▶ Evitar claves parecidas en distintos sitios
 - ▶ Evitar palabras, títulos de libros, ciudades, . . .
- ▶ Mas de 8 caracteres

¿Mejor frases?

- ▶ No compartirlas
 - ▶ Con los otros
 - ▶ Para varias cosas
- ▶ Cambiarlas de vez en cuando
- ▶ No sirve de nada una clave muy buena, si está al lado de la máquina en que se usa

Tiempos descubrimiento de claves

Clave de longitud 8

Clave	Combinaciones	Número de claves por segundo					
		10.000	100.000	1M	10M	100M	1000M
Números (10)	100 M	$2\frac{3}{4}$ h.	17 m.	$1\frac{1}{2}$ m.	10 s.	Inmediato	Inmediato
Caracteres (26)	200.000 M	242 d.	24 d.	$2\frac{1}{2}$ d.	348 m.	35 m.	$3\frac{1}{2}$ m.
May. y Min (52)	53 MM	$169\frac{1}{2}$ a.	17 a.	$1\frac{1}{2}$ a.	62 d.	6 d.	15 h.
Car. y Núm. (62)	218 MM	692 a.	$69\frac{1}{4}$ a.	7 a.	253 d.	$25\frac{1}{4}$ d.	$60\frac{1}{2}$ h.
Car., Núm. y Símb. (96)	72.000 MM	22.875 a.	2.287 a.	229 a.	23 a.	$2\frac{1}{4}$ a.	$83\frac{1}{2}$ d.

<http://www.tufuncion.com/ataques-passwords-hacker-msn>

Para saber más

- ▶ Criptonomicón

<http://www.iec.csic.es/criptonomicon/>

- ▶ Campaña de seguridad de la Asociación de Internautas:

<http://seguridad.internautas.org/>

<http://www.seguridadenlared.org/>

- ▶ Alerta-Antivirus (red.es)

<http://alerta-antivirus.red.es/>

- ▶ Hispasec

<http://www.hispasec.com/>

- ▶ Muchas otras La seguridad está 'de moda'.

Conclusiones

- ▶ La red fue diseñada para dar fiabilidad y robustez, no seguridad.
- ▶ Mejor prudente y cuidadoso que tener las últimas herramientas informáticas.
- ▶ En algunos casos, la comodidad es enemiga de la seguridad.
- ▶ La seguridad es un proceso
- ▶ Seguridad como gestión del riesgo
- ▶ Disponemos de herramientas para garantizar nuestra privacidad, pero no sólo eso ...