Seguridad y Privacidad en la Red

Octubre 2012

Andalucía lab

Ya hemos sido hackeados (*)…

¿ahora qué?

* Hackear: *vulnerar la seguridad informática.*

Imagen: Oak Ridge National Laboratory (07/04/2011)

- *“El único sistema seguro es aquél que está apagado, en el interior de un bloque de hormigón, protegido en una habitación sellada rodeada por guardias armados. Y aún así, no estoy del todo seguro.”*__ Eugene (Gene) Spafford.

- *“Pienso que los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva.“*__ Stephen Hawking.

Algunos datos para situarnos…

- 14 millones de nuevos códigos maliciosos entre Julio y Diciembre del 2011.
- Aproximadamente el 39,38% de los PC están infectados.
- USA con el 64,39% encabeza los países con web maliciosas.
- Mensualmente suceden entre 20.000 y 32.000 campañas de ataques únicos de phishing.
- Se crean mensualmente entre 32.000 y 48.000 webs fraudulentas.
- El sector financiero (42,4%) es el mas atacado.

Falsas creencias sobre seguridad.

- Si mi ordenador está infectado, notaré los síntomas.
- La mayoría de los virus llegan por correo electrónico.
- El ordenador no se puede infectar sólo con visitar una página web.
- La mayor parte de los virus se propagan a través de P2P y sitios torrent.
- En las páginas de pornografía hay mayor riesgo de toparse con malware que en cualquier otra.
- Los ordenadores de los usuarios no son de interés para los ciberdelincuentes.

…por consiguiente...

- No pensemos que lo sabemos todo sobre internet.

  La mejor manera de protegernos es conocer e identificar los riesgos.

Principales agentes de riesgo.

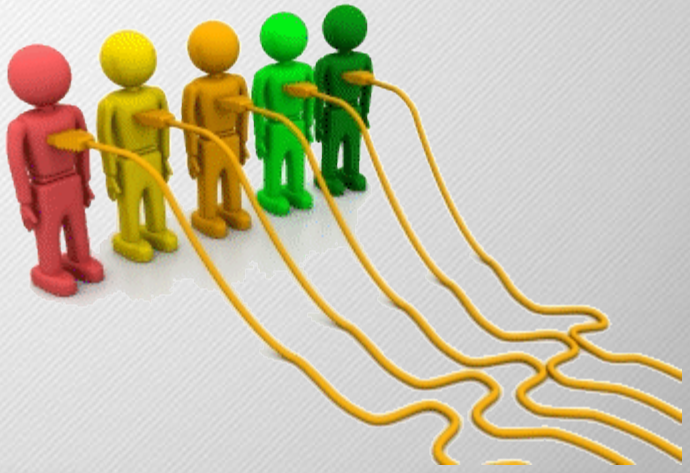
- Malware genérico (Troyanos, Rookits, Spyware, Backdoors, hijackers, etc.)
- Phishing , robo y suplantación de identidad.
- Ataques DDoS.
- Correos circulares. Hoax (bulos y leyendas urbanas)
- Herramientas de hacking.
- Popularización de redes sociales.
- Apps móviles maliciosas.
- Pérdida total o parcial de datos.

Malware genérico

Ingeniería Social como medio de fraude.

(No todo lo que leemos en internet tiene que ser cierto.)

- Los defraudadores aprovechan la credulidad en su beneficio.
- El engaño puede hacer que ejecutemos ficheros.
- Facilitar claves de acceso.
- Cualquier tipo de dato confidencial.



Phishing

Phishing

Es la estafa a través de medios telemáticos con la que se consigue información confidencial de usuarios legítimos. (contraseñas, datos bancarios, tarjetas de crédito, etc.)

- El robo de contraseñas y/o identidades, tiene una larga tradición en internet.

Ejemplo de phishing iniciales en AOL:

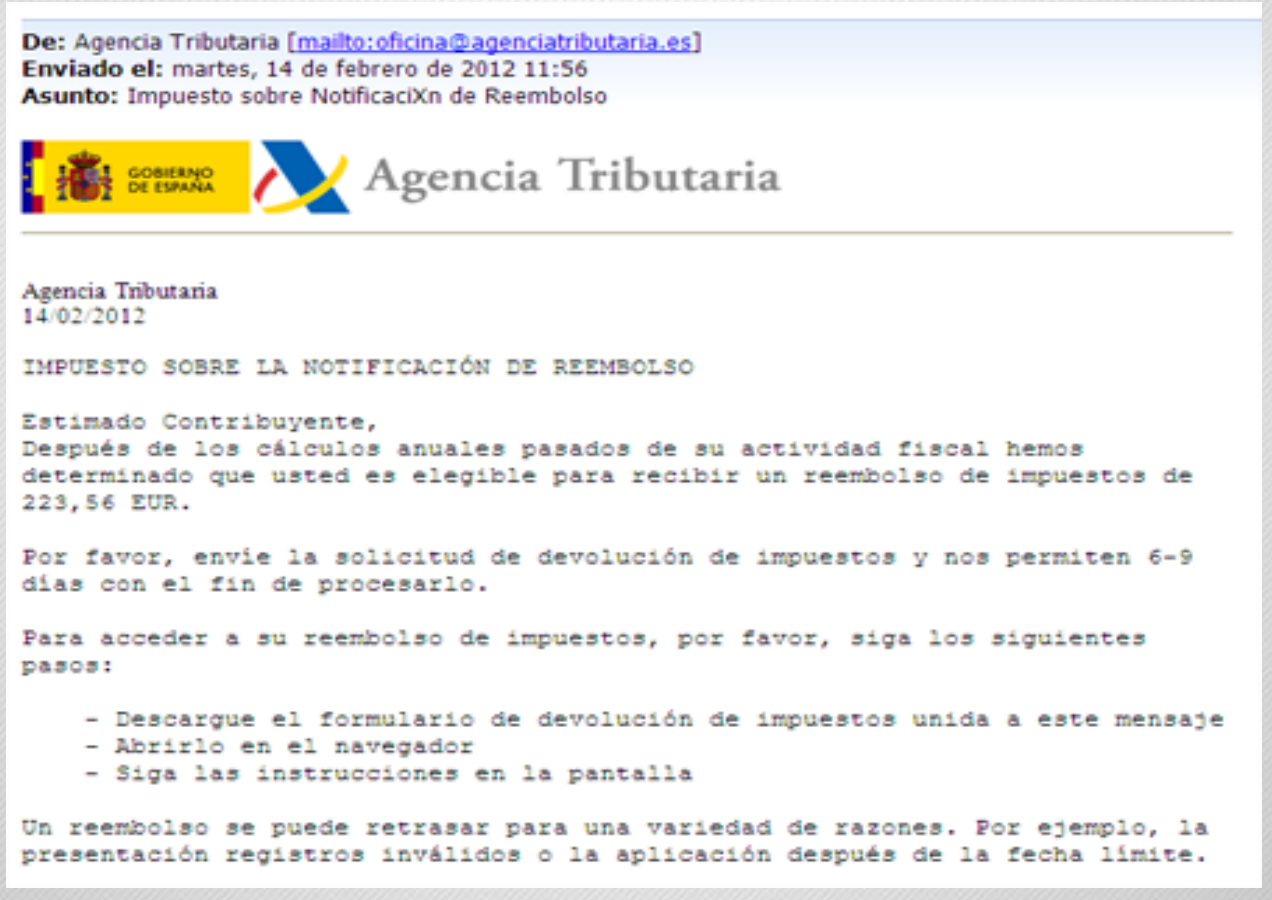
Sector 4G9E of our data base has lost all I/O functions. When your account logged onto our system, we were temporarily able to verify it asa registered user. Approximately 94 seconds ago, your verificationwas made void by loss of data in the Sector 4G9E. Now, due to AOL verification protocol, it is mandatory for us to re-verify you. Please click 'Respond' and re-state your password. Failure to comply will result in immediate account deletion.

…Phishing

- La estrategia preferida es el envío de correos masivos, enmascarándose en marcas de confianza.
- Al enmascaramiento de páginas se suma la utilización creciente de acortadores URL.
- Suplantanción de instituciones públicas. (Policía, Hacienda, Correos, etc.).
- Cartas nigerianas.
- Premios de lotería.
- Muleros y falsas ofertas de trabajo.

…Phishing

Oleada de correos de la Agencia Tributaria (febrero 2012)



De: Agencia Tributaria [mailto:oficina@agenciatributaria.es]
Enviado el: martes, 14 de febrero de 2012 11:56
Asunto: Impuesto sobre NotificaciXn de Reembolso

GOBIERNO DE ESPAÑA Agencia Tributaria

Agencia Tributaria
14/02/2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

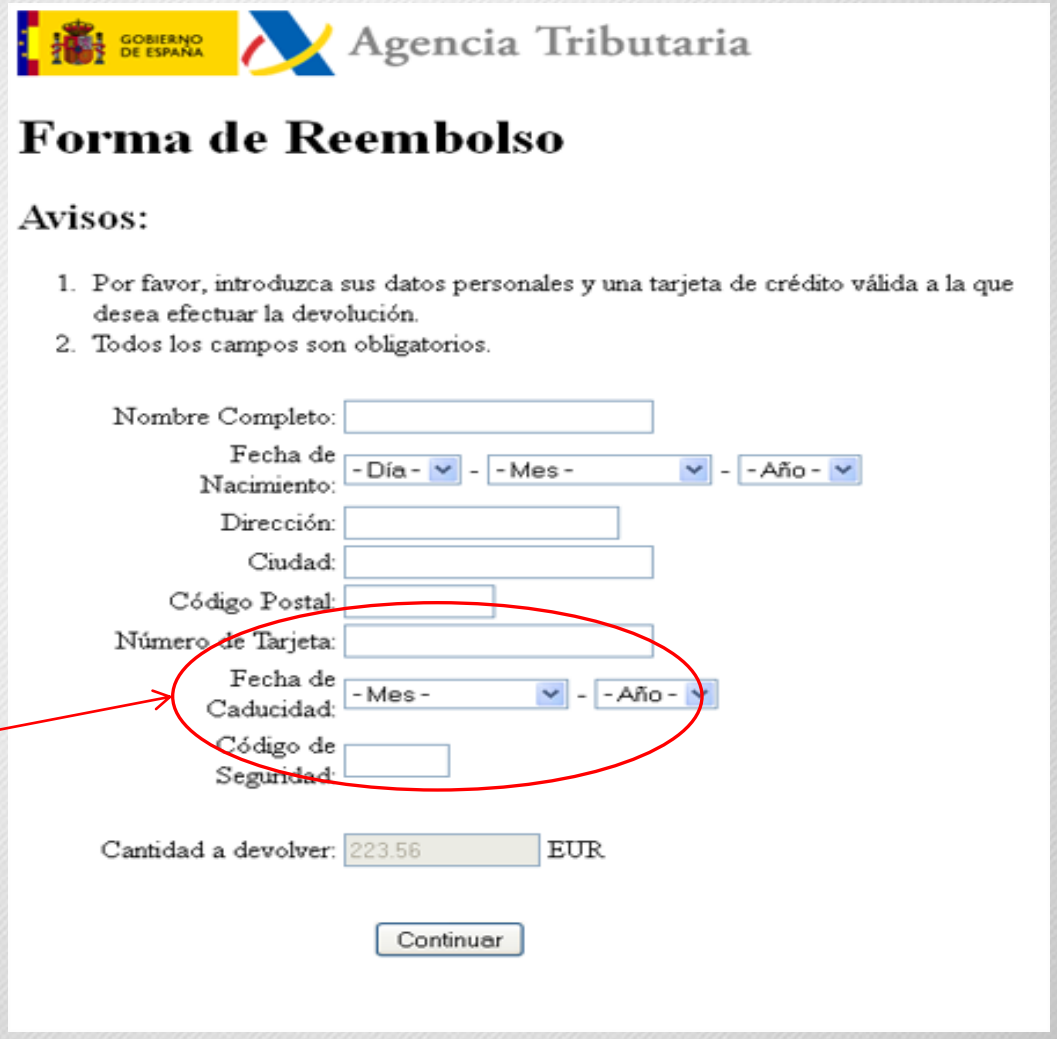
Por favor, envie la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.

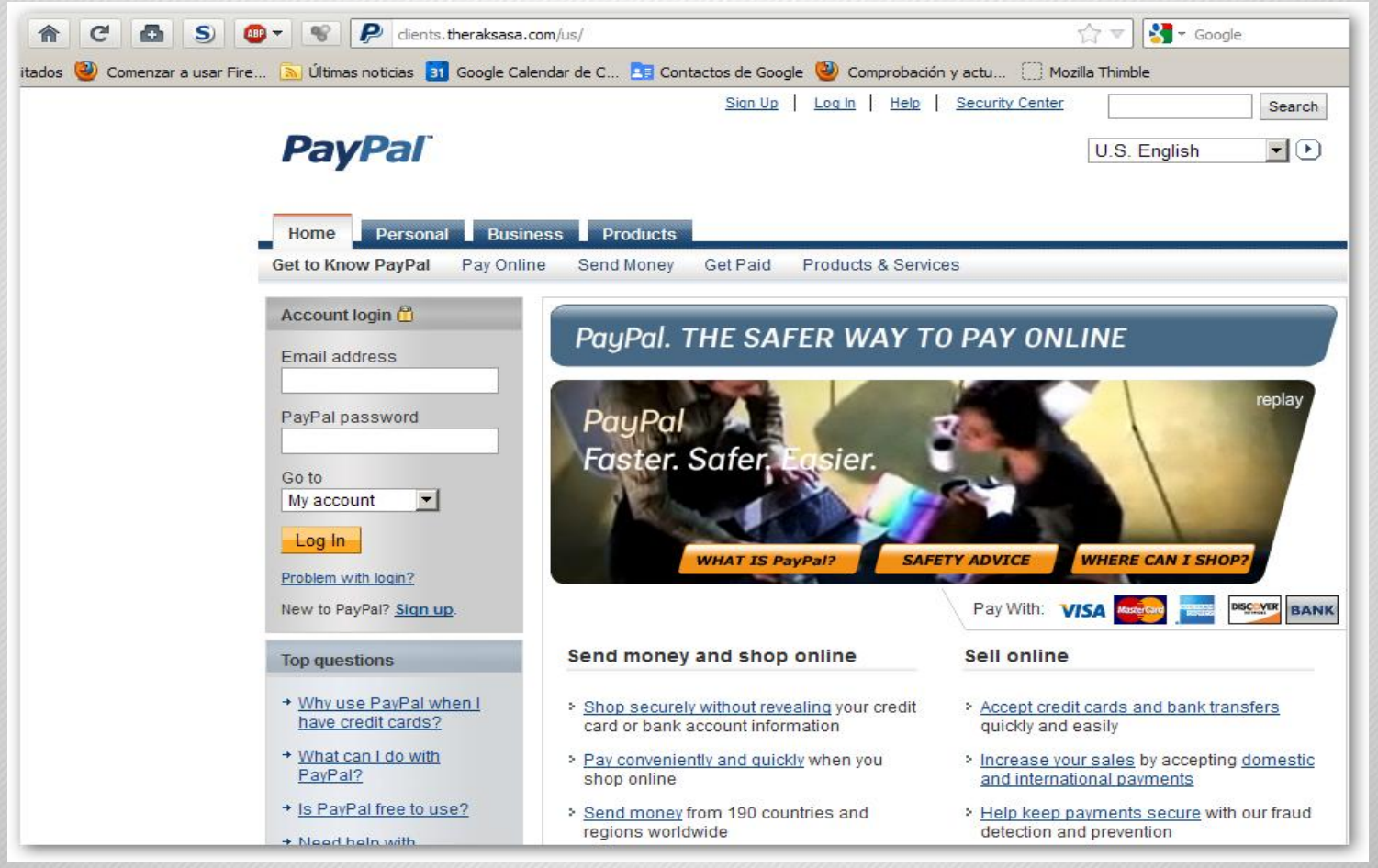
…Phishing



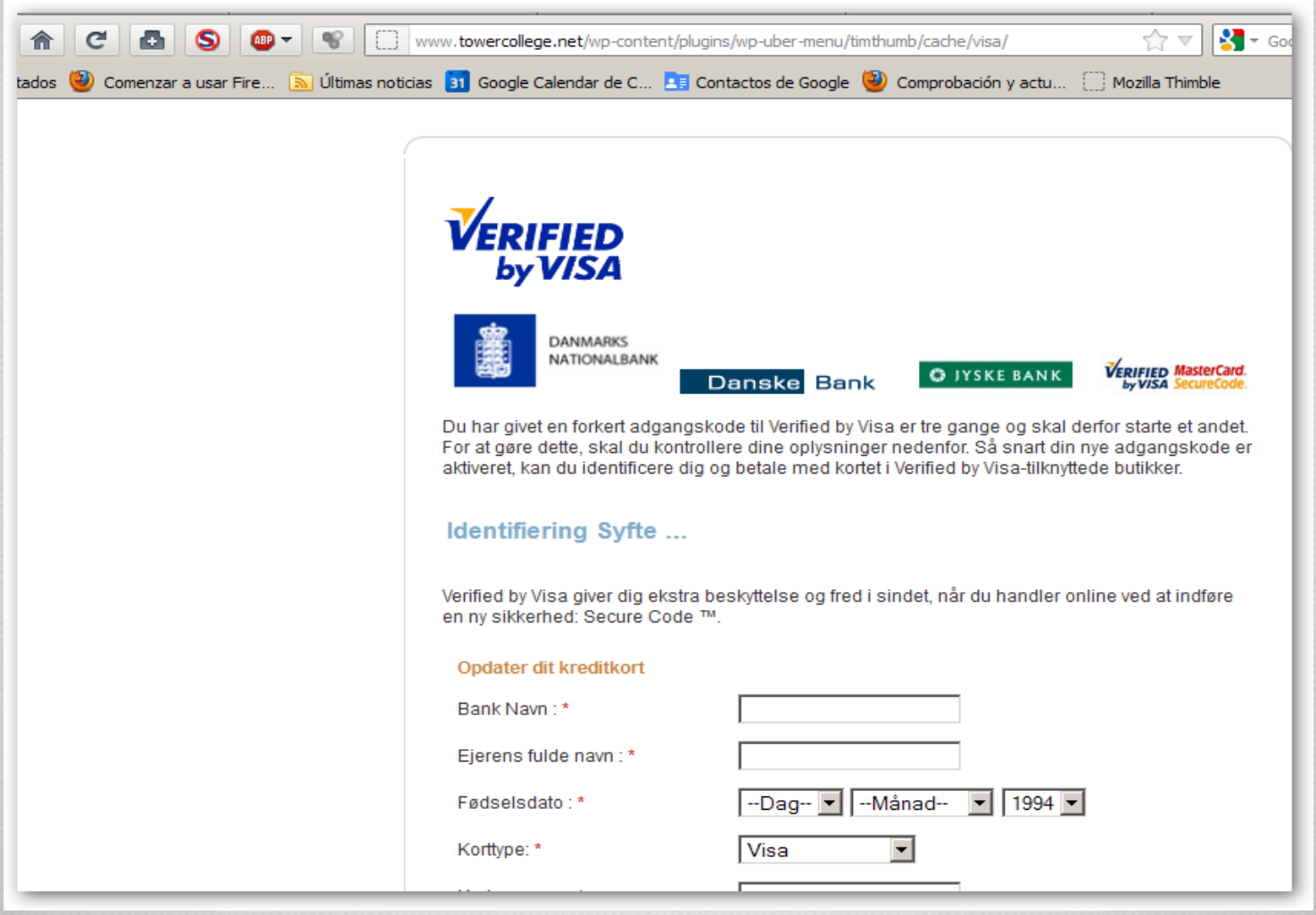
¡¡ solicita entre otros datos, el nº de tarjeta, caducidad y PIN !!

…Phishing

Falsa página activa el 29/09/2012 (fuente: www.phishtank.com)



…Phishing

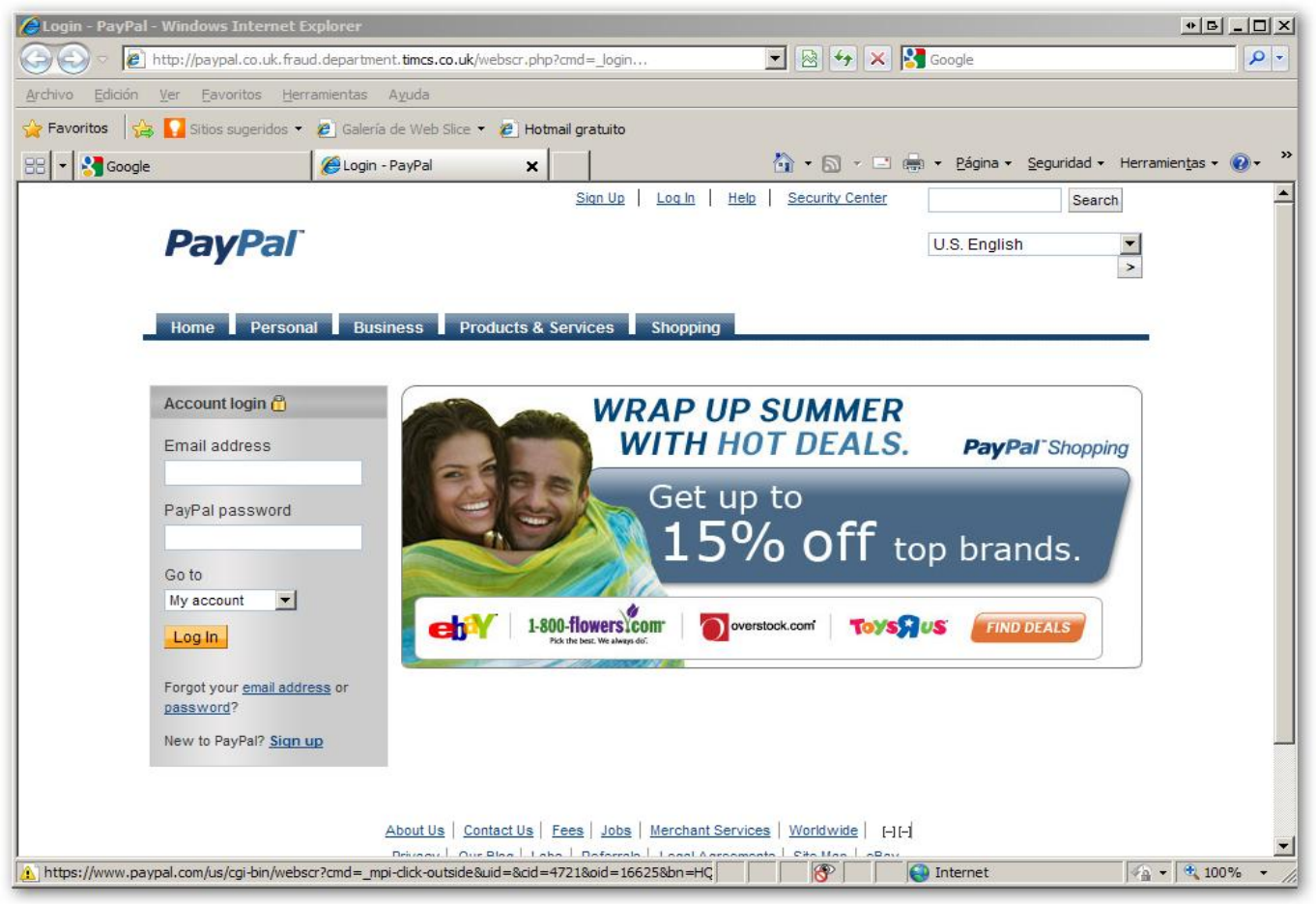

www.towercollege.net/wp-content/plugins/wp-uber-menu/timthumb/cache/visa/
tados
Comenzar a usar Fire...
Últimas noticias
Google Calendar de C...
Contactos de Google
Comprobación y actu...
Mozilla Thimble
VERIFIED by VISA
DANMARKS NATIONALBANK
Danske Bank
JYSKE BANK
VERIFIED by VISA MasterCard SecureCode.
Du har givet en forkert adgangskode til Verified by Visa er tre gange og skal derfor starte et andet. For at gøre dette, skal du kontrollere dine oplysninger nedenfor. Så snart din nye adgangskode er aktiveret, kan du identificere dig og betale med kortet i Verified by Visa-tilknyttede butikker.
Identifiering Syfte ...
Verified by Visa giver dig ekstra beskyttelse og fred i sindet, når du handler online ved at indføre en ny sikkerhed: Secure Code ™.
Opdater dit kreditkort
Bank Navn : *
Ejerens fulde navn : *
Fødselsdato : *
--Dag--
--Månad--
1994
Korttype: *
Visa

…Phishing

ejemplo de intento de phishing bloqueado por el navegador (Firefox)…

…Phishing

la misma página en el navegador Internet Explorer…



…otros tipos de Phishing

- Las “cartas nigerianas” son correos que ofrecen grandes sumas de dinero, previo pago de un anticipo.

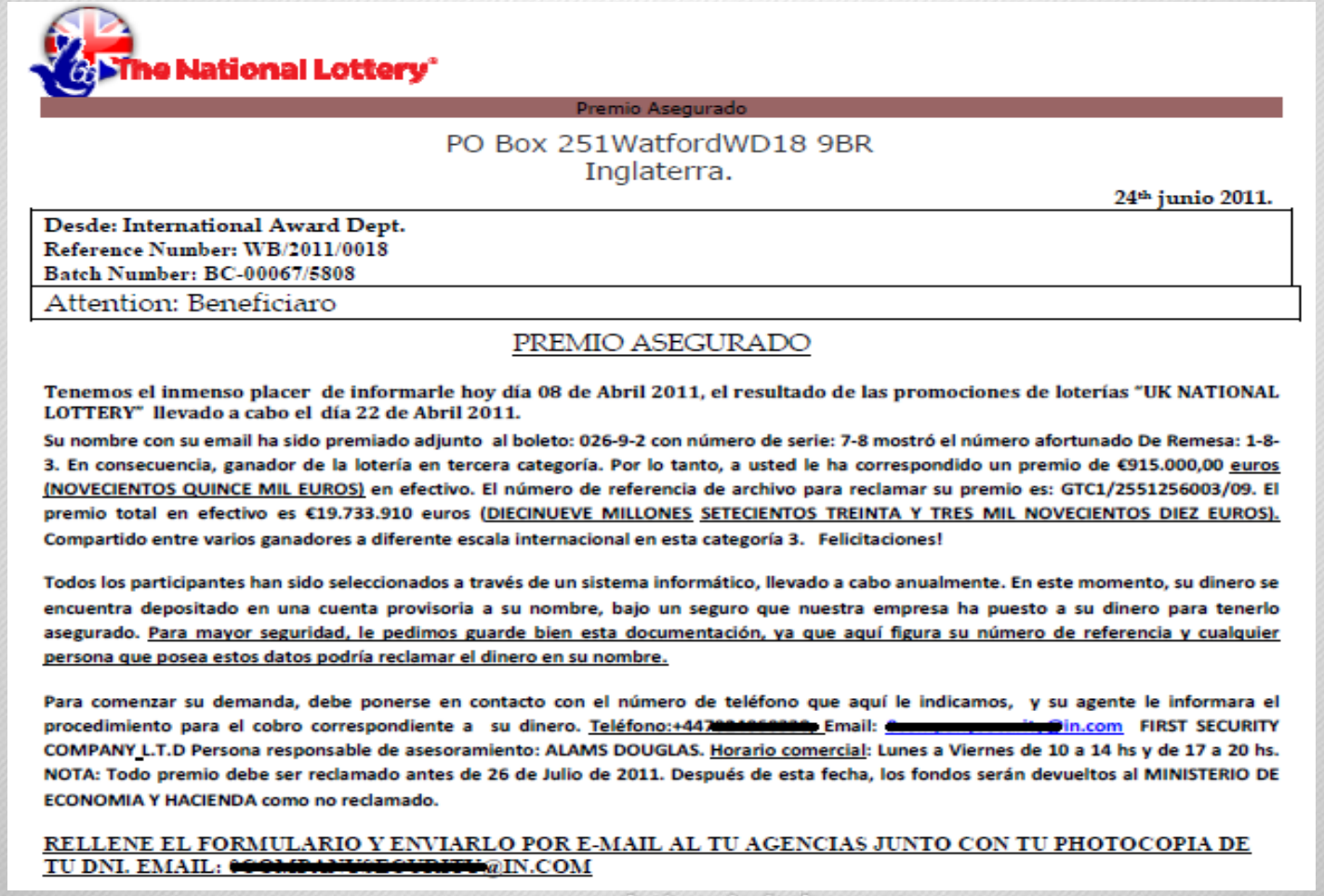
Estimado amigo,

Soy Emmanuel Egobiawa, un abogado en derecho y abogado personal para fines Ingeniero S. García, que murió con su esposa y su único hijo en un accidente de coche espantoso en el día 13 de diciembre de 2008, que utilizan para trabajar en la Compañía de Desarrollo de Shell y También era un contratista del gobierno aquí en Lomé. Deseo llamar su atención para informarle que Engr tarde. S. García antes de su muerte dejó a la suma de dieciocho millones de dólares (EE.UU. $ 18,000.000, 00) sólo en su cuenta bancaria que quiero poner en su atención ahora. Él murió sin dejar ninguno de sus familiares la información a mí oa cualquier otra persona y tengo mis mejores tratar de localizar a sus parientes o familiares, incluso en la embajada de su país, pero sin ningún éxito. Ahora bien, como su abogado personal y por la ley y el orden, el banco me pedirá que proporcione a sus familiares o parientes más cercanos a este hombre para que el fondo / el dinero se traslado a su familia que no tienen.

Ahora ya no tiene ningún miembro de la familia o parientes como (familiares hermano, hermana, tío o familiar), y tener / respuesta el mismo apellido (García) con él, quiero y han decidido a presentar al banco como uno de sus miembros de la familia o pariente más cercano a él por lo tanto ponerse en contacto con usted para que el banco va a transferir este dinero / fondos en su cuenta. Después de recibir este fondo / dinero en su cuenta en su país, voy a venir a su país a efectos de compartir y de la inversión porque parte de este fondo / el dinero se debe utilizar para la Fundación del Orfanato y otras inversiones como la construcción de una buena Estate en su país que se nos está dando otro fondo adicional / dinero. Pero esto no se puede lograr sin un socio extranjero como a ayudar a mí llevar a cabo esta operación, y que es por eso que estoy en contacto con usted hoy en día para que me ayude en este tema. Tengo los documentos necesario para que nos ayude en la toma de este éxito.

…otros tipos de Phishing

- Premios de lotería (¡a la que nunca se ha jugado!)



The National Lottery

Premio Asegurado

PO Box 251WatfordWD18 9BR
Inglaterra.

24th junio 2011.

Desde: International Award Dept.
Reference Number: WB/2011/0018
Batch Number: BC-00067/5808

Attention: Beneficiaro

PREMIO ASEGURADO

Tenemos el inmenso placer de informarle hoy día 08 de Abril 2011, el resultado de las promociones de loterías "UK NATIONAL LOTTERY" llevado a cabo el día 22 de Abril 2011.

Su nombre con su email ha sido premiado adjunto al boleto: 026-9-2 con número de serie: 7-8 mostró el número afortunado De Remesa: 1-8-3. En consecuencia, ganador de la lotería en tercera categoría. Por lo tanto, a usted le ha correspondido un premio de €915.000,00 euros (NOVECIENTOS QUINCE MIL EUROS) en efectivo. El número de referencia de archivo para reclamar su premio es: GTC1/2551256003/09. El premio total en efectivo es €19.733.910 euros (DIECINUEVE MILLONES SETECIENTOS TREINTA Y TRES MIL NOVECIENTOS DIEZ EUROS). Compartido entre varios ganadores a diferente escala internacional en esta categoría 3. Felicitaciones!

Todos los participantes han sido seleccionados a través de un sistema informático, llevado a cabo anualmente. En este momento, su dinero se encuentra depositado en una cuenta provisoria a su nombre, bajo un seguro que nuestra empresa ha puesto a su dinero para tenerlo asegurado. Para mayor seguridad, le pedimos guarde bien esta documentación, ya que aquí figura su número de referencia y cualquier persona que posea estos datos podría reclamar el dinero en su nombre.

Para comenzar su demanda, debe ponerse en contacto con el número de teléfono que aquí le indicamos, y su agente le informara el procedimiento para el cobro correspondiente a su dinero. Teléfono:+44[redacted] Email: [redacted]@in.com FIRST SECURITY COMPANY L.T.D Persona responsable de asesoramiento: ALAMS DOUGLAS. Horario comercial: Lunes a Viernes de 10 a 14 hs y de 17 a 20 hs. NOTA: Todo premio debe ser reclamado antes de 26 de Julio de 2011. Después de esta fecha, los fondos serán devueltos al MINISTERIO DE ECONOMIA Y HACIENDA como no reclamado.

RELLENE EL FORMULARIO Y ENVIARLO POR E-MAIL AL TU AGENCIAS JUNTO CON TU PHOTOCOPIA DE TU DNI. EMAIL: [redacted]@IN.COM

…otros tipos de Phishing

- Muleros, ofrecen empleos consistentes en recibir una cantidad de dinero en su cuenta bancaria…

Asunto: Trabajar en casa, pago semanal de l.768 euros por semana.

Bienvenida.

Aumentamos nuestra dependencia y necesitamos le..

Si no esta satisfecho con sus ingresos- aprovechar la oportunidad para convertirse en remoto te propuesto nuestro

corporacion y cobrar de 10 a 30 euros por hora en la Internet.

Todo lo que necesita- posesion nivel de usuario de PC, disponibilidad y una demanda enviada,

que contengan datos de nombre completo, edad y lugar de residencia.

Encuesta que desea expulsar aqui [redacted]@west-ug.org

Ya un par de horas. Le enviaremos una carta en respuesta con explicaciones de la obra detalladas.

Solo esperamos de usted responsabilidad y el deseo para ganar. Y ningunos costes iniciales!

…otros tipos de Phishing

… consecuencias de aceptar trabajos como el anteriormente mostrado…

18 MÁLAGA

Domingo 22.07.12
SUR

Condenada por blanquear dinero desde sus cuentas

:: SUR

MÁLAGA. La Audiencia de Málaga ha condenado por un delito de blanqueo de capitales a una mujer que aceptó una oferta de trabajo como gestor de transferencias, que consistía en recibir en su cuenta bancaria dinero sin comprobar su posible origen ilícito, el cual tenía que remitirlo a otras personas. La pena que se le impone por este delito es de seis meses de prisión y una multa de 7.600 euros.

Según se declara probado en la sentencia, la mujer contactó por correo electrónico con una empresa que le ofreció a cambio de 2.500 euros y un porcentaje por transferencias, recibiendo determinados ingresos que tendría que remitir a las personas que se le indicaran a través de un sistema conocido de envío rápido.

Después de haber realizado otras operaciones similares, en abril de 2010, la mujer recibió en una cuenta tres transferencias por importes de 2.998, 2.997 y 1.650 euros «que habían sido ordenadas fraudulentamente por personas no identificadas con cargo a la cuenta corriente» de otra persona, según la resolución judicial dictada.

Entonces, la acusada hizo dos extracciones de 3.000 euros «a sabiendas del origen delictivo de esas cantidades». La acusada se mostró de acuerdo con los hechos y con las penas solicitadas por el ministerio fiscal al igual que hizo su defensa.

produjo el pasado 28 de junio, en concreto en la calle Papabellotas de Antequera. Las investigaciones se iniciaron el 10 de junio a raíz del robo con intimidación a una joven en un parque de la ciudad del Torcal.

La policía busca a un ciudadano holandés

COLABORACIÓN

:: SUR. La Policía Nacional pidió la colaboración ciudadana para poder localizar a Nerlinio Emerson Greene, nacido en Amsterdam en 1979 y del que se tiene constancia de que estuvo alojado en la Costa del Sol, en la zona de los municipios de Marbella o Estepona en el verano de 2011. Se trata de un hombre de color, de complexión corpulenta, de 1,85 metros de altura, y que suele vestir ropa deportiva, según se informó desde Comisaría Provincial de Málaga.

…otros tipos de Phishing

- Estafas piramidales.

  llega a través de email ofreciendo trabajo basado en la promoción de productos y en la captación de clientes entre tu círculo familiar y de amistades.

- Hoax (bulos).

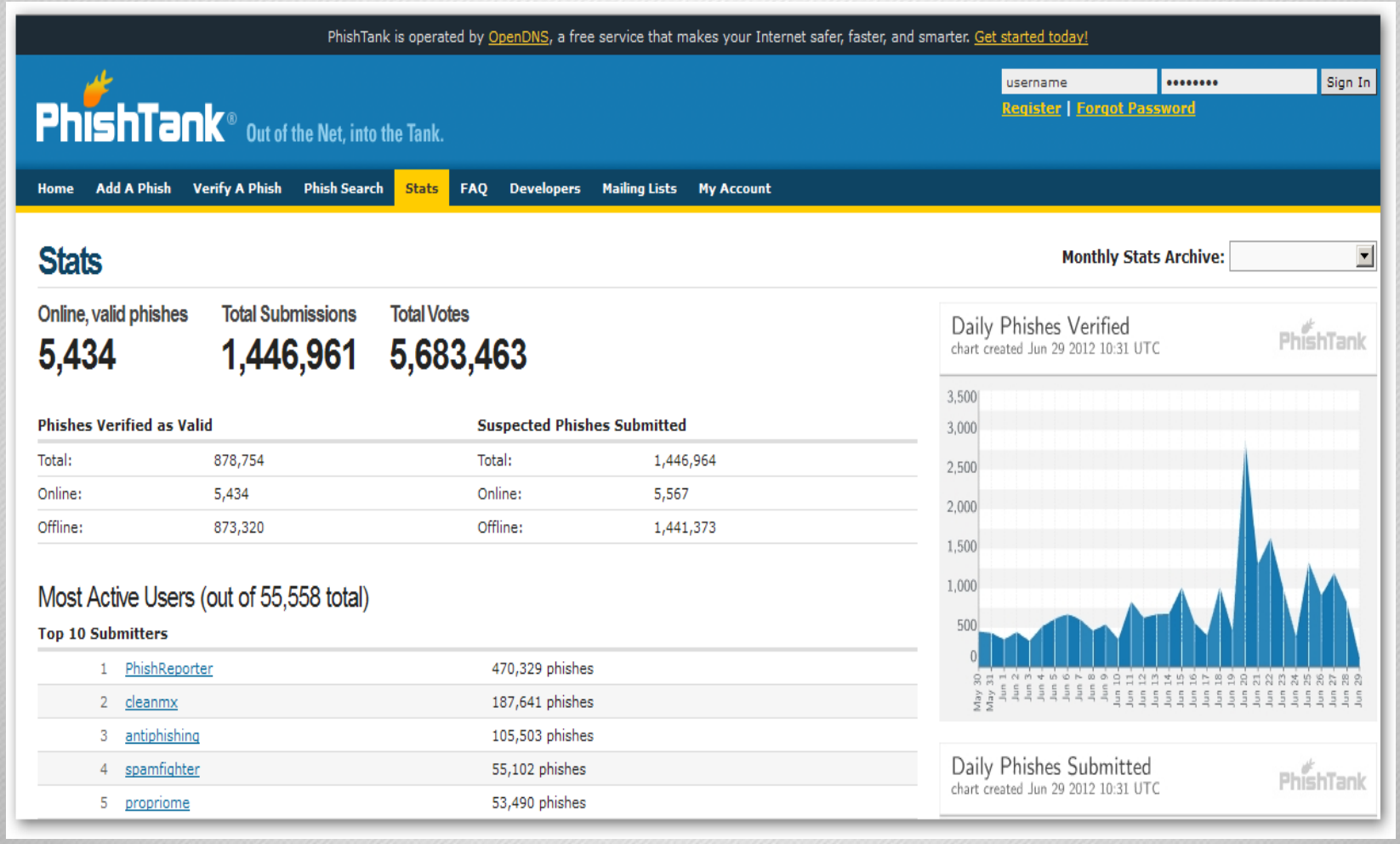
  mensajes con la típica leyenda urbana que debemos obligatoriamente reenviar. Su fin no es otro que recolectar direcciones de correo para su utilización en posteriores spams.

- Ofertas de trabajo.

  también conocidas como scam, en la cual la supuesta empresa se pone en contacto con la víctima a la que piden una cantidad de dinero a cambio de un trabajo bien remunerado.

Phishing … algunas cifras

Fuente Phishtank.org -Junio 2012-



PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank® Out of the Net, into the Tank.

username ••••••••• Sign In

Register | Forgot Password

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Stats

Monthly Stats Archive:

Online, valid phishes	Total Submissions	Total Votes
5,434	1,446,961	5,683,463

Phishes Verified as Valid		Suspected Phishes Submitted	
Total:	878,754	Total:	1,446,964
Online:	5,434	Online:	5,567
Offline:	873,320	Offline:	1,441,373

Most Active Users (out of 55,558 total)

Top 10 Submitters

1	PhishReporter	470,329 phishes
2	cleanmx	187,641 phishes
3	antiphishing	105,503 phishes
4	spamfighter	55,102 phishes
5	propriome	53,490 phishes

Daily Phishes Verified

chart created Jun 29 2012 10:31 UTC

PhishTank

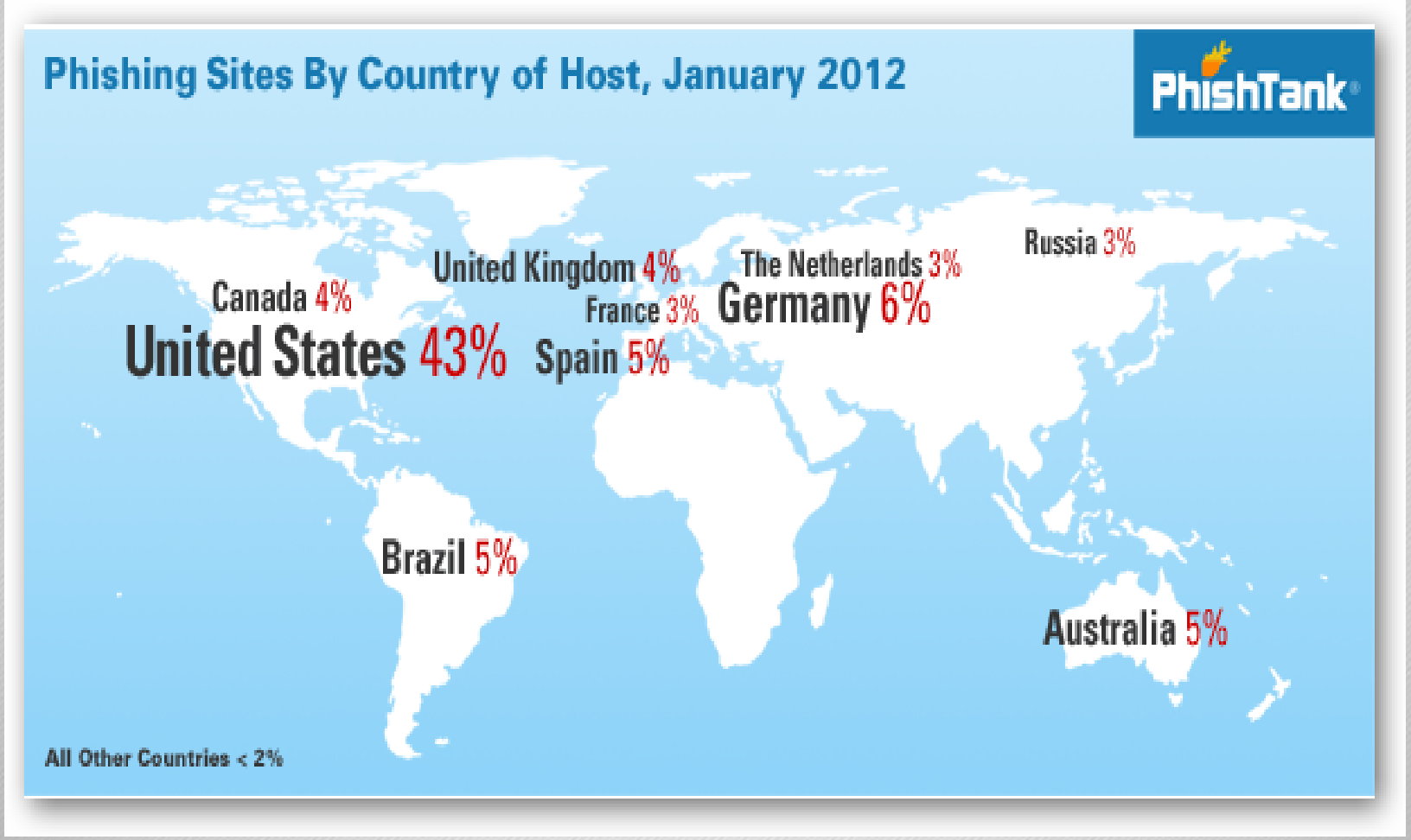
Daily Phishes Submitted

chart created Jun 29 2012 10:31 UTC

PhishTank

Phishing … algunas cifras (continúa)

Fuente Phishtank.org -Junio 2012-



Phishing … algunas cifras (continúa)

Fuente Phishtank.org -Junio 2012-

Popular Targets

These are the brands that were fraudulently represented in phishing emails. Targets are identified by the submitter at the time of submission, or determined by PhishTank's software to the best of its ability. The majority of phishes are not categorized with a target.

Top 10 Identified Targets		Valid Phishes
1	PayPal	6,317
2	Facebook	993
3	TAM Fidelidade	741
4	Santander UK	537
5	Mastercard	291
6	Cielo	257
7	AOL	241
8	Poste Italiane	211
9	Bradesco	179
10	JPMorgan Chase and Co.	174

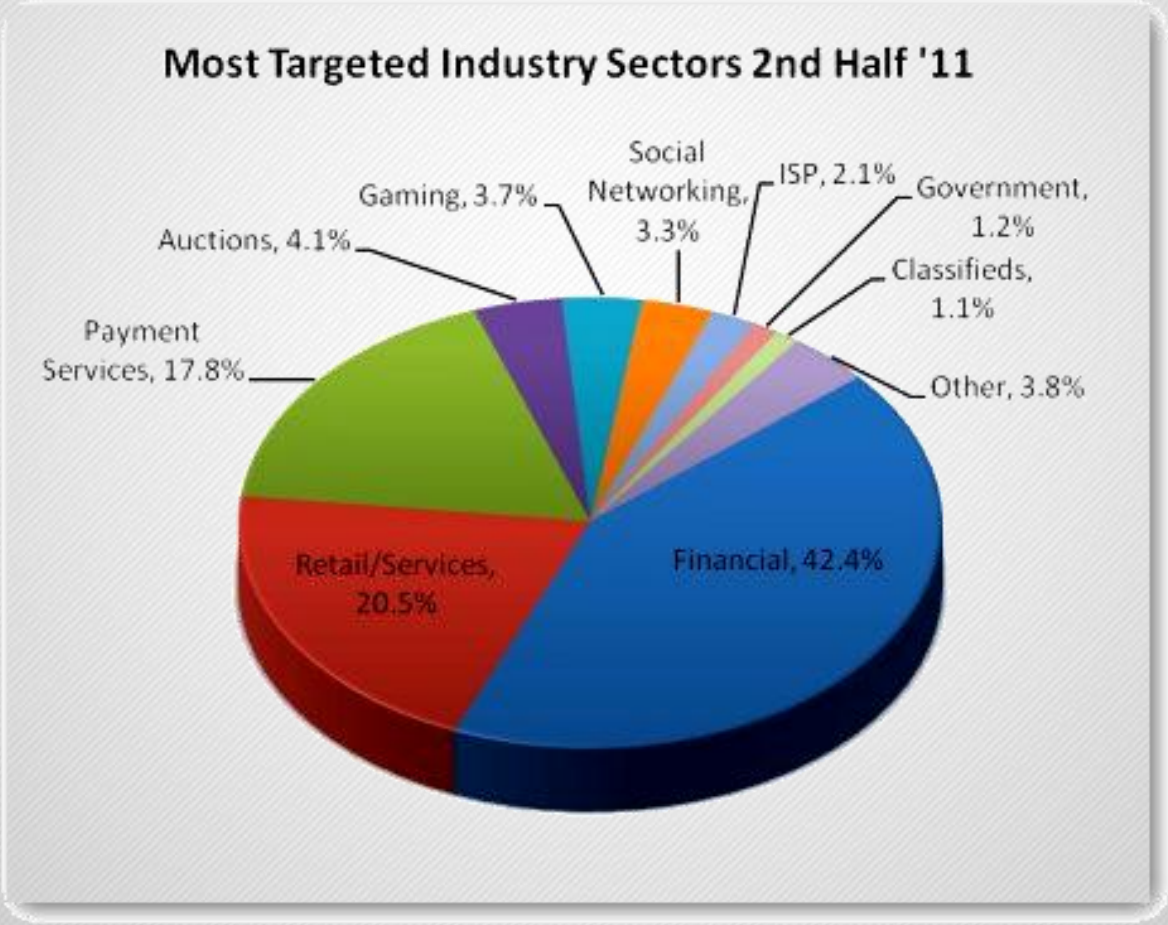
Phishing … algunas cifras (continúa)

Tabla 2: Datos de cuentas bancarias en venta, tomados de un sitio Web de carding

Nombre del banco	País	Saldo	Precio
Bank of América	EE.UU.	…..	Vendido
Asmouth Bank	EE.UU.	16.040 $	700 €
Washington Mutual bank	EE.UU.	14.400 $	600 €
Washington Mutual bank	EE.UU.	7.950 $ + 2.612 £	500 €
Washington Mutual bank	EE.UU.	….	Vendido
MBNA America Bank	EE.UU.	22.003 $	1.500 €
Banco Bradesco S.A.	Brasil	13.451 $	650 €
Citibank	Reino Unido	10.044 £	850 €
NatWest	Reino Unido	12.000 £	1.000 €
BNP Paribas	Francia	30.792 €	2.200 €
Caja de Ahorros de Galicia	España	23.200 €	1.200 €
Caja de Ahorros de Galicia	España	7.846 €	500 €
Banco Sabadell	España	25.663 €	1.450 €

Fuente: PhishTank

Phishing …algunas cifras

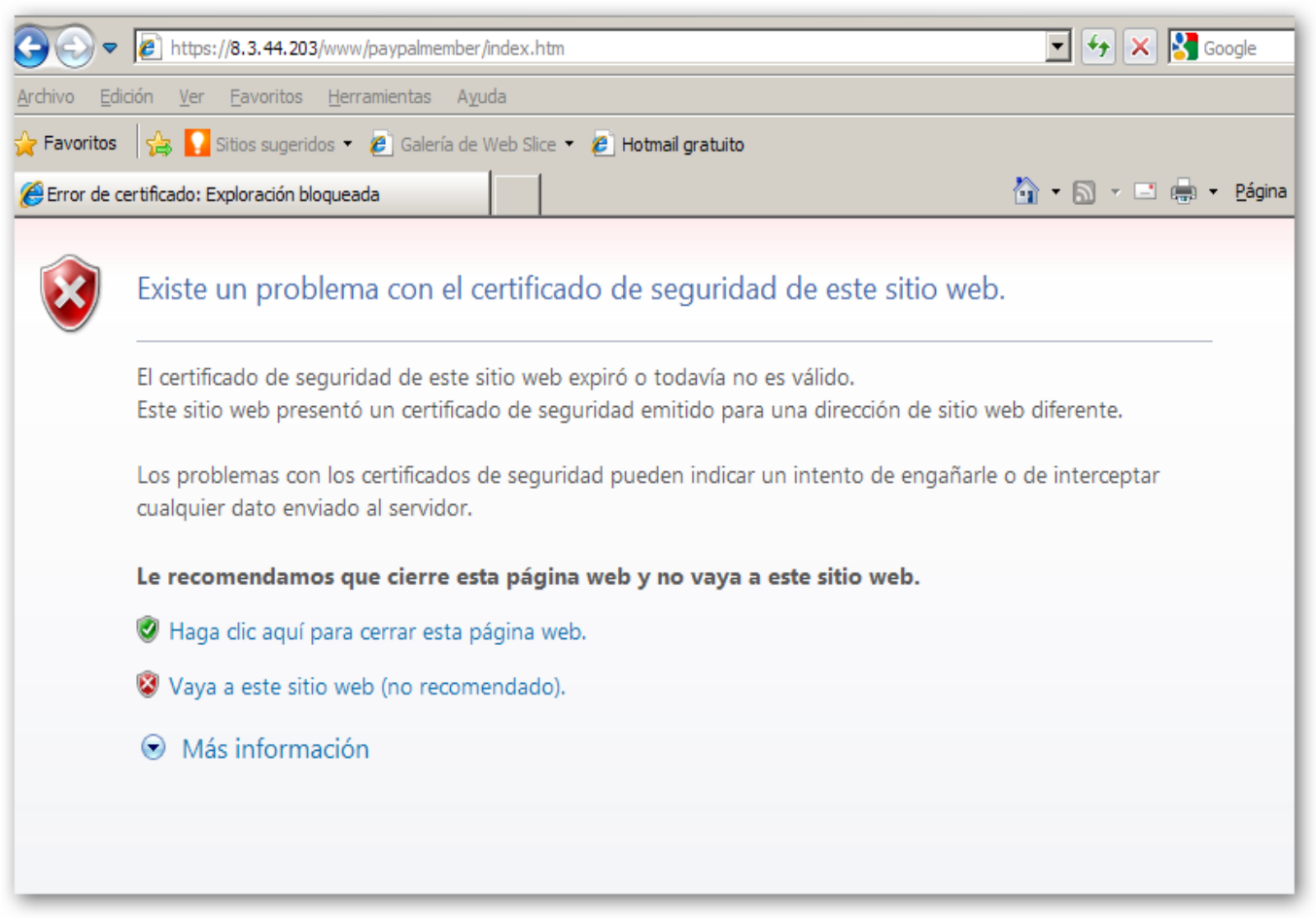


Phishing -comprobaciones con navegadores-

…Intento de phishing con certificado de seguridad falso (navegador Firefox) …

…Phishing -comprobaciones con navegadores-

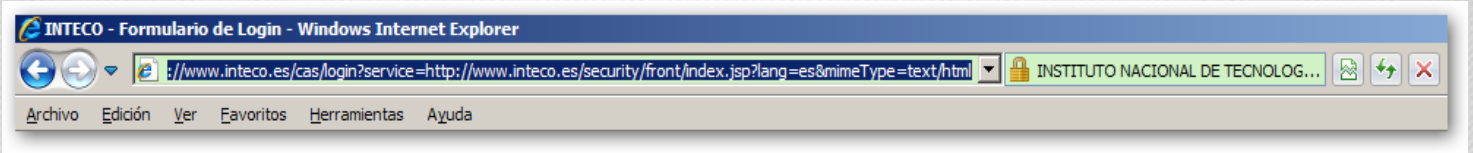
…el mismo intento (navegador Internet Explorer) …



…Phishing -comprobaciones con navegadores-

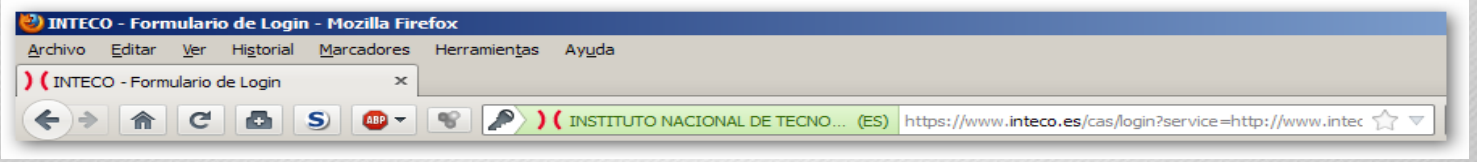
Verificar la autenticidad de un sitio web:

Comprobar su certificado digital.



Internet Explorer
- Fondo de la barra de direcciones de color verde
- Muestra el nombre completo al lado del candado.

Google Chrome
- Muestra el nombre completo al lado del candado.
- Muestra información sobre el certificado al hacer click en el nombre.

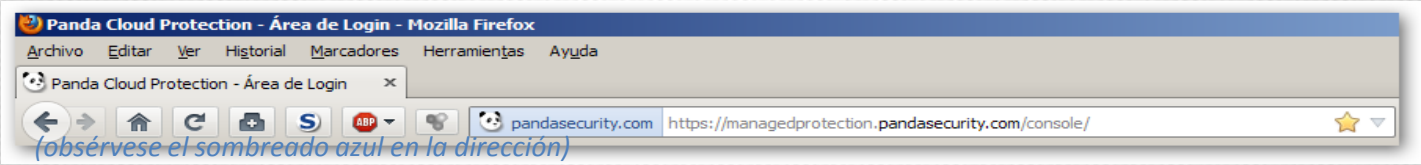


Mozilla Firefox
- Muestra el nombre completo al lado del candado.
- Muestra información sobre el certificado al hacer click en el nombre.

…Phishing -comprobaciones con navegadores-

Navegador Safari
•Aparece el nombre de la entidad con fondo verde, al pasar el ratón por encima.

Si la página sigue manteniendo "https", pero la barra de direcciones no se muestra en color verde , deberemos tener alguna consideración más:



(obsérvese el sombreado azul en la dirección)

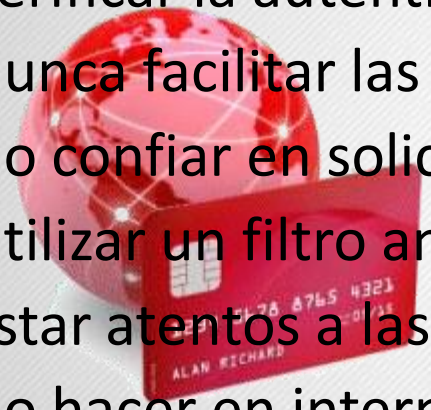
En este caso, el tipo de certificado que usa la página no proporciona información de identidad, es decir, no se ha llegado a verificar que la dirección pertenece realmente a la entidad. Pero no necesariamente indica que no sea una página segura.

Resúmen y precauciones

- Todos tienen en común la posibilidad de dinero fácil y rápido.
- Generalmente están mal redactados con errores ortográficos y gramaticales.
- Las direcciones de correo de procedencia, suelen tener un formato raro.
- Observar detenidamente la información de los navegadores, caso de pulsar sobre el enlace, verificar la autenticidad.

<u>Utilizar siempre el sentido común. No confiar en correos solicitando dinero y/o datos personales.</u>

Phishing – medidas de protección -



- Comprobar con la entidad emisora la veracidad del mensaje.
- Verificar la autenticidad del sitio web.
- Nunca facilitar las claves de acceso.
- No confiar en solicitudes de dinero o información personal.
- Utilizar un filtro antispam.
- Estar atentos a las alertas de seguridad.
- No hacer en internet lo que no haríamos en el mundo real.
- No pulsar en un link de un email de procedencia desconocida.
- Una vez mas. Utilizar el “sentido común”.

Hijackers

Hijackers

- Muestran un mensaje alarmista. (scareware).
- Simulan ser una aplicación de seguridad gratuita.
- Ofrecen su descarga para solucionar el problema.
- Anulan las protecciones del sistema (caso de haberlas).
- Secuestran el sistema operativo haciendo imposible su utilización.
- Solicitan el pago de una cantidad para restituir el sistema a la normalidad.
- No pagar nunca, ninguna cantidad.

Hijackers


New AntiVirus 2010-Trial Version
New Antivirus 2010
Stay Protected, Care of Earth
Registration
LiveSupport
System Scan
Privacy
Attention!
This computer is infected with spyware / adware.
Your Security and Privacy are in danger.
WARNING!
YOU'RE IN DANGER!
SECURE YOURSELF RIGHT NOW!
REMOVE ALL SPYWARE FROM YOUR PC!
UPGRADE NOW
Antispyware Soft
Innovative protection for your PC
Performing Scan
Stop scan
Perform Scan
Current state: Scanning computer
Total: 1812
C:\WINDOWS\inf\netdm.inf
Out of date
STATISTICS
SpyFalcon
Status
Location
Critical
High
41% completed
CleanUp Antivirus
Activate
Advanced Security Center
Scan results
Critical System Error!
System detected virus activities. They may cause critical system failure. Please, use antimalware software to clean and protect your system from parasite programs.
Click this baloon to get all available software.
SYSTEM STOPPED
SpyTrooper Spyware Protection Status
SpyTrooper No protection (extremely dangerous)
How to get protected:
- Double-click on the tray icon to open SpyTrooper Control Panel
- Click Settings on the left
- Select as much options as possible for you
- The more options you select the better
Virus.BAT.Gray.705
Recommended:
Please click "Remove all" button to erase all infected files and protect your PC
Remove All
Lawsuites preview
Your computer is infected!
Windows has detected spyware infection.
It is recommended to use special antispyware tools to prevent data loss.
Windows will now download and install the most up-to-date antispyware for you.
Click here to protect your computer from spyware.
Warning!
Spyware detected on your computer!
Install an antivirus or spyware remover to clean your computer.
Enter a previously purchased license code

Hijackers


La policía ESPAÑOLA
Atención!!! Ha sido detectada actividad ilegal! Su sistema operativo ha sido bloqueado debido a una infracción de la legislación alemana!
Han sido detectadas las siguientes infracciones: Su dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la difusión de la pornografía infantil, zoofilia e imágenes de violencia contra menores! En su ordenador han sido detectados los archivos de vídeo de contenido pornográfico con elementos de violencia y pornografía infantil! Además, desde su ordenador se realiza un envío ilegal (SPAM) de orientación pro terrorista. El presente bloqueo ha sido realizado para prevenir la posibilidad de difusión de dichos materiales desde su ordenador en Internet.
Sus datos IP: Browser: OS: Country: City: ISP:
Para desbloquear su ordenador, usted ha de pagar una multa de 100 euros! La multa ha de ser pagada antes de 24 horas desde el momento del bloqueo de su ordenador! En el caso de impago, todos los datos de su ordenador serán eliminados!
Usted tiene dos formas de pagar la multa:
1) Usted puede adquirir un cupón Ukash por el importe de 100 euros. El número de ese cupón Ukash, usted ha de introducir en el campo del pago y apretar el botón "OK". Si el sistema no confirma el pago realizado con éxito, usted ha de enviar el número de su voucher por e-mail.
2) Usted puede pagar la multa mediante paysafecard. Usted ha de pagar paysafecard por el importe de 100 euros. Usted ha de introducir el código PIN del cheque en el campo del pago y apretar el botón "OK". Si el sistema no confirma el pago realizado con éxito, usted ha de enviar el código PIN por e-mail.
Envíe los datos por e-mail: info.lapoliciaespanola@yahoo.com
Donde conseguir Ukash
CAIXAGALICIA
canalrecargas
CORREOS
cajamar
epay
TELECOR
Telefónica
MundiRecargas
Ukash
Ok
paysafecard
pay cash. pay safe.
Ok

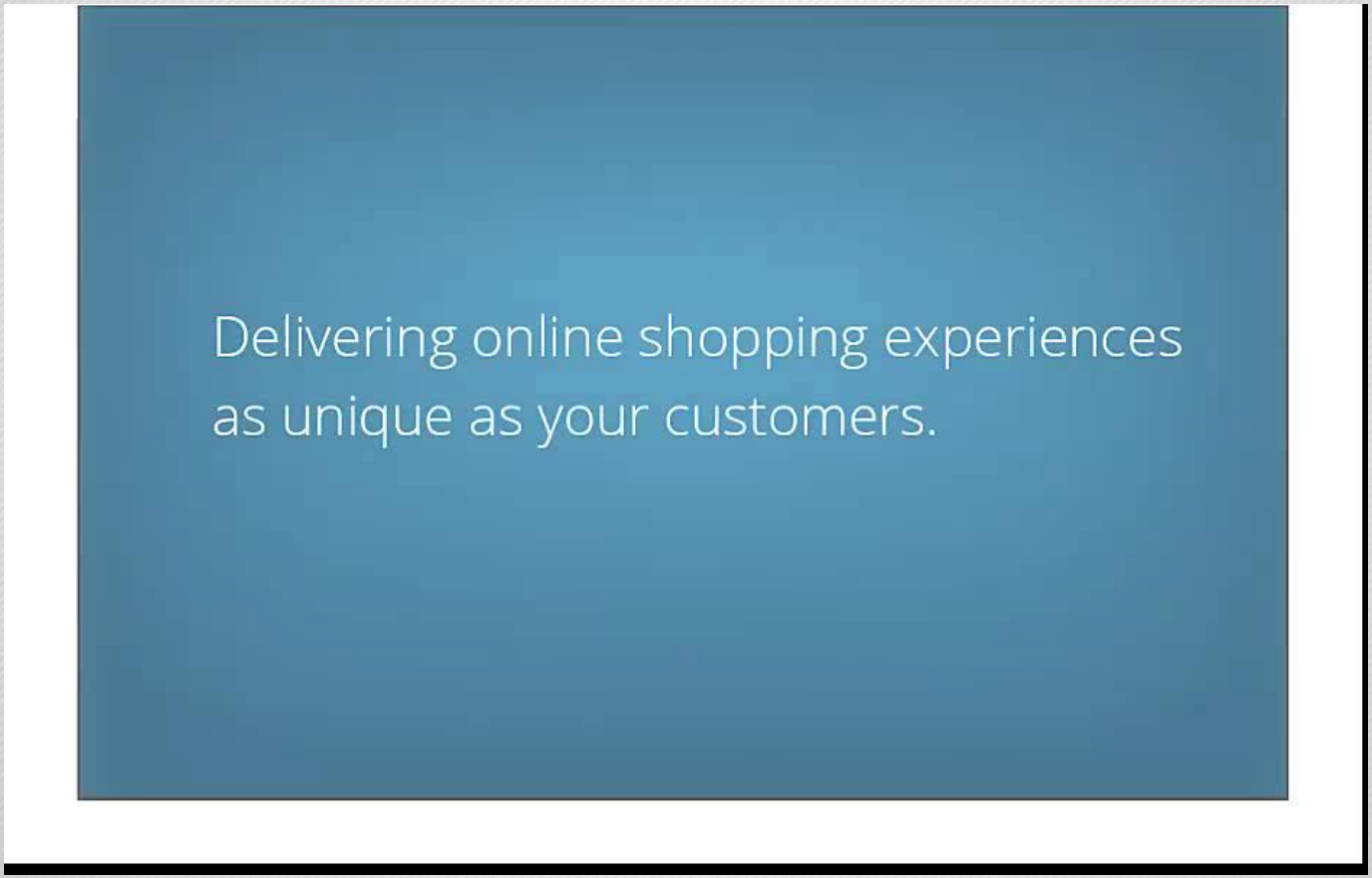
Redes Sociales

Privacidad en redes sociales

- Las redes sociales recaban mas datos de los usuarios que ninguna otra actividad en internet.
- Voluntariamente: teléfono, email, tarjeta crédito, etc.
- Involuntariamente: preferencias navegación, búsquedas, geolocalización, compras, IP, etc.
- Comparten o comercializan dicha información con terceros.

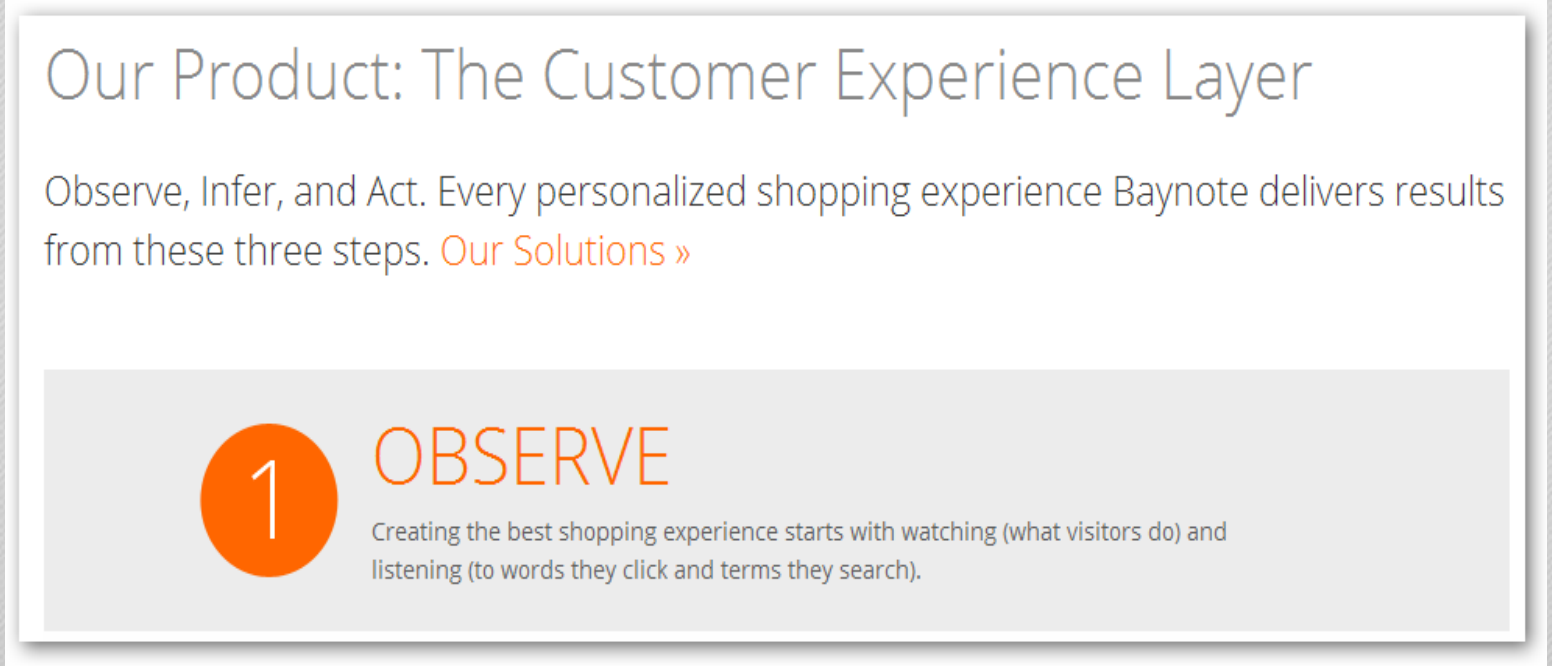
http://www.youtube.com/watch?feature=player_embedded&v=F7pYHN9iC9I

…privacidad en redes sociales



…privacidad en redes sociales

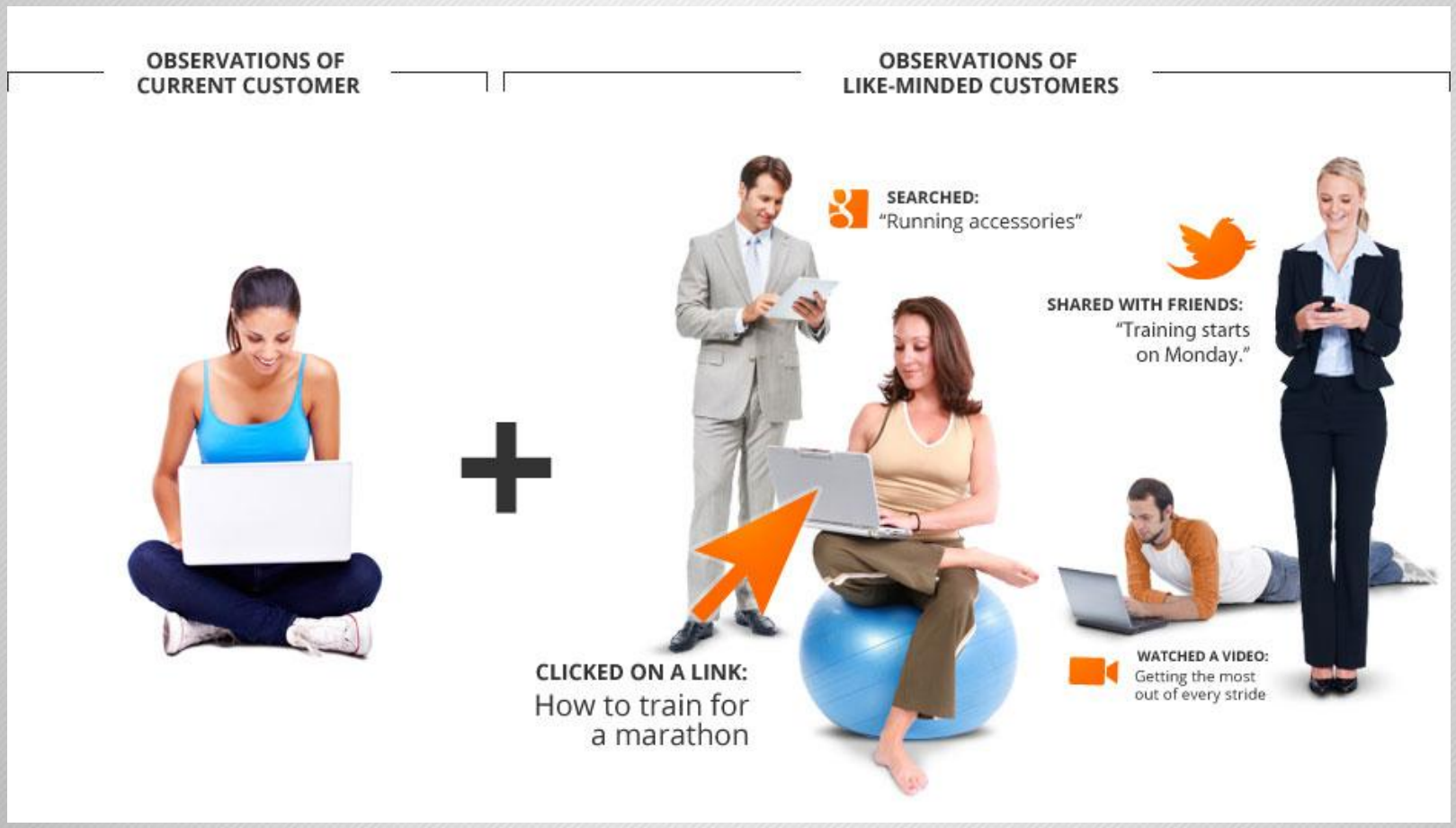
ejemplo de compañía especializada: www.baynote.com



…privacidad en redes sociales

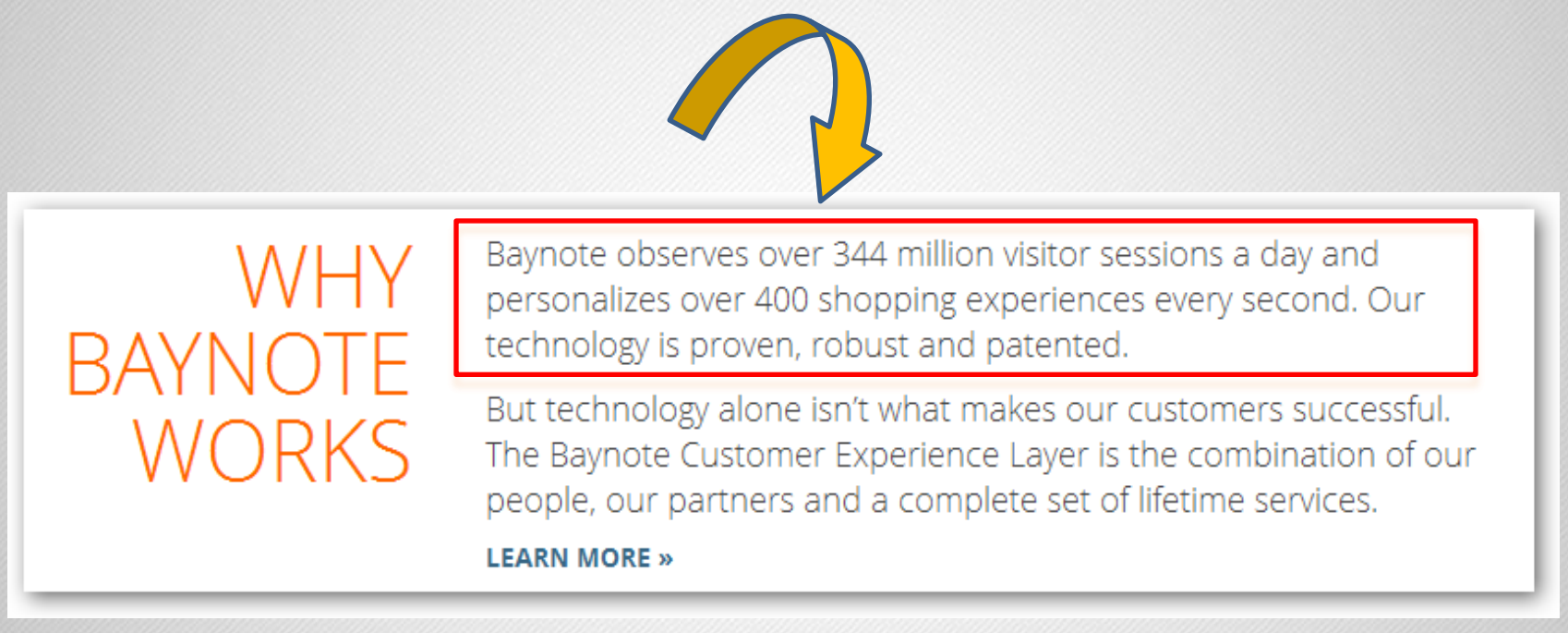
…privacidad en redes sociales

…privacidad en redes sociales



…privacidad en redes sociales

…privacidad en redes sociales



Seguridad – riesgos en las Redes Sociales

Procedimientos mas frecuentes

- Debido a su popularidad actual, los delincuentes las convierten en blancos de sus artimañas.
- Es frecuente falsificar dichas páginas con otras aparentemente auténticas.
- El ataque a los proveedores para obtener contraseñas es de plena actualidad (LinkedIn, LastFM, eHarmony, Yahoo,etc.)
- Difusión de enlaces mediante entradas en el muro. Con el uso de acortadores se intentan disimular las páginas “gancho”.

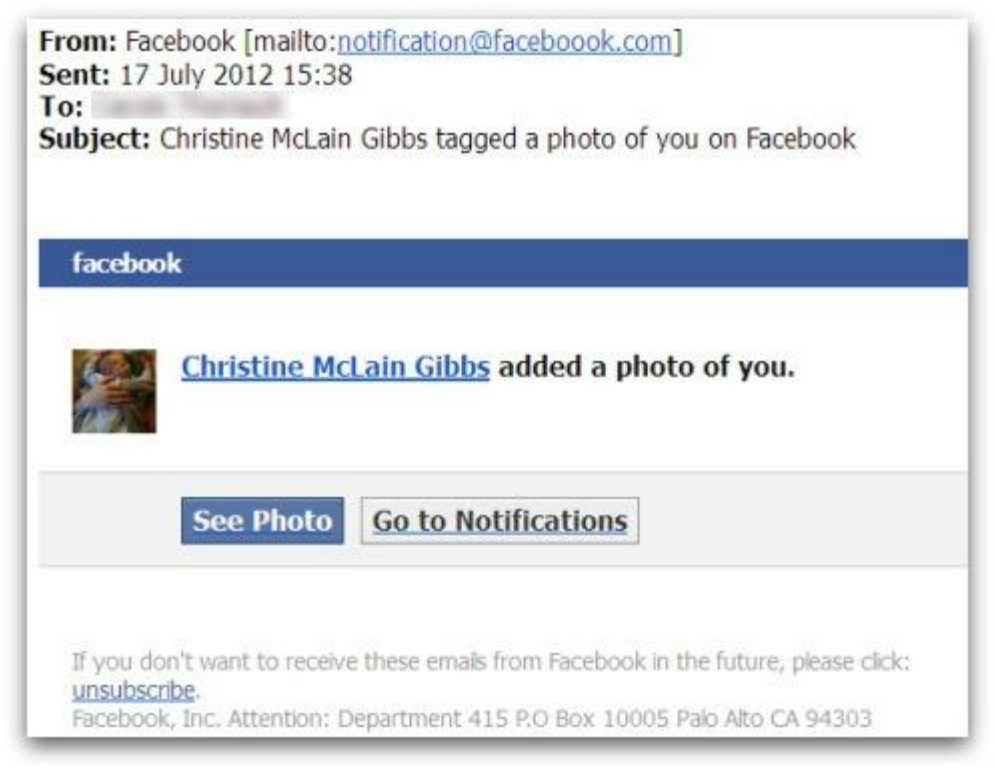
… Redes Sociales

Ejemplo de cebo colocado en el muro.

Otro ejemplo ofreciendo un “test de inteligencia”

…redes sociales

última alerta reportada el 17/07/2012 por SophosLab.



Se recibe un correo en el que nos informan que una foto nuestra, ha sido publicada en Facebook.

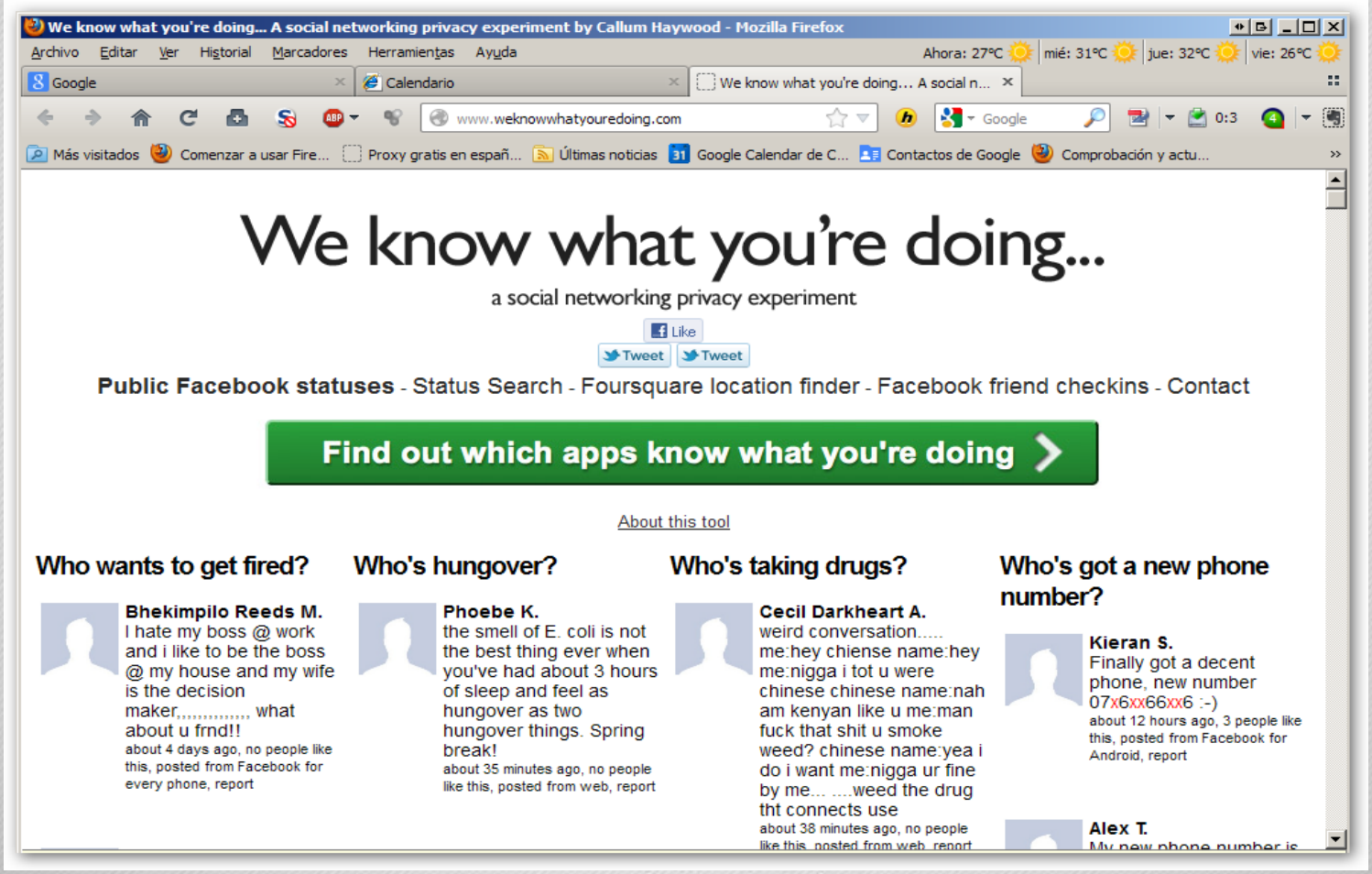
…redes sociales

Al pulsar sobre el enlace nos redirige hacia una página de Facebook, pero de forma oculta nos encamina hacia otra…

…mediante un script inyecta el código malicioso en nuestra máquina.

…privacidad en redes sociales

Página creada para mostrar lo vulnerables que son algunos de nuestros comentarios en las redes sociales.



Redes Sociales – recomendaciones -

- Intenta cambiar la contraseña periódicamente.
- Controla que usuarios pueden ver tu información y cual.
- Restringe que personas pueden buscarte en Facebook.
- No agregues a personas desconocidas a tu lista de contactos.
- Cuidado con las aplicaciones que se utilizan y revisa la lista de permisos concedidos.
- Se siempre respetuoso con el resto de usuarios.
- Piensa antes de publicar un mensaje, foto o vídeo.
- Contrasta la información publicada en otros perfiles, antes de creer cualquier noticia y/o mensaje.
- Usa el sentido común.

Navegación en internet

Navegación segura y privada

Plugins y configuración de los navegadores.

- Configurar el cache del navegador en el mínimo imprescindible.
- Borrar el cache y el historial. (Ctrl+Mayus+Supr)
- Bloquear las ventanas emergentes.
- Cuidado con controles ActiveX y Java scripts.
- Instalar plugins de protección a la navegación. (DoNotTrackPlus, NoScript, AdBlock, etc.).
- Utilizar proxys o DNS seguros (OpenDNS, etc.)

Navegación segura y privada

- La inyección de código malicioso a través de la navegación es cada vez mas frecuente.
- Numerosas páginas legítimas están siendo comprometidas por atacantes.
- La protección http en antivirus se hace imprescindible.
- No pulsar de forma compulsiva cualquier link o mensaje que aparezca.
- Asegurarse de tener perfectamente actualizado el navegador y el S.O. así como el resto de los programas instalados. (Acrobat, Flash, Java, etc.)

Actualizaciones

- Comprobar la activación de actualizaciones automáticas del S.O.
- No posponer o ignorar las actualizaciones.
- Reiniciar el sistema inmediatamente después de actualizar.
- Comprobar las actualizaciones de firmas del antivirus.
- Aceptar las actualizaciones de terceros (Java, navegadores, Adobe, etc.)

y cuando todo falla…

Plan de recuperación de desastres.

- Sistemas de backup.
- Copias en dispositivos externos.
- Almacenamiento en la nube.
- Imágenes de recuperación.
- Virtualización.

¡Gracias !

(Carlos Rodríguez Sánchez)