Delitos informáticos

Estudio concreto sobre Fraudes y Phishing.

Grado en Ingeniería Informática

2013

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Jaén

Raúl Moya Reyes

www.raulmoya.es

Índice de contenido

NOTA: No me hago responsable del mal uso de este documento. Es solo una muestra de un tipo de fraude a nivel educativo.

Introducción

¿Qué es el Phishing?

El termino Phishing es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la victima.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

¿Es el Phishing un Fraude?

¿Has leído la definición? Por supuesto es un fraude. Realizando ataques de este tipo se estafan cantidades increíbles de dinero. En el 2012, se detuvieron en España a un grupo de personas que habían estafado 120 000 €.

¿Cómo funciona?

El mecanismo más habitual es la generación de un correo electrónico falso que simule proceder de una determinada compañía, a cuyos clientes se pretende engañar. Dicho mensaje contendrá enlaces que apuntan a una o varias páginas web que replican en todo o en parte el aspecto y la funcionalidad de la empresa, de la que se espera que el receptor mantenga una relación comercial. Si el receptor del mensaje de correo efectivamente tiene esa relación con la empresa y confía en que el mensaje procede realmente de esta fuente, puede acabar introduciendo información sensible en un formulario falso ubicado en uno de esos sitios web.

Tipos de ataques relacionados con el Phishing

Deceptive Phishing

Es la modalidad más común. Consiste en el envío de un correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza. El receptor pulsará en el enlace contenido en el mensaje, siendo desviado de manera inconsciente a un sitio web fraudulento.

Malware-Based Phishing

Se refiere a la variante del delito que implica la ejecución de un software malicioso en el ordenador. El usuario deberá realizar alguna actuación que permita la ejecución del malware en su ordenador (abrir un archivo adjunto, visitar una web y descargar un programa, etc.).

Keyloggers y Screenloggers

Son una variedad particular de malware. Los Keyloggers son programas que registran las pulsaciones del teclado cuando la máquina en la que están instaladas accede a una web registrada. Los datos son grabados por el programa y enviados al delincuente por Internet. Los Screenloggers tienen la misma función, pero capturan imágenes de la pantalla.

Session Hijacking

Describe el ataque que se produce una vez que el usuario ha accedido a alguna web registrada por el software. Estos programas suelen ir disfrazados como un componente del propio navegador.

Web Trojans

Son programas que aparecen en forma de ventanas emergentes sobre las pantallas de validación de páginas web legítimas. El usuario cree que está introduciendo sus datos en la web real, mientras que lo está haciendo en el software malicioso.

System Reconfiguration Attacks

Este ataque se efectúa modificando los parámetros de configuración del ordenador del usuario, por ejemplo modificando el sistema de nombres de dominio.

Data Theft

Se trata de códigos maliciosos que recaban información confidencial almacenada dentro la máquina en la que se instalan.

DNS-Based Phishing ("Pharming")

Este delito se basa en la interferencia en el proceso de búsqueda de un nombre de dominio, es decir modifica fraudulentamente la resolución del nombre de dominio enviando al usuario a una dirección IP distinta.

Hosts File Poisoning

Es otra forma de llevar a cabo el Pharming. En este caso la transformación se lleva a cabo mediante el fichero hosts albergado en los servidores DNS.

Content-Injection Phishing

Esta modalidad consiste en introducir contenido fraudulento dentro de un sitio web legítimo

Man-in-the-Middle Phishing

En este caso, el delincuente se posiciona entre el ordenador del usuario y el servidor, pudiendo filtrar, leer y modificar información.

Search Engine Phishing

Los phishers crean buscadores para redireccionarte a los sitios fraudulentos.

Phishing en la práctica – Facebook

Pasos previos

Este ejemplo lo vamos a realizar en una red wifi, por tanto vamos a realizar unos pasos previos para entrar en la red, interceptar las conexiones y analizar los resultados obtenidos.

Hurto de la red

No es el caso de estudio, pero es muy conocido que muchos métodos de seguridad wifi han quedado obsoletos por múltiples vulnerabilidades. Incluso podemos partir de que estemos en una red pública como la de un hotel, aeropuerto, etc.

Man in the Middle

En este punto ya estamos conectados en una red, ya sea pública, mediante hurto de la red o cualquier método. Hace tiempo realicé otro manual para realizar ataques MITM, os animo a repasarlo en este enlace.

http://demos.raulmoya.es/documentos/MITM.pdf

Aquí podréis aprender a hacer un MITM, redireccionamiento DNS y algún otro punto de interés.

Análisis de resultados

Una vez que ya hemos interceptado el tráfico debemos analizar los resultados. Para este ejemplo suponemos que una de las páginas visitadas es Facebook pero por algún motivo de seguridad no nos ha sido posible obtener las credenciales de acceso. Vamos al ataque Phishing.

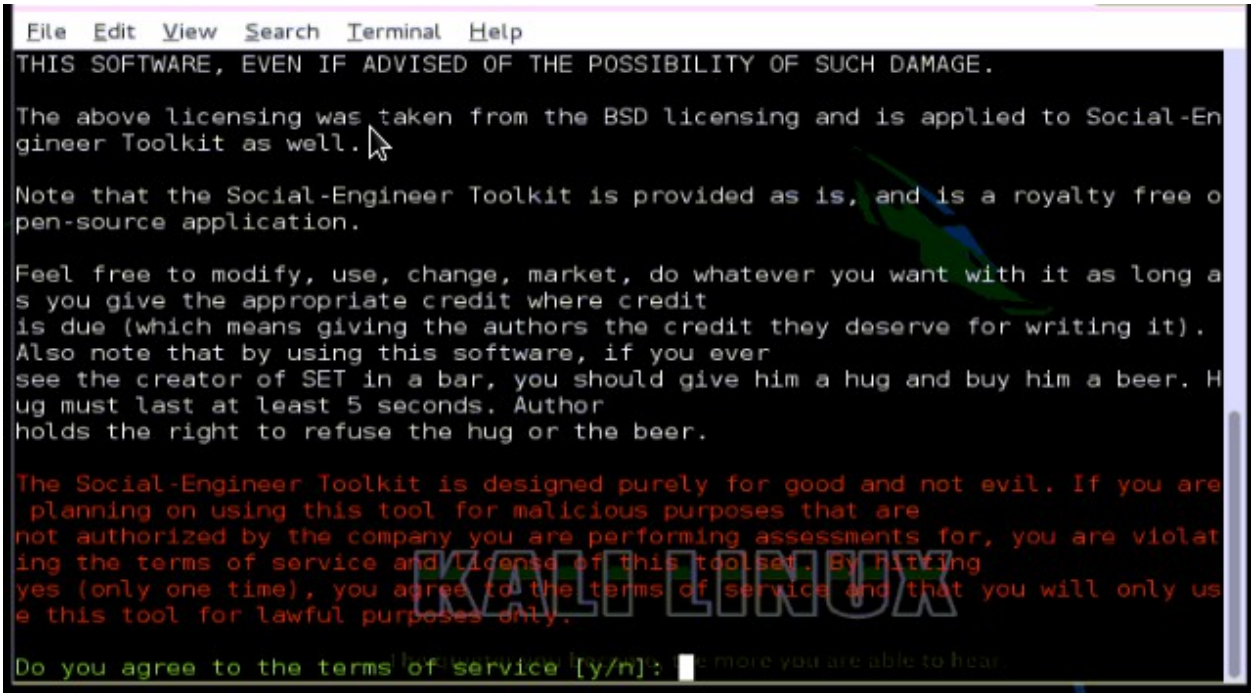
Ataque usando Kali Linux y SE-Toolkit

Para realizar este ataque voy a utilizar la aplicación Social Engineering Toolkit (SET). Para ahorrarme problemas de instalación o compatibilidades voy a usar la distribución de linux llama Kali.

Abrimos una consola y ejecutamos SET

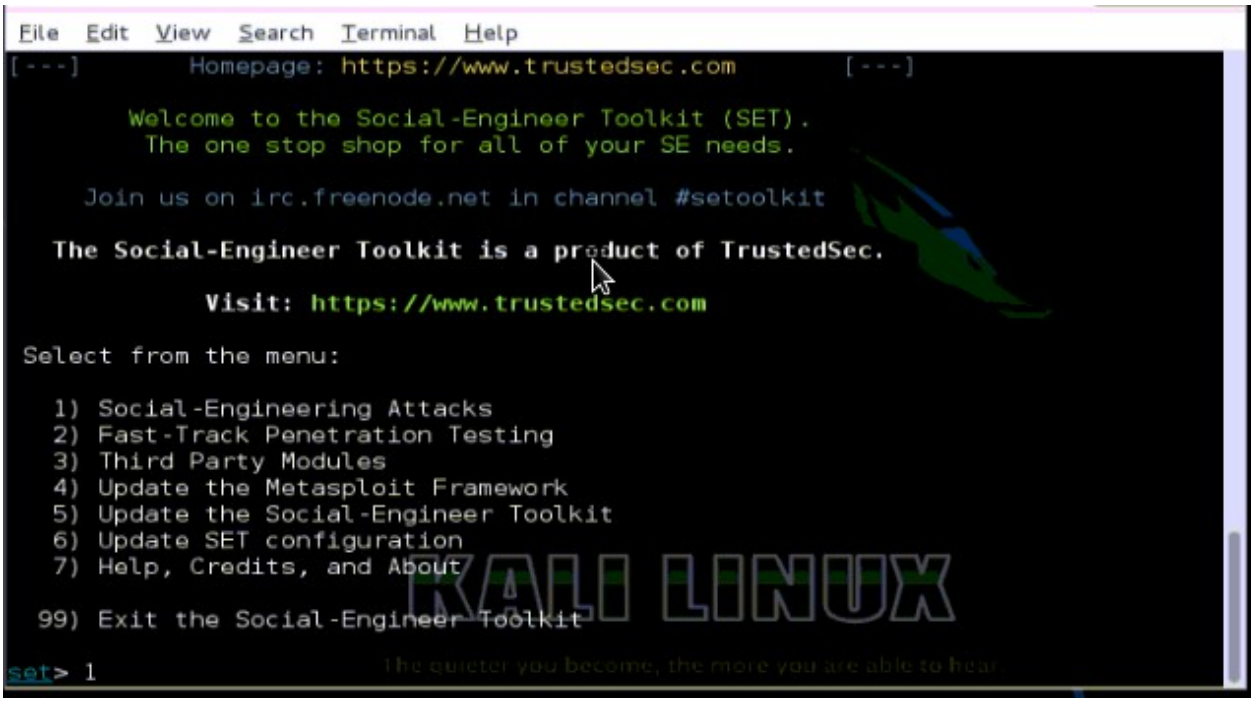
```
$ se-toolkit
```

Nos pide aceptación de su política de uso, si queremos usar la aplicación hay que acertar.



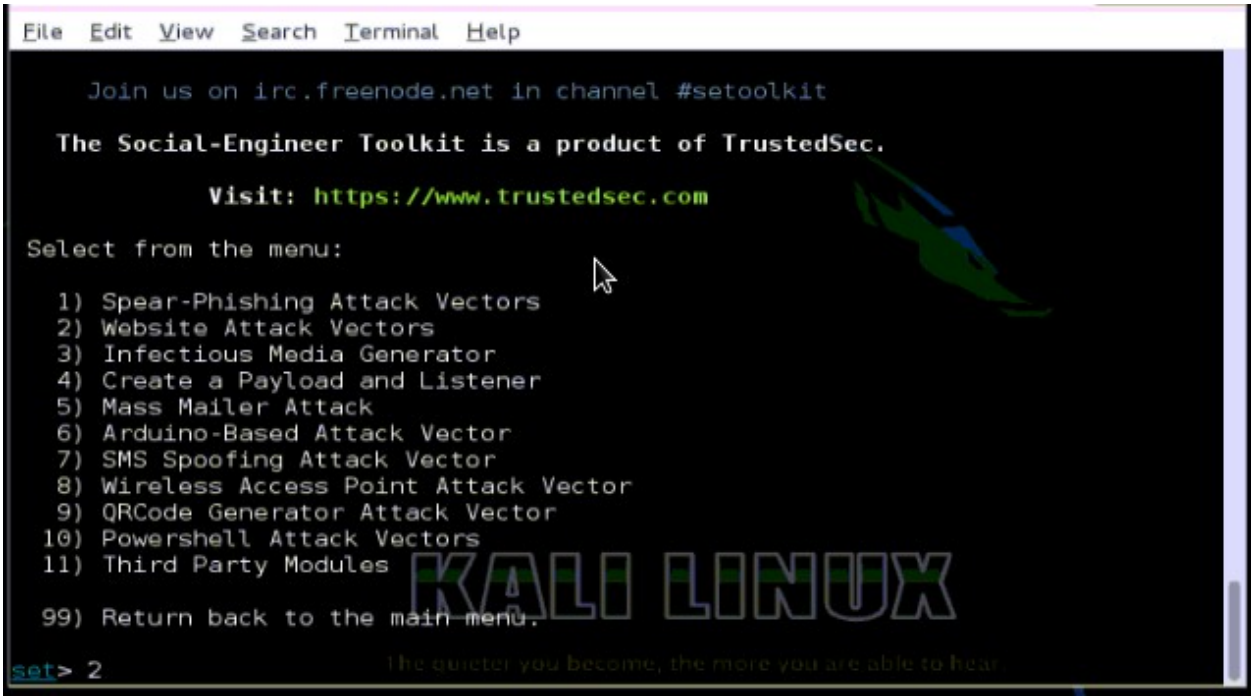
Seleccionamos la opción Social-Engineering Attacks

```
$ 1
```



A continuación seleccionamos la opción Website Attack Vectors

```
$ 2
```

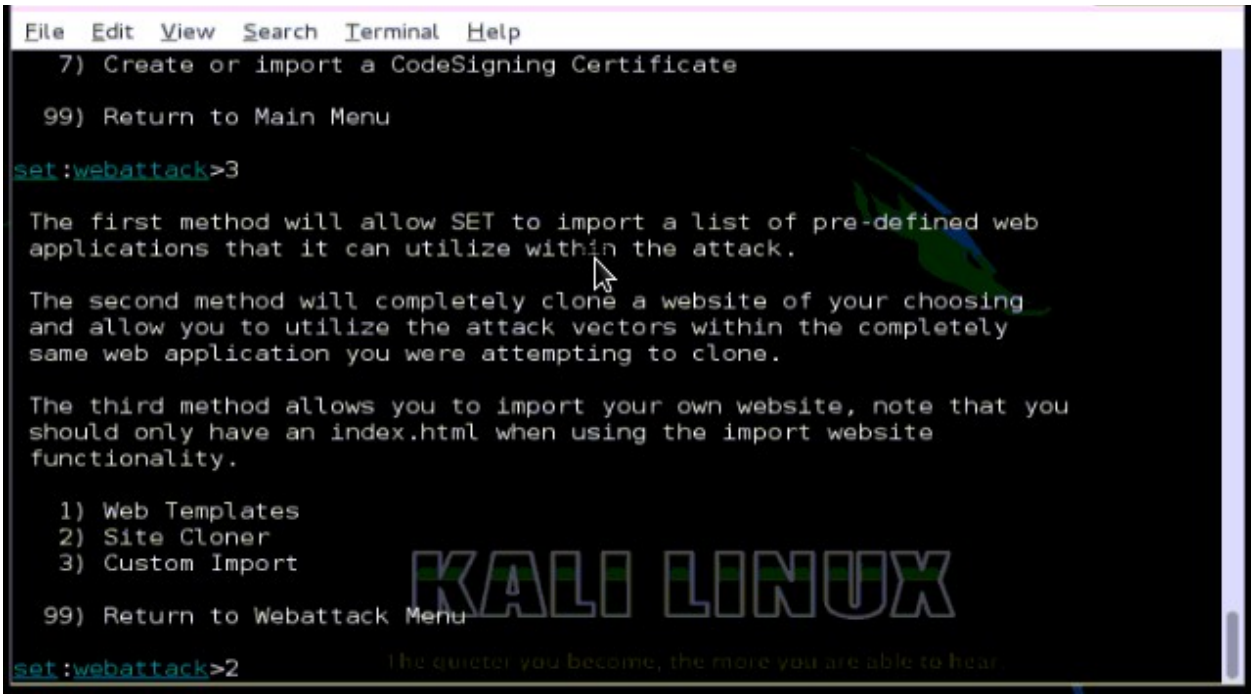


Después la opción Credential Harvester Attack Method

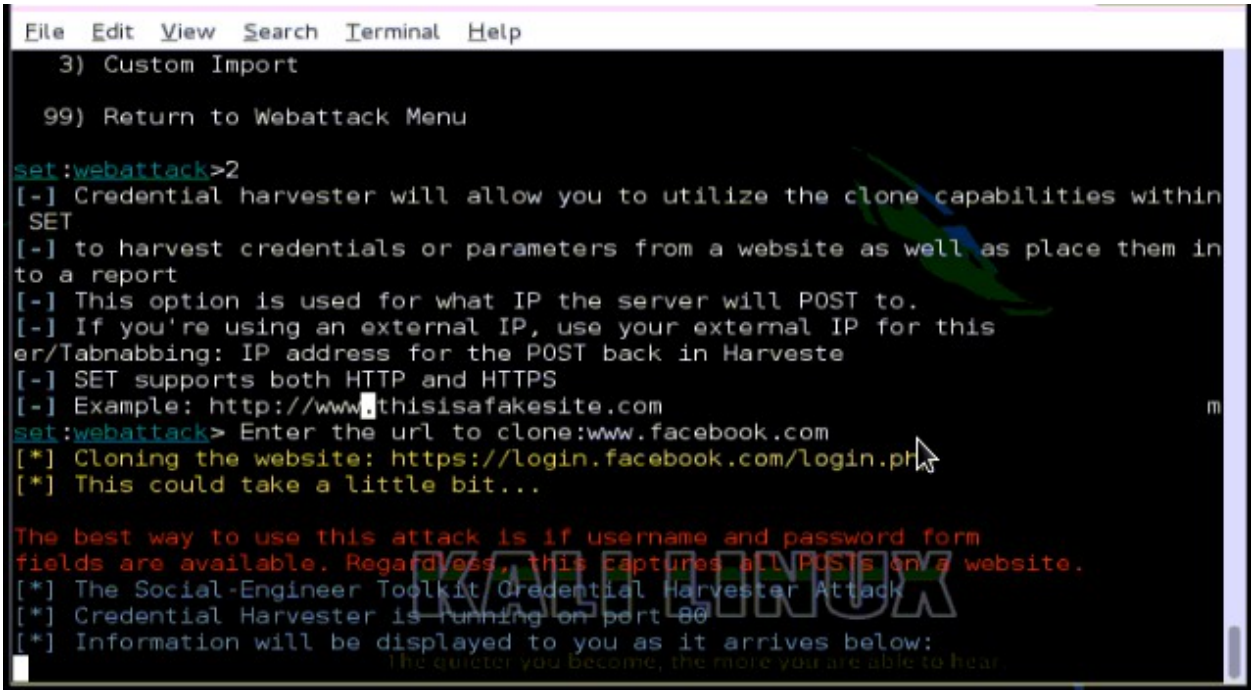
```
$ 3
```

Ahora la opción Site Cloner

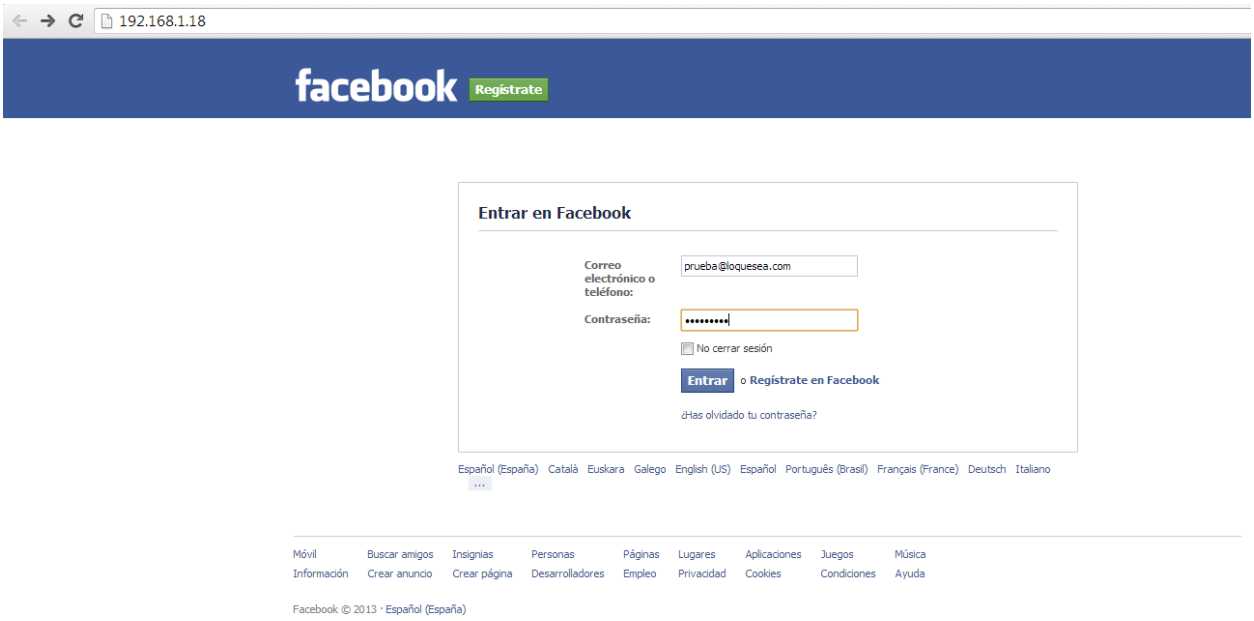
```
$ 2
```



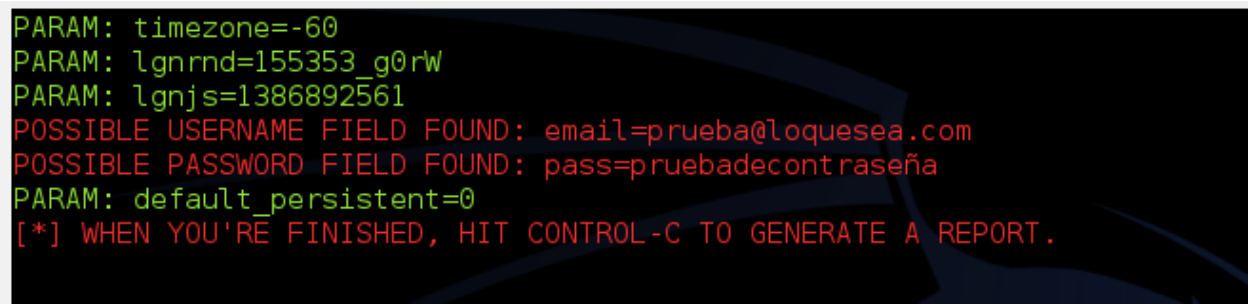
En este punto debemos introducir la ip desde donde hacemos el ataque y la url de la página que vamos a clonar



Ahora en nuestra ip tenemos un clon de la página de login de facebook.



Al introducir los datos y darle a enviar, se realiza una redirección a Facebook y nos aparecen los datos en la consola.



Protección ante el Phishing

Depende de lo elaborado que esté el ataque, pero la mayoría son fácilmente detectables. Las entidades u organismos nunca te solicitarán contraseñas, números de tarjeta de crédito o cualquier información personal por correo electrónico, por telefóno o SMS. Ellos ya tienen tus datos. Lo más seguro en estas situaciones es no enviar ningún tipo de información de la que nos soliciten.

Como hemos visto hay que tener cuidado con los enlaces a los que hacemos clic. Una combinación de distintos ataques puede hacer que la detección sea muy difícil. Por ello, antes de hacer clic en una url acortada, por ejemplo, podemos ver donde conduce con un alargador de urls como http://knowurl.com/. Siempre es mejor teclear la url directamente pero debemos asegurarnos de que cuando intentamos acceder a una url, realmente accedemos a esta.. Utilizar los sistemas de seguridad y navegar utilizando conexiones seguras (https) pueden ayudarnos a no caer en estos ataques.

En este enlace podemos ver distinto software antiphishing http://www.dragonjar.org/anti-phishing.

Aun así, no hay que tener miedo a usar internet, solo hay que usarlo sabiendo lo que hacemos.

Enlaces de interés

www.pandasecurity.com
www.infospyware.com
www.elhacker.net/
www.securitybydefault.com/
www.dragonjar.org/

http://es.wikipedia.org/wiki/Phishing

http://demos.raulmoya.es/documentos/MITM.pdf
http://demos.raulmoya.es/documentos/phishing.pdf