Experiencias educativas

SECUNDARIA / BACHILLERATO

Concienciando sobre los peligros de Internet y su prevención

Pablo Díaz Márquez
IES Francisco de Orellana (Trujillo).

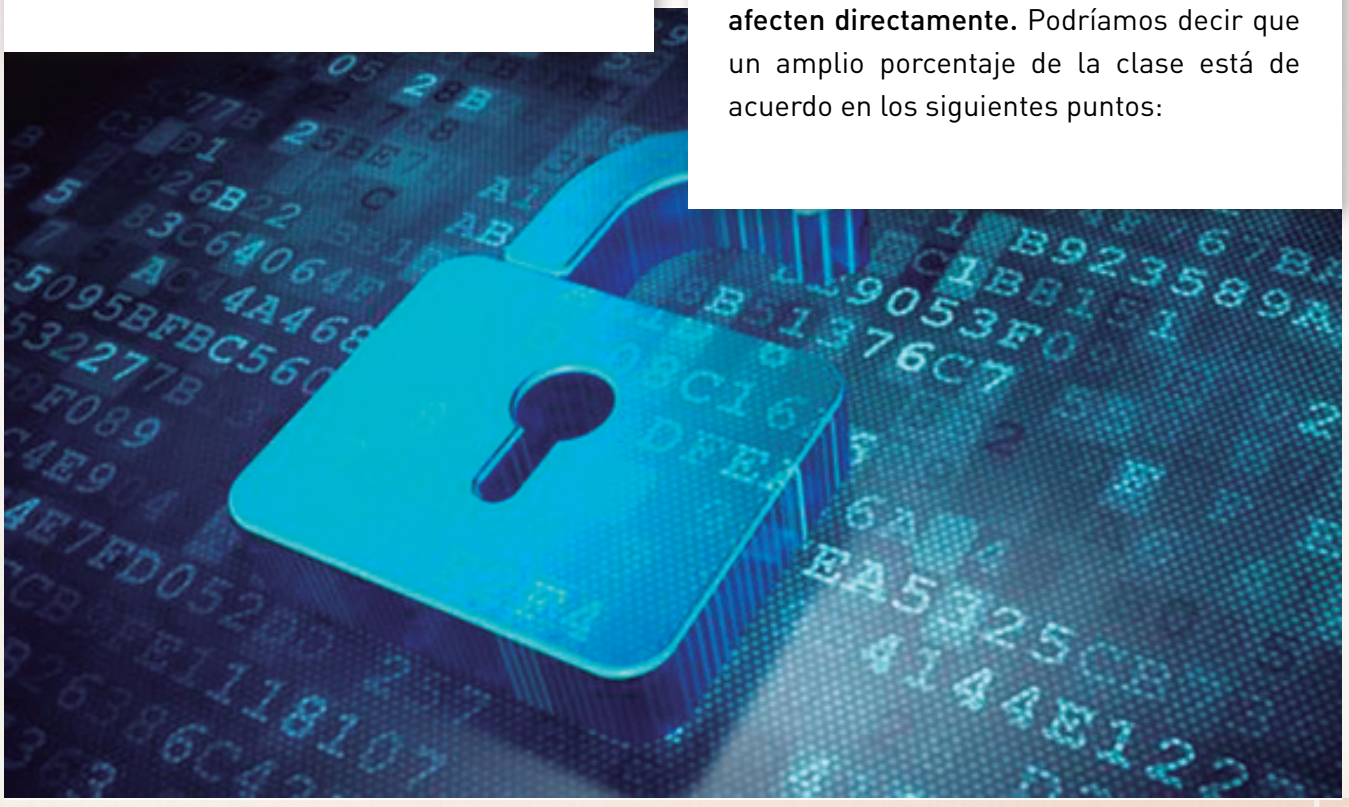
Internet, una de las herramientas más útiles y poderosas de la actualidad para nuestro desarrollo, se encuentra infestada de amenazas y peligros, de los cuales muchas veces no somos conscientes. Uno de nuestros objetivos como docentes es el de dar a conocer su existencia, cercanía y alcance real del problema, así como el de enseñar a protegerse de los mismos mediante el seguimiento serie de sencillas pautas y sobre todo, haciendo uso del sentido común. Quizá estas medidas nunca consigan protegernos totalmente, pero al menos podrán evitar la mayor parte de los males que conocemos.

Palabras clave: Internet, malware, seguridad, WIFI, hackers, Ingeniería Social

Introducción

Uno de los temas impartidos en la asignatura de 4º de ESO de Informática del IES Francisco de Orellana de Trujillo hace referencia a los problemas de seguridad que surgen con el uso masivo de redes y en concreto con Internet. Ciberdelitos, malware, problemas de privacidad relacionados con las Redes Sociales o el uso indebido de redes WIFI ajenas son tratados dentro de este bloque de contenidos con la intención de que el alumno adquiera una visión más amplia de las situaciones a las que puede enfrentarse cuanto utiliza este tipo de tecnologías.

Previo al desarrollo de los conceptos teóricos, los alumnos realizan un pequeño debate informal, guiado y moderado por un el que escribe estas líneas, mediante el cual se intenta determinar su visión particular de peligros existentes en la red. **Todos están de acuerdo en que existen serias amenazas en Internet, pero por lo general, ni las consideran importantes, ni piensan que les afecten directamente.** Podríamos decir que un amplio porcentaje de la clase está de acuerdo en los siguientes puntos:



■ IES Francisco de Orellana (Trujillo).

1. Sus datos personales son poco importantes. La mayoría de los alumnos no disponen de cuentas bancarias, tarjetas de crédito o información susceptible de ser robada. Cualquier otra información como mensajes, fotos, vídeos... no es muy importante y por tanto es poco probable que alguien quisiera robarla para sacar algún provecho de la misma.

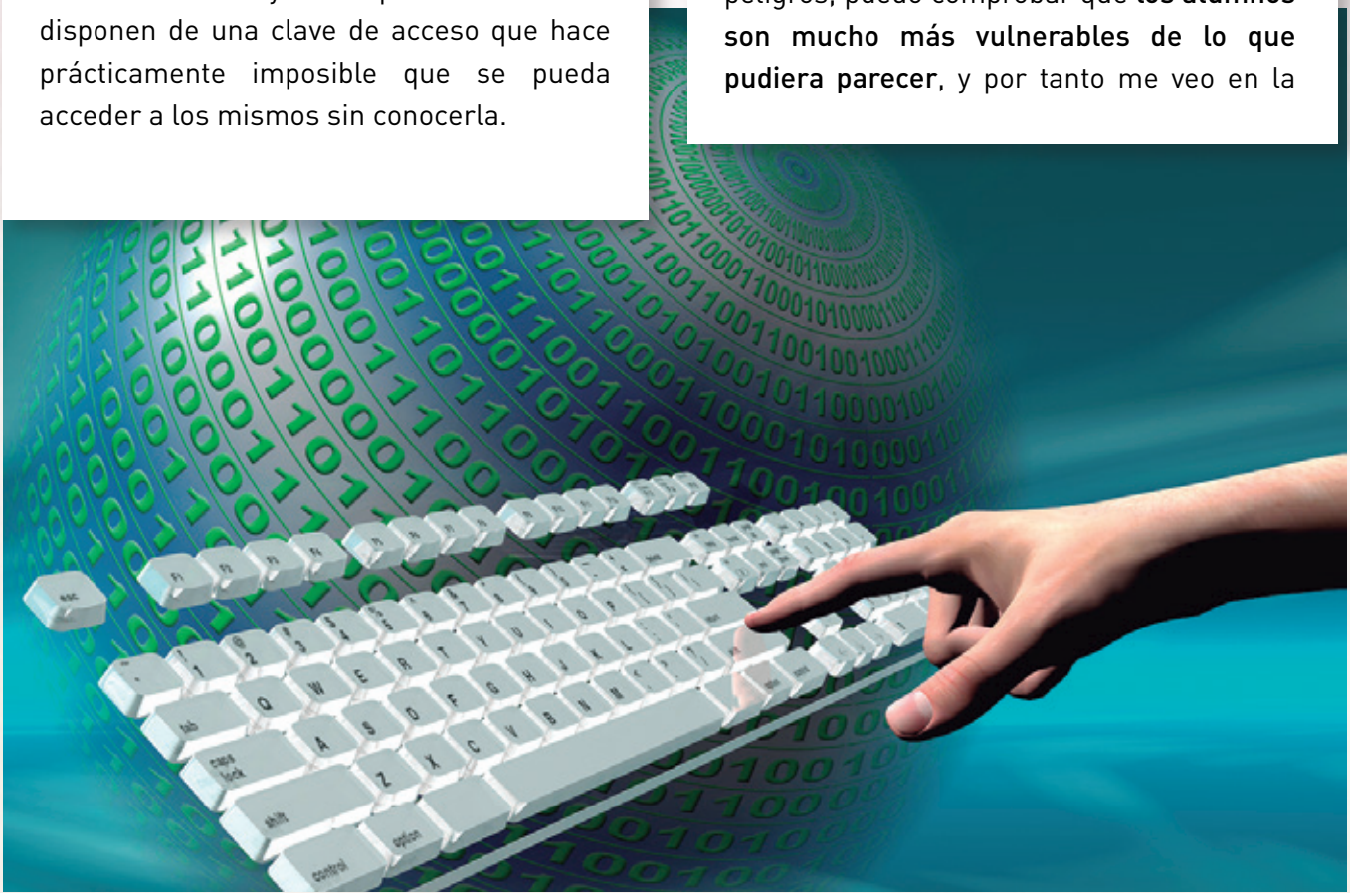
2. Aquellas personas que pudieran estar interesadas en nuestros datos (principalmente personas cercanas) no tienen conocimientos suficientes para acceder a ellos, salvo en el caso de sustracción o robo físico del ordenador o dispositivo que los contiene.

3. El uso de redes WIFI ajenas, no es considerado por ellos como un robo de datos. Tampoco piensan que sea peligroso. En el peor de los casos, si alguien se conecta a tu red, podría ralentizar tus propias conexiones a Internet. Además, la mayoría de los routers de ADSL y fibra óptima domésticos disponen de una clave de acceso que hace prácticamente imposible que se pueda acceder a los mismos sin conocerla.

4. El acceso no autorizado a nuestros datos y recursos informáticos tales como nuestra red WIFI solo puede ser realizado por hackers con conocimientos muy elevados de informática.

Hubiera sido interesante realizar tras el debate una encuesta formal con una batería de preguntas correctamente estructurada a fin de obtener unos resultados que pudieran ser mostrados de forma gráfica en este artículo. Sin embargo, cuando me surgió la posibilidad de escribirlo, esta actividad ya había sido realizada. Plantear la encuesta con posterioridad no habría proporcionado los resultados correctos. No obstante, esta actividad queda abierta para futuros cursos. Es más, a largo plazo podría estudiarse la evolución, promoción a promoción, de cómo perciben los alumnos los peligros existentes en Internet.

Basándome en estas opiniones, relativas a su propia percepción sobre Internet y sus peligros, puedo comprobar que **los alumnos son mucho más vulnerables de lo que pudiera parecer**, y por tanto me veo en la



obligación de definir una serie de pautas de trabajo y objetivos que les permitan abrir sus mentes para comprender la situación real a la que se enfrentan cuando usan esta red. Podríamos enumerar estos objetivos en:

1. Estudiar ejemplos de situaciones reales ocurridas a personas comunes (en muchos casos adolescentes) fruto del desconocimiento de amenazas existentes en la red o de subestimar su peligrosidad.
2. Entender que podemos ser víctimas de cualquiera, tenga o no conocimientos elevados en Informática.
3. Conocer las medidas básicas de actuación para protegernos de estas amenazas.

Amenazas existentes y víctimas reales

El primero de los objetivos propuestos en este tema es el de enseñar el tipo de amenazas con las que podemos encontrarnos con el uso de Internet, y el cambiar la forma en que los alumnos las perciben, dándoles la importancia que se merecen. Y quizá la mejor forma de realizar este cometido es mostrar experiencias reales de distintas personas. En primer lugar, yo mismo puedo contar mis propias vivencias. Pero es posible que la voz de otras personas pueda abrirles más los ojos. **Quizá sea complicado contactar con verdaderos expertos para dar una charla en nuestro IES, pero si buscamos en la red, encontraremos cientos de entrevistas, documentales o ponencias en donde profesionales del tema describen sus propias anécdotas o vivencias.** De entre todos los que pude visionar, me quedé con algunos que me parecieron bastante interesantes:

> Los alumnos son mucho más vulnerables de lo que pudiera parecer.

- Charla de Chema Alonso, considerado como uno de los mejores hackers españoles y experto en seguridad de redes, además de humorista, en el congreso "Creo en Internet" celebrado en septiembre de 2011 en Madrid[CREO]
- Capítulo "Policias y L@drones" de la serie Crónicas de RTVE emitido en mayo de 2013 por esta cadena[POLI]
- Capítulo "El precio de lo gratuito" de la serie Revolución Virtual de la BBC[PREC]
- Algunas entrevistas realizadas en los distintos capítulos de la serie "Mundo Hacker" de Discovery Channel[SPAM][WIFI][MOVI]

Después del visionado de estos documentos, y de alguna experiencia adicional que pude yo aportar, parece que los alumnos comenzaron a ser conscientes de que Internet puede ser una herramienta peligrosa para todos si no se hace un correcto uso de la misma.

Quién puede ejecutar las amenazas

Una vez conseguido el objetivo de que el alumno sea consciente de muchas de las amenazas a las que se enfrentan los usuarios de Internet, el siguiente paso es concienciar de que la realización técnica de las mismas puede ser llevada a cabo por personas cercanas a nosotros con no demasiados conocimientos de Informática. Para ello, qué mejor forma que convertir a los alumnos en "pequeños hackers". Si conseguimos que los alumnos aprendan a romper la seguridad

■ IES Francisco de Orellana (Trujillo).

de algún sistema informático de una forma sencilla, les estaremos enseñando al mismo tiempo que cualquiera con un poco de interés también puede hacerlo. **Quizá no sea fácil romper la seguridad de cualquier equipo informático, pero sí la de aquellos que estén mal configurados, o en los que sus usuarios no tengan ningún tipo de precaución a la hora de instalar programas.** De forma indirecta intentamos conseguir que los alumnos aprendan a proteger sus equipos y sus datos de terceras personas que pudieran hacer lo que ellos van a intentar realizar en el entorno controlado de la clase.

Con anterioridad, ya estudiamos en clase los conceptos de cliente/servidor, y vimos algunas conocidas aplicaciones como SSH o VNC que permiten utilizar los recursos de un equipo remoto desde nuestra máquina local, independientemente del tipo de máquina o sistema operativo que usemos, las cuales nos pueden servir perfectamente para nuestro cometido en clase. Además de estos programas de uso general, existe también gran cantidad de malware específico diseñado para este fin[Viru], aunque en nuestro caso no nos centraremos en su estudio.

En la imagen 1 vemos distintas versiones de servidores y clientes SSH disponibles para la plataforma Android que pueden ser descargados gratis directamente desde el Google Play. *Ver imagen 1.*

Vamos a enumerar a continuación, de forma muy general, los distintos pasos a seguir para que el alumno pueda tomar el control de una determinada máquina objetivo por medio de éstas u otras herramientas.

■ Lo primero es lograr instalar y configurar el software de control que deseemos en la máquina de la víctima. Para pruebas en clase, esta máquina puede ser un teléfono propio. Pero en una situación real, la instalación debería realizarse en una máquina ajena. Existen numerosos sploits que pueden facilitarnos la tarea, pero en nuestro caso haremos uso de **la Ingeniería Social, una de las amenazas más simples y eficaces[CINC], además de ser considerada como la más peligrosa de la red[INGE].** En uno de los capítulos de "Mundo Hacker" vistos por los alumnos[MOVI] se planteaba una curiosa y efectiva manera de "colar un

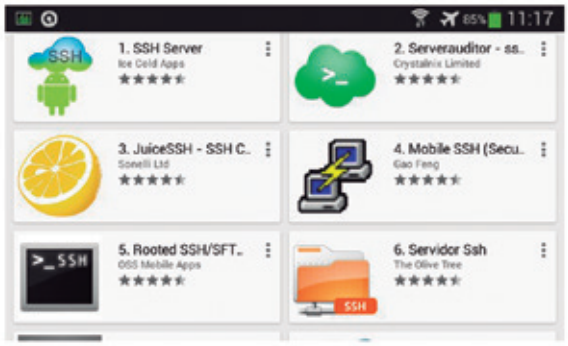


Imagen 1. Distintas versiones de servidores y clientes SSH disponibles para Android

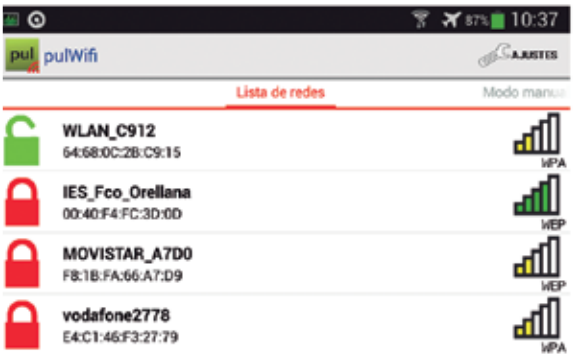


Imagen 2. Programa PulWifi para Android detectando redes nuestro IES

software" en un teléfono, sin que el usuario se percatara de lo que estaba instalando, haciendo uso de códigos QR[CODI]. Existen numerosas aplicaciones gratuitas que nos permiten generar este tipo de códigos de una forma sencilla.

Una vez instalado y configurado el software de control podremos acceder a la máquina objetivo, siempre que se den las condiciones adecuadas. Quizá lo más sencillo para que todo funcione sea trabajar en un entorno de prueba controlado, como puede ser la clase, compartiendo la misma red local mediante una conexión WIFI. Si esto no ocurre, nuestro acceso se puede complicar bastante. Fuera de clase, también es posible acceder a la máquina objetivo a través de una red local si esta se conecta a Internet a través de un punto de acceso WIFI vulnerable, incluso si este está protegido con una clave.

De forma indirecta intentamos conseguir que los alumnos aprendan a proteger sus equipos y sus datos de terceras personas.

Muchos de los puntos de acceso WIFI domésticos existentes en el entorno de nuestro domicilio o de trabajo están mal configurados. Algunos cifran las comunicaciones con una clave que viene de serie, y que en la mayoría de los casos puede ser calculada fácilmente. En otros casos, se utiliza el obsoleto cifrado WEP, en cuyo caso, solo hay que esperar a que alguien utilice esa conexión para capturar paquetes y calcular la clave en un tiempo razonable. Si por el contrario se utilizan cifrados WPA/WPA2 con claves robustas, puede ser muy complicado calcular la clave, salvo en algunos casos en los que se utilicen routers antiguos con tecnología WPS, o bien la configuración de esta no sea la adecuada. En estos casos, puede ser posible realizar un ataque Reaven[VULN] y obtener todos los datos de conexión en un tiempo inferior a 24 horas. Existen numerosos programas que realizan todos estos cálculos[HERR]. Nosotros hemos utilizado la suite WIFISlax para PC[WIFI2] y programas de apoyo adicionales

■ IES Francisco de Orellana (Trujillo).

como PulWIFI para Android[PULW], el cual se muestra en funcionamiento en la imagen 2.

■ Desde el propio IES hicimos un estudio de qué redes WIFI del entorno estaban mal configuradas. **Nos topamos con un dato escalofriante: un 40% de las redes WIFI ubicadas a nuestro alcance desde el instituto eran vulnerables.** Si bien es cierto que no fuimos capaces de encontrar más que 15 redes WIFI con una potencia aceptable, seguramente debido a que la zona no está muy densamente poblada, también es cierto que la muestra es razonablemente representativa.

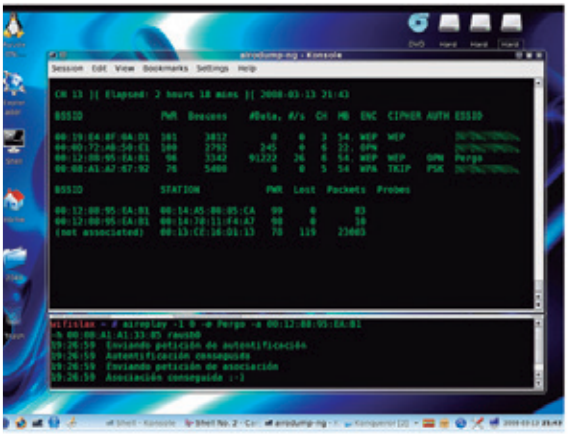
- 4 redes WEP (incluyendo la de nuestro IES y la del CEIP las Américas)
- 8 redes WPA con WPS activo (al menos una claramente débil)
- 1 red WPA con la clave de fábrica activada.

Medidas preventivas a tener en cuenta

El último de los objetivos propuestos para estas clases es que el alumno sepa defenderse de las amenazas tratadas. Esto no va a ser siempre posible, pero al menos, con un poco de sentido común, siguiendo una serie de pautas, podremos evitar la mayoría de estas.

■ Hemos aprendido que la amenaza más peligrosa con la que podemos toparnos parte de la Ingeniería Social, la cual nos convierte a nosotros mismos en el eslabón débil del sistema. Siempre nos encontramos a un solo clic de "meter la pata". Así que debemos ser cautos y desconfiar. No debemos instalar ningún programa de ninguna fuente que no sea de plena confianza, incluso cuando esta proceda de un amigo, de un código QR promocional pegado en un cartel, o de una página vistosa y elegante que nos encontramos navegando por la red. **Debemos usar el sentido común y ser muy conscientes de qué es lo que instalamos, y por qué lo hacemos.**

■ Debemos intentar proteger con algún tipo de clave los aparatos que utilicemos para evitar el acceso físico a los mismos de personas no autorizadas. Además, muchas aplicaciones aparentemente inofensivas que usamos a diario pueden realizan instalaciones de terceros programas en background sin nuestro consentimiento. Es por ello por lo que deberíamos bloquear los sistemas de instalación con algún tipo de clave.



Herramienta de auditoría de redes ejecutada desde WifiSlax

■ Deberíamos instalar en nuestros ordenadores/smartphones algún antivirus, así como algún tipo de firewall a fin de evitar conexiones no deseadas, desde o hacia el software que tenemos funcionando en ellas. Es un poco absurdo, por ejemplo, que un programa "linterna" para el móvil pueda conectarse a Internet. Si no tenemos más remedio que utilizarlo, al menos podremos bloquear sus intentos de conexión, pudiendo evitar así posibles problemas.

■ Debemos proteger nuestros puntos de acceso WIFI mediante el uso de claves poco comunes y distintas a las que vienen de serie en los mismos. También debemos evitar los cifrados WEP, y deshabilitar los cómodos sistemas WPS.

Conclusión

Internet, pese a ser una de las mejores herramientas creadas por el hombre para su desarrollo, está plagada de peligros. Debemos ser conscientes de su existencia, y actuar en todo momento con precaución. Si seguimos las pautas mostradas en este documento, podremos evitar muchas situaciones indeseadas. Es cierto que **nunca estaremos seguros al 100%, pero al menos hay que intentar ponérselo un poco más difícil los delincuentes que quieren aprovecharse de nosotros.** ■

Bibliografía

[CINC] Nota de prensa. "Cinco motivos por los que las trampas de la ingeniería social funcionan". MicroTrend España. http://www.trendmicro.es/newsroom/pr/cinco-motivos-por-los-que-las-trampas-de-la-ingeniera-social-funcionan/

[CODI]Artículo. "Códigos QR: la nueva puerta de entrada para malware en Android". Mónica Tilves. http://www.siliconweek.es/security/virus/codigos-qr-nueva-puerta-de-entrada-para-malware-en-android-15410

[CREO] Congreso "Creo en Internet", Madrid. 11/11/2011. Charla de Chema Alonso (hacker, cómico, profesor y experto en seguridad informática). https://youtu.be/GpXjM0oCSvQ

[CRON] Crónicas (RTVE). 24/May/2013. "Policias y l@drones" http://www.rtve.es/alacarta/videos/cronicas/cronicas-policis-ldrones/1834689/

[GENE] Generador de códigos QR online. http://www.codigos-qr.com/generador-de-codigos-qr/

[HERR] Artículo. "5 herramientas para obtener claves de redes inalámbricas". Neoteo. http://www.neoteo.com/5-herramientas-para-obtener-claves-de-redes-inalambricas/

[INGE] Artículo. "La ingeniería social sigue siendo la amenaza más peligrosa". Bárbara Madariaga. http://xombra.com/index.php?do/noticias/nota/4025/op/4/t/la-ingeniera-social-sigue

[MOVI] Mundo Hacker (Discovery MAX). Capítulo 4. Temporada 1. "Seguridad Móvil". http://mhd004.blob.core.windows.net/mhd004/mundohacker_moviles.mp4

[PREC] La Revolución Virtual (BBC). Capítulo 3. "El precio de lo gratuito". https://youtu.be/9CghMhaNdZI

[PULW] Página oficial de PulWIFI. http://pulWIFI.net/

[SPAM] Mundo Hacker (Discovery MAX). Capítulo 1. Temporada 1. "Spam y phishing". http://mhd001.blob.core.windows.net/mhd001/mundohacker_spam.mp4

[VIRU] Viruslist.com. "Todo sobre Seguridad en Internet" http://www.viruslist.com/sp/hackers

[VULN] Artículo. "Vulnerabilidad en el protocolo WIFI Protected Setup (WPS)". Seguridad para todos. http://www.seguridadparatodos.es/2012/01/vulnerabilidad-en-el-protocolo-wifi.html

[WIFI] Mundo Hacker (Discovery MAX). Capítulo 2. Temporada 1. "Redes WIFI". http://mhd002.blob.core.windows.net/mhd002/mundohacker_WIFI.mp4

[WIFI2] Página oficial de WIFISlax. http://www.WifiSlax.com/