La seguridad cibernética en los adolescentes y su vulnerabilidad al hackeo

José Miguel Cánovas Garay

Tutor:

Vicente Cotanda Rodenas

IES Floridablanca, El infante (Murcia)

A primera vista, se cree que el conocimiento de la seguridad informática en adolescentes es bueno y saben mucho acerca del tema; lo que nos llevaría a concluir que no podrían ser hackeados con facilidad. Mi objetivo es conocer de verdad si los adolescentes realmente tienen un conocimiento acerca de este tema y si saben defenderse ante los peligros de la red. En mis hipótesis planteo totalmente lo contrario, los adolescentes tienen un conocimiento muy por debajo de lo adecuado y el que tienen no lo utilizan como es debido o lo ignoran. Para ello los pondré a prueba mediante un cuestionario, al que más tarde le seguirá un correo falso el cual será mandado a todos los encuestados y por último, una entrevista a un porcentaje para corroborar los datos obtenidos anteriormente cara a cara. Esto nos lleva a los resultados, donde se muestra que los adolescentes realmente tienen un conocimiento por debajo de lo adecuado, revelando la verdadera vulnerabilidad de los adolescentes ante un hackeo o robo de información. La más clara y peligrosa es el uso descuidado de la conexión a redes públicas de wifi gratis, sin saber sin son fiables o no, dejando una total vulnerabilidad a robar datos del dispositivo conectado.

ÍNDICE

1. Introducción
2. Objetivos
3. Marco teórico
4. Metodología
5. Resultados de la investigación
6. Análisis de resultados
7. Conclusiones
8. Webgrafía

1. INTRODUCCIÓN

Mi trabajo de investigación tiene como objetivo descubrir el conocimiento de los adolescentes acerca de la seguridad cibernética y los hackers, así como conocer si los adolescentes toman las medidas necesarias acorde a lo que saben.

He elegido este tema por mi interés de saber qué conocimientos tienen los adolescentes acerca de la seguridad cibernética. Por otro lado, la información que tienen y la responsabilidad de los jóvenes con todas la cuentas y multimedia de los dispositivos que se pueden conectar a internet. No comprender nada de este tema puede ocasionar un problema en el futuro, aunque cada vez el problema puede crearse antes.

El enfoque del trabajo lo he decidido orientar a los centros de secundaria y en concreto a los alumnos de bachillerato, puesto que ellos están en plena adolescencia con un toque de madurez, mayor al de los alumnos de la ESO. Además una parte de los alumnos de bachillerato tienen 18 años por lo que da una mayor bandeja de posibilidades sobre el uso de internet, sin salir de la adolescencia. Todo ello nos lleva a darle un enfoque más amplio respecto a los datos que podemos obtener.

En conclusión, me he decidido por centrar mi trabajo de investigación en conocer el nivel de responsabilidad de los adolescentes, en el ámbito tecnológico, y la vulnerabilidad que tienen

a ser hackeados. Mi interés va enfocado al objetivo de dar a conocer el verdadero conocimiento que tienen respecto al tema o lo que hacen con él, para ver realmente las verdaderas medidas que hay que tomar respecto a este asunto.

2. OBJETIVOS

El objetivo principal de mi tema es demostrar,mis dos hipótesis:

1. Los adolescentes no tienen realmente el conocimiento sobre este tema y tampoco tienen en cuenta las consecuencias de su uso descuidado y sin límites.

2. Los adolescentes no toman los recursos que saben a la hora de utilizar las redes, por lo que la facilidad de obtener datos de ellos o hackearles resulta realmente sencillo.

3. MARCO TEÓRICO

Los jóvenes han nacido en la era de la tecnología y viven completamente rodeados de ella, ¿realmente controlan lo que hacen y lo que les rodea?
La seguridad informática que está a nuestro alcance es muy grande, pero la mayoría de las personas lo ignora o desconoce, por lo que la vulnerabilidad de los adolescentes frente al posible hacking es realmente fácil. ¿Realmente los adolescentes estamos preparados,conocemos y controlamos nuestro entorno digital?¿Estamos seguros frente al intento de violar nuestra seguridad?

Un hacker es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador.
Un hacker en plenitud tiene la capacidad de dominar en un buen porcentaje varios aspectos como: lenguajes de programación, manipulación de hardware & software, telecomunicaciones, y demás; todo esto lo pueden realizar para lucrarse, darse a conocer, por motivación, pasatiempo o para realizar actividades sin fines lucrativos.
Existen dos tipos de hackers principales: los Black Hat y los White Hat.
Los White Hats o hacker éticos se encargan de encontrar vulnerabilidades en un sistema para estudiar y corregir los fallos encontrados. Por otra parte, los Black Hat o ciberdelincuente, son aquellos hackers de sombrero negro que realizan actividades ilícitas para vulnerar y extraer información confidencial, principalmente con un fin monetario. También son creadores de todo tipo de malware.

A nivel empresarial cada vez más empresas mejoran sus defensas frente a los ciberdelincuentes pero en su mayoría estas son las grandes empresas frente a las pequeñas que tan solo una minoría tiene una defensa al menos básica. Todo esto nos lleva al tema de que ya no solo nuestra privacidad e identidad puede ser violada, sino que en un futuro y cada vez más frecuente, el robo digital y los ciberdelincuentes serán más y mejores, así que si ya nuestra seguridad es nula o baja en nuestra adolescencia solo será un peligro para nuestro futuro y seguridad digital, a nivel tanto personal como profesional. Tan solo en España el número de robos está subiendo exponencialmente en las pequeñas empresas debido al nulo conocimiento de seguridad informática, lo que nos lleva a que en un futuro y con el constante avance de la tecnología, será imprescindible un mínimo conocimiento de este tema por seguridad.

Sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54% de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan.

Los grandes Hackers apuntan a grandes proyectos, pero cada vez hay más pequeños Hackers que se centran en pequeños robos, y debido al escaso conocimiento a la seguridad informática en la sociedad lo pueden hacer con una gran facilidad. Lo que lleva a un interés cada vez mayor por este tipo de acciones.

Por otro lado, la vida privada es un espacio personal reservado sólo a unos pocos, familiares y amigos. Forman parte del ámbito privado los datos personales y todo tipo de información personal (texto, imagen, audio, vídeo). “Al menos el 40% de los usuarios de las redes sociales tiene abierto el acceso a su perfil a todo el que pase por ellas, sin restricción alguna de privacidad. Entre los menores de 18 años, este porcentaje se eleva al 77%, según un estudio reciente de la AEPD y el Instituto de Tecnologías de la Comunicación. Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles para cualquier persona. Se desconoce en gran medida que los perfiles pueden ser archivados, facilitando la creación de bases de datos de personas con fines ilícitos y del valor que éstos pueden llegar a alcanzar en el mercado. Por ello, se debe leer toda la información concerniente a la página web. En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos”

4. METODOLOGÍA

Mis métodos de recogida de información se centran en encuestas teóricas, una prueba práctica basada en una simulación de phising y por último una entrevista a un porcentaje de los encuenstados.

El procedimiento de mi investigación consiste en realizar una encuesta online pero en acto presencial a diversas clases de 1º y 2º de Bachillerato, para saber el conocimiento que tienen sobre la seguridad informática. Luego una prueba de simulación de phising para contrastar los resultados de la teoría, con una prueba práctica a los participantes de la encuesta anterior y terminando con una entrevista para contrastar todos los datos con respuestas cara a cara en una entrevista semiabierta acerca de su conocimiento de la seguridad informática.

La población y muestra de mi estudio está comprendida en los alumnos del IES FLORIDABLANCA de 1º y 2º de bachillerato de las cuatro modalidades educativas, con edades comprendidas entre 15 y 18 años, para realizarles la prueba, el cuestionario y la entrevista para conseguir los datos.

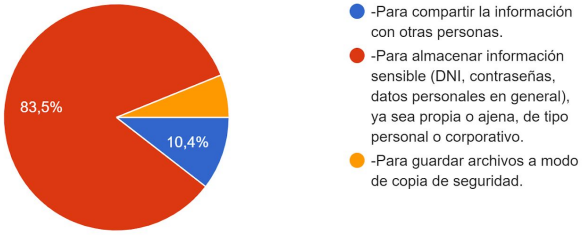
Mis instrumentos son “formularios de google” para mi cuestionario y por otro lado una página para crear mi correo falso y las estadísticas de él, para el phising y así realizar una prueba de campo. Y por último Word y Excel para la entrevista y el análisis de los resultados.

5. RESULTADOS DE LA INVESTIGACIÓN

El cuestionario mencionado anteriormente, contiene respuestas de opción múltiple y verdadero o falso para tener datos generales acerca del conocimiento de los alumnos sobre la seguridad informática.

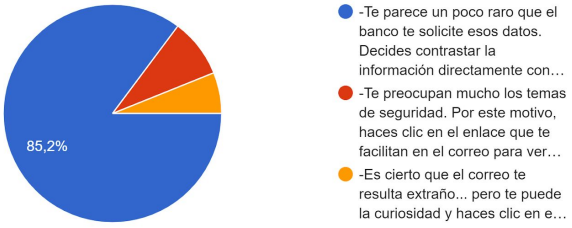
En primer lugar, vamos a representar las respuestas con porcentajes de los adolescentes a cada pregunta, incluyendo la pregunta en cada una.

Pregunta 1: En qué casos no se recomienda hacer uso de la nube
115 respuestas

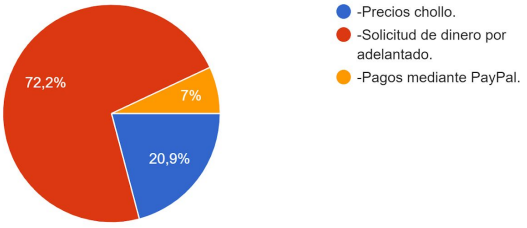


Pregunta 2: Las redes sociales son un servicio que te permiten estar en contacto con otras personas, por eso...
115 respuestas

Pregunta 3: Recibes este correo de tu banco en el que te solicita confirmar tus datos personales y bancarios de manera...supuestamente por motivos de seguridad
115 respuestas

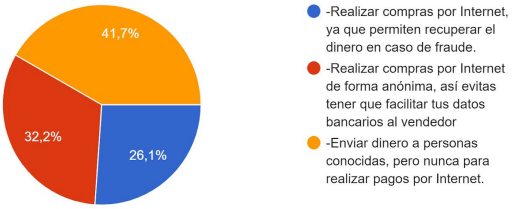


Pregunta 4: ¿Qué indicios deben hacerte sospechar sobre un posible anuncio fraudulento publicado en una página web?
115 respuestas

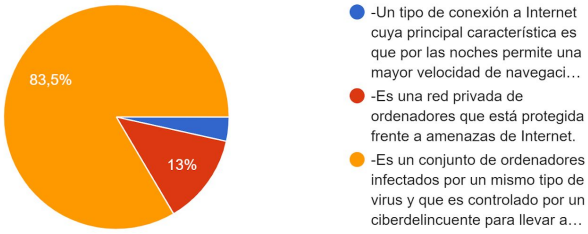


Pregunta 5: ¿Qué protocolo de seguridad debe tener configurado el router WiFi de tu casa?
115 respuestas

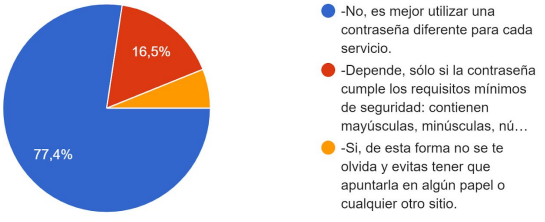
Pregunta 6: El uso de empresas de envío de dinero instantáneo se debe utilizar para
115 respuestas



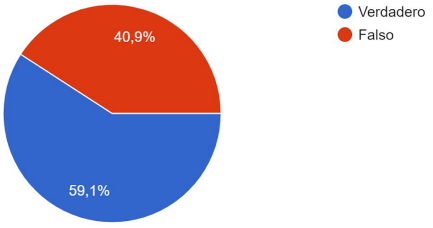
Pregunta 7: ¿Qué es una red zombi?
115 respuestas



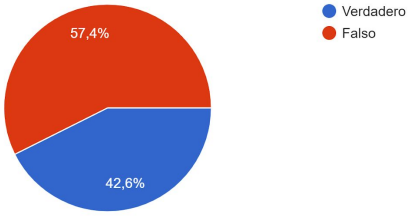
Pregunta 8: ¿Es una buena práctica utilizar la misma contraseña para acceder a varios servicios de Internet?
115 respuestas



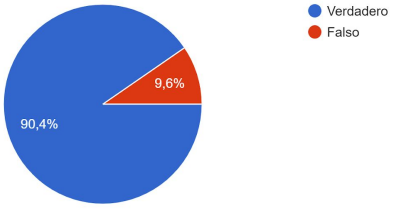
Pregunta 9: Las redes WIFI públicas que están protegidas con un nombre de usuario y contraseña son seguras. Las pe...o requieren un proceso de autenticación.
115 respuestas



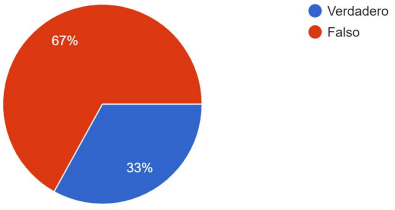
Pregunta 10: Si alguien entra en nuestro router y se conecta a nuestra red WIFI, no podemos acceder legalmente a sus carpetas compartidas.
115 respuestas



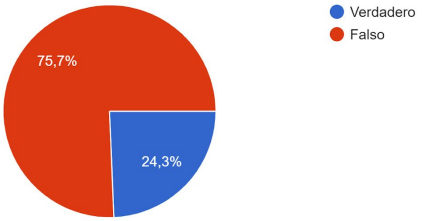
Pregunta 11: Un virus podría colarse en tu ordenador simplemente visitando una página.
115 respuestas



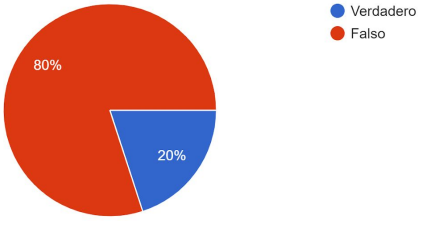
Pregunta 12: El antivirus es la única herramienta de seguridad capaz de proteger tus dispositivos de todos los riesgos que circulan por Internet.
115 respuestas



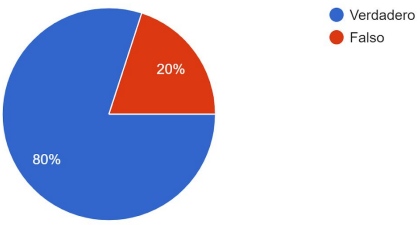
Pregunta 13: Cuantos más programas antivirus tengas instalados el ordenador, mejor. Menos virus se colarán en él.
115 respuestas



Pregunta 14: Los únicos ordenadores que no se ven afectados por virus son los de Apple, por eso los fabricantes de antiv...ridad para los dispositivos de esa marca.
115 respuestas



Pregunta 15: Si la web donde vas a comprar te muestra en el navegador un icono de candado y su URL empieza por HTTPS, si... tus datos viajarán cifrados por la Red.
115 respuestas



A continuación, el correo falso me dio estadísticas concretas:

Los resultados de la entrevista, la cual ha sido realizada a un 10% de los encuestados, es de tipo semi abierta, por lo que he cogido las respuestas de cada persona y las he transformado en variables, para así poder sacar estadísticas. Aquí están las preguntas con el porcentaje de cada respuesta.

Pregunta 1: ¿En qué casos no se recomienda hacer uso de la nube?

-Cosas privadas /75%
-Para nada (sube cualquier cosa) /10%
-Depende de la nube a la que se suba /15%

Pregunta 2: ¿Qué haces al ver un correo sospechoso en tu bandeja de entrada?

-Ignorarlo/ 80%
-Pinchar en el enlace para saber más /10%
-Preguntar a terceros antes de hacer nada /10%

Pregunta 3: ¿Qué haces si ves un anuncio en una página web que te interesa?

-Ignorarlo/ 85%
-Buscarlo directamente desde la página oficial /15%

Pregunta 4: ¿Qué protocolo de seguridad debe tener configurado el router WiFi de tu casa?

-Conocimiento nulo/ 90%
-Conocimiento acerca del protocolo de seguridad /10%

Pregunta 5: ¿Compras online?

-Nada /30%
-Si, personalmente /20%
-Si, pero a partir de otros /50%

Pregunta 6: ¿Usas la misma contraseña en todas las cuentas?

-Si, la misma /40%
-Una contraseña general pero con variantes en cada sitio /40%
-No, diferentes /20%

Pregunta 7: ¿Cuántas horas dedicas al día a usar internet?

- Una media de 6 horas

Pregunta 8: ¿Qué elementos están en tu perfil? (En orden de más a menos utilizadas)

-Nombre -Foto -Provincia

Pregunta 9: Conocimiento acerca de los virus

-Nulo conocimiento, dependencia de un antivirus o terceras personas /80%
-Conocimiento bajo, sigue dependiendo un poco del antivirus /15%
-Conocimiento medio, no depende del antivirus (sabe prevenir virus y identificarlos) /5%

Pregunta 10: ¿Qué idea tienes acerca de los hackers?

-Son malos, se dedican a robar /25%
-Se distinguen en buenos y malos según para quién trabajen y sus intenciones /75%

Pregunta 11: ¿A cuántas redes sociales estás apuntado que uses con frecuencia? (Por orden de popularidad)

-Instagram -Twitter -Snapchat

Pregunta 12: ¿Te conectas a las redes públicas que desconoces?

-Me meto a cualquiera si es gratis /35%
-Me meto si pone un nombre oficial /40%
-No me meto por seguridad /25%

Pregunta 13:¿Aparte de dar wifi, existe algún otro uso de este?

-Conocimiento nulo /80%
-Pasar datos de un dispositivo a otro /20%

Pregunta 14: Información que contiene tu móvil (Por orden de popularidad)

-Cuentas -Correo -Conversaciones -Fotos íntimas -Cuenta bancaria<10%

Pregunta 15: N.4 ¿Con qué dispositivo te conectas internet?
-Con móvil y ordenador indistintamente

6. ANÁLISIS DE RESULTADOS

Para comprobar si nuestras hipótesis enunciadas anteriormente son verdaderas o falsas, vamos a comparar los resultados más relevantes de cada parte de la investigación, y así comprobar el conocimiento real de los adolescentes y qué hacen con él.

Lo primero de todo, relacionando la segunda pregunta de la entrevista con la tercera pregunta de la encuesta, se saca en relación que los adolescentes saben distinguir correos falsos y por lo tanto lo ignoran. Pero estos resultados teóricos son muy diferentes a la práctica que hice mediante mi correo, el cual dio estadísticas donde de 24 personas que leyeron el correo, 14 de ellas, más del 50% abrió el enlace del susodicho correo, esto nos lleva a la undécima pregunta del cuestionario, en la cual, el 90% de las personas son conscientes de que al entrar en una página pueden ser hackeadas o se les puede introducir un virus.

El correo específico:

Además, tenemos la siguiente relación, en la octava pregunta de la encuesta más del 70% de las personas afirmaban que la mejor opción era tener una contraseña diferente para cada cosa, pero al llegar a la sexta pregunta de la entrevista el 80% de las personas admitían que ponían la misma contraseña para todo o con alguna variante como una letra o un número.

Por otra parte, la siguiente relación que vamos a ver es acerca del wifi, se puede observar que tanto en la quinta pregunta de la encuesta como en la cuarta y decimotercera pregunta de la entrevista el conocimiento acerca del wifi es deficiente, los que nos lleva a lo siguiente: En la novena y décima pregunta de la encuesta las personas se dividen en 60%/40% acerca de la legalidad y la seguridad que puede tener un wifi, a pesar de este desconocimiento el 35% de las personas se mete a cualquier red pública y el 40% se mete si pone un nombre oficial, lo que asegura en lo más mínimo que sea fiable, esto se ve reflejado en la duodécima pregunta de la entrevista.

Por último, las 4 preguntas finales de mi test están relacionadas con los virus, y de ellas he podido evaluar que la mayoría de las personas teóricamente saben acerca de ellos y cómo identificarlos, pero después en la entrevista en su novena pregunta,al preguntar acerca de los virus, la mayoría de adolescentes admiten que su conocimiento prácticamente es nulo y solo saben de su existencia, lo que los hace depender totalmente de un antivirus donde el de la mayoría es uno gratuito o de prueba para defender su ordenador, ya que ellos no sabrían identificarlo ni erradicarlo.

7.CONCLUSIONES

Podemos ver que en el análisis de datos se han confirmado mis hipótesis, los adolescentes creen tener conocimiento suficiente, y controlar la tecnología que les rodea; pero la realidad es que los adolescentes tienen conocimientos por debajo del necesario y el que tienen, lo ignoran, dejándolos expuestos a cualquier tipo de hackeo.

En el correo falso se puede ver claramente el problema. Ellos creen saber identificarlo y no caer en la trampa, pero más del 50% de estos pincharon en el enlace sin dudarlo más de una vez, lo que deja ver claramente que aunque sepan identificarlo o no, los adolescentes caen en la trampa, pudiendo llegar a causar graves problemas ahora y en un futuro.

El siguiente problema son las contraseñas, los adolescentes son conscientes de que lo idóneo es una diferente para cada cosa, pero aún así más del 70% pone la misma contraseña en todas sus cuentas o con una variable. Teniendo en cuenta la gran cantidad de cuentas que se hacen, para todo usar la misma es claramente un peligro, debido que a si se sabe una se saben todas y eso puede llegar a falsificación de identidad o robo de datos.

El problema más grande y peligroso es acerca del wifi, el desconocimiento de su usos y lo que puede llegar a hacer es muy grave, el 75% de los adolescentes se mete en redes públicas de wifi sin estar seguros de que es fiable, esto ya no solo deja abierta el robo de cuentas si no todos los datos del dispositivo con el que te conectes, lo que engloba multimedia, cuentas, datos privados o cuentas bancarias. El uso despreocupado de esta medida para no gastar datos o tener wifi gratis, puede llegar a tener consecuencias muy graves y cada vez más, el dispositivo móvil cada vez guarda más información personal e importante, y si no tenemos el debido cuidado, puede caer en manos equivocadas sin mucha dificultad.

El último problema es el desconocimiento general acerca de los virus, las únicas personas que tienen algún tipo de conocimiento acerca de esto, son las personas que cursan o han cursado la asignatura de informática. El resto de personas tienen un conocimiento nulo acerca de ellos, dejándolos totalmente expuestos a cualquier tipo de hackeo sin ellos saberlo. Por otra parte la cada vez mayor dependencia de un antivirus, les quita la necesidad de saber defenderse por ellos mismos de un ataque, el cual puede hacerse igualmente; Además, hay que valorar que la mayoría de los adolescentes usan un antivirus gratis o de prueba, lo que realmente no protege el ordenador ante un ataque.

La conclusión final que he alcanzado con este trabajo de investigación es que, efectivamente, los adolescentes tienen un conocimiento acerca de la seguridad informática por debajo de lo que deberían; lo que los deja expuestos a ser hackeados sin mucha dificultad, y si cada vez dependemos más de la tecnología, y guardamos más información en nuestros dispositivos, deberíamos tener unos mínimos conocimientos para protegernos ante posibles ataques o no dejarnos expuestos a ellos. La despreocupación de este tema, y la poca importancia que se le da sólo puede acabar en desgracia para los afectados, y el “ a mi eso no me va a pasar”, se va a convertir en “si hubiera sabido que esto de verdad podía pasar”.

8. WEBGRAFÍA

Oficina de seguridad del internauta.
https://www.osi.es/es

Acerca de las contraseñas:
https://www.osi.es/es/campanas/contrasenas-seguras

Acerca de las redes sociales:
https://www.osi.es/es/campanas/redes-sociales

Acerca del wifi:
https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil

Estudio sobre la privacidad en el uso de las redes sociales de Internet.
http://e-spacio.uned.es/fez/eserv/bibliuned:masterComEdred-JIgarcia/Documento.pdf

Panorama actual de la ciberseguridad en España.
https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Todo sobre el hackeo.
https://es.malwarebytes.com/hacker/