rutaEle

ficha introductoria

nombre de la actividad	Nos espían. Licencia Safe Creative nº 1406121224018.
autor/es	Adriana REPILA RUIZ.
nivel y destinatarios	B2.
duración	Dos horas y media.
objetivos	Sensibilizar a los estudiantes con el tema del ciberespionaje a través de los ordenadores y los teléfonos inteligentes. Debatir acerca de los límites de lo moralmente aceptable cuando se trata de espiar a terceros.
destrezas	Comprensión oral y escrita y expresión oral.
contenidos funcionales, léxicos y gramaticales	Vocabulario relacionado con la informática y los teléfonos inteligentes.
dinámica	Individual, parejas y pequeños grupos.
material y recursos	Fotocopias de la actividad, artículo de prensa y vídeo de la entrevista.
secuenciación	En esta actividad se trata el tema del ciberespionaje a través de los ordenadores y los teléfonos inteligentes. Para empezar, se pide a los estudiantes que comenten en grupos de tres las preguntas del primer ejercicio. Si el profesor lo desea, se puede hacer una breve puesta en común en clase abierta. A continuación, el profesor les formula las dos cuestiones del apartado 2a y les pide que elaboren una lista de medidas y precauciones que se pueden tomar para evitar que nuestros datos personales caigan en manos de terceros. Transcurridos cinco minutos, se hace una puesta en común y el profesor anota las sugerencias de los estudiantes en la pizarra. Después, leen el artículo de prensa que se les propone y comparan su lista con las medidas que aconseja el autor del artículo. Una vez comentadas las coincidencias, comentan de nuevo en pequeños grupos cuáles de las herramientas del artículo conocen, qué medidas ponen ellos en práctica y si han tenido alguna mala experiencia relacionada con el tema. Finalmente, realizan un ejercicio de vocabulario que consiste en buscar un sinónimo para una serie de palabras extraídas del texto. Una posible solución sería: filón económico: buen negocio (3er párrafo); escudándose: protegiéndose, defendiéndose, justificándose (4º párrafo); neutralice: elimine, evite, detenga (párrafo "Protección contra virus y troyanos"); rastreo: seguimiento (párrafo "Bucear por Internet de incógnito"); disponen de: tienen (párrafo "Bucear por Internet de incógnito");

secuenciación

precavidos: cautos, cuidadosos (párrafo "Borrar el rastro"); terceros: otras personas (párrafo "¿Huellas dactilares?"); monitorizados: vigilados, observados, controlados (párrafo "Subirse a la nube"); perogrullada: obviedad (párrafo "Sentido común y más formación").

A continuación, el profesor les anuncia que van a ver un fragmento del programa de televisión "Salvados", concretamente una entrevista de Jordi Évole a Chema Alonso, un importante hacker informático a nivel internacional. Antes del visionado, los alumnos realizan otro ejercicio de vocabulario con expresiones y términos que van a escuchar en la entrevista. Las soluciones son: 1e, 2k, 3a, 4h, 5c, 6i, 7b, 8d, 9f, 10g, 11j.
Una vez corregido el ejercicio, los estudiantes leen las preguntas de comprensión a las que tienen que contestar y se visiona el vídeo. En principio, al tratarse de una entrevista de dieciséis minutos, bastaría con verlo una sola vez, ya que un segundo visionado podría alargar en exceso la tarea. No obstante, si el profesor lo considera oportuno, puede volver a ponerlo o bien invitarlos a que lo vean de nuevo en sus casas. En cualquier caso, tras el primer visionado los alumnos comparan en parejas sus respuestas y se ponen en común después en clase abierta. La soluciones se encuentran en el anexo I.

Para terminar, en grupos de tres o cuatro personas comentan las preguntas del apartado 4a. Transcurrido el tiempo suficiente, el profesor les pide que lean entonces el apartado b y lo comenten también. Finalmente, se hace una puesta en común en clase abierta y se debate acerca de la cuestión principal: ¿Es posible establecer un límite sobre lo moralmente aceptable?

Las imágenes están tomadas de la galería de www.pixabay.com y pertenecen a: Geralt (ordenador con estetoscopio); Open Clips (espía y cámara de vídeo); y PublicDomainPictures (móvil con corazón).

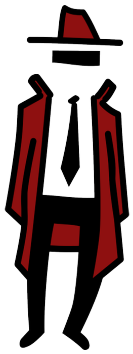
Adriana Repila Ruiz

NOS ESPÍAN...

1. Comenta con tu compañero las siguientes cuestiones:

¿Tienes un *smartphone*? ¿Para qué lo utilizas? ¿En qué lugares? ¿Qué aplicaciones usas con más frecuencia? Si tienes un ordenador portátil, ¿sueles usarlo fuera de casa? ¿Te conectas a las redes wifi públicas y abiertas?

2. Seguro que has oído hablar de la privacidad en internet y la protección de datos.



a) ¿Crees que la gente es consciente de hasta qué punto expone su vida al público? ¿Y tú, también lo eres? En parejas, haced una lista de las medidas y precauciones que se pueden tomar para evitar que otros puedan acceder a nuestra información personal.

b) Lee el siguiente artículo del periódico *20 minutos* y compara tu lista con la suya.

http://www.20minutos.es/noticia/1968724/0/privacidad/espionaje/internet/

c) ¿Hay alguna coincidencia? ¿Conocías ya algunas de las herramientas que aconsejan utilizar? ¿Pones en práctica las medidas que nos recomiendan? ¿Has tenido alguna mala experiencia por no tomar las precauciones necesarias?

d) A continuación, sustituye las palabras en negrita extraídas del texto por otras que no alteren el significado de la frase:

Han encontrado un **filón económico**...	
...**escudándose** en el argumento...	
...un antivirus que **neutralice** los ataques...	
Para evitar el **rastreo**...	
Todos estos navegadores **disponen de** sistemas...	
...en caso de no haber sido lo suficientemente **precavidos**.	
...vayan a parar a manos de **terceros.**	
...servicios como DropBox estén siendo **monitorizados**.	
...otra **perogrullada**...	

3. Vamos a visionar un fragmento del programa *Salvados* que emite la cadena de televisión *La Sexta*. Jordi Évole, director y presentador del programa, entrevista a Chema Alonso, un importante *hacker* informático a nivel internacional.

a) Antes de ver el vídeo, relaciona las siguientes palabras que vas a escuchar con su significado:

1. Difamación	a. Ser castigado o regañado.
2. Velcro	b. Contraseña.
3. Caerle a alguien un puro (coloquial)	c. Atractivo, aliciente.
4. Pillar a alguien (coloquial)	d. Fingir ser otra persona, suplantar su identidad.
5. Anzuelo	e. Calumnia; acción de desacreditar a alguien.
6. Aplicar un filtro	f. Fragilidad, debilidad.
7. Clave	g. Ser el que dirige, gobierna o manipula, generalmente con algún interés.
8. Hacerse pasar por alguien	h. Sorprender a alguien haciendo algo que no debe.
9. Vulnerabilidad	i. Hacer una selección.
10. Mover los hilos (coloquial)	j. Contagiar.
11. Inocular un virus	k. Sistema de cierre formado por dos tiras de tejidos diferentes que se enganchan.

b) A continuación, ve el vídeo y contesta a las preguntas siguientes:

1. ¿A qué se dedican los auténticos *hackers* según el entrevistado? ¿Qué nombres reciben los "*hackers* malos"?

….....
.....
.....
.....

2. ¿Qué peticiones recibe a menudo Chema Alonso?

….....
.....

3. ¿Cuál es una de las manera más fáciles de *hackear* a alguien?

….....
.....

4. ¿Qué tipo de prácticas ilegales puede llevar a cabo un *cibercriminal* después de haber accedido a los datos de una persona en *Facebook*, por ejemplo?

….....
.....

5. Según él, ¿es necesario tener una amplia formación y conocimientos en informática para saber acceder a los datos de alguien? ¿Por qué?

….....
.....

6. ¿Es posible correr los mismos peligros si estamos conectados a la red privada de nuestra casa? ¿Por qué?

….....
.....
.....

7. ¿Para qué pone un velcro en su ordenador?

….....
.....

8. Según Chema, para espiar un móvil hay que instalarle un virus o un troyano antes. ¿Cómo es posible hacerlo? ¿Cómo se consigue dicho virus?

….....
.....
.....
.....

9. ¿Qué hecho paradójico existe en cuanto a la legalidad de vender y usar este tipo de virus?

….....
.....
.....

10. ¿Por qué se corre más peligro con los *smartphones*?

.....
.....

11. ¿Quién puede estar detrás de este tipo de prácticas? ¿Cuál es su principal motivación?

.....
.....

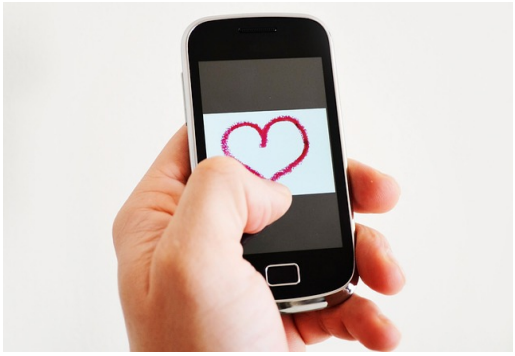
12. ¿Qué utilidad puede encontrar un pederasta?

.....
.....

4. ¿Dónde está el límite de lo moralmente aceptable?

a) Comentad en grupos las siguientes cuestiones:

- ¿Con qué objetivos crees que los gobiernos espían a sus ciudadanos? ¿Te parece lícito que lo hagan?
- En muchas empresas es habitual controlar las páginas de Internet por las que los empleados navegan, o incluso los correos electrónicos que envían desde sus cuentas corporativas. ¿Te parece lícito que lo hagan?
- Imagina que tu pareja se deja abierta su sesión de correo electrónico, o se olvida su móvil en casa. ¿Te parecería aceptable revisar sus mensajes?



b) Imagina ahora que, gracias a dicho espionaje, el gobierno de tu país consigue destapar una red de tráfico infantil; o que una empresa averigua que un empleado le está haciendo competencia desleal; o que, motivado/a por los celos, lees los *whatsApp* de tu pareja y descubres que te está siendo infiel. ¿Cambiaría en algo tus respuestas anteriores? ¿Qué conclusiones se podrían sacar sobre los límites de lo moralmente aceptable?

Anexo I: Respuestas a las preguntas

1. Se dedican a investigar la tecnología, intentar llevarla más allá de los límites, encontrar los fallos de seguridad e intentar arreglarlos. Los *hackers* malos reciben el nombre de criminales, cibercriminales y piratas informáticos.

2. Recibe peticiones de gente que quiere *hackear* a su vecino, a su mujer o a su empleado.

3. Levantar una red wifi libre y gratuita.

4. Ver su facebook, robar su identidad, difamar a la persona, cambiar los permisos de configuración y hacer públicos sus mensajes.

5. No es necesaria una formación amplia porque en internet se pueden encontrar muchos vídeos, tutoriales, conferencias, herramientas y documentos que te enseñan a hacerlo.

6. Sí, es posible si la red wifi o el dispositivo de conexión no están bien configurados. Entran dentro del router y hacen la misma operación.

7. Pone un velcro para tapar su webcam y que no le graben.

8. Se envía un correo con una aplicación no oficial y, al descargarse e instalarse en el móvil, se instala también el virus. Dicho virus se puede conseguir a través de una empresa que los vende por Internet, aunque también existen herramientas gratuitas menos elaboradas.

9. La paradoja es que Internet es global, pero la legislación es local, por ese motivo vender esos productos es legal, aunque en determinados países es totalmente ilegal usar sus servicios, como por ejemplo en España.

10. Es más peligroso porque la gente no es consciente de que lleva un ordenador encima donde expone constantemente sus datos personales.

11. Pueden ser desde gente amateur que busca simplemente probar y curiosear, hasta auténticas bandas del cibercrimen. Su motivación principal es el dinero, el cual consiguen traficando con la intimidad de las personas.

12. Un pederasta puede comprar un vídeo de un niño chateando con su ordenador y utilizarlo para poder suplantar su identidad y ganarse la confianza de otro niño.