Formación: Seguridad: Protección de la salud y el bienestar en entornos digitales y el ciberacoso

Título	Seguridad: Proteger la salud y el bienestar online
Palabras clave	Seguridad, ciberseguridad, entorno digital, bienestar
Proporcionado	Learning for integration (LFI), Finlandia
por	
Idioma	Español
Objetivos/ Metas/ Resultados de aprendizaje	 Ser capaz de entender el concepto de salud y bienestar digital Ser capaz de comprender y evitar los riesgos para la salud y el bienestar físico y psicológico derivados del uso de las tecnologías digitales. Ser capaz de entender el concepto de acoso cibernético y protegerse a sí mismo y a los demás de posibles peligros en los entornos digitales (ciberacoso) Ser capaz de comprender y ser consciente del bienestar y la inclusión en las redes sociales
Área de	1. Información y alfabetización mediática
competencia	Competencias ☑ Alfabetización mediática ☐ Navegar, buscar y filtrar datos, información y contenido digital
	2. Comunicación y Colaboración
	Competencias
	☐ Comprometer a la ciudadanía a través de las tecnologías digitales ☐ Interactuar con las tecnologías digitales para el entretenimiento y la cultura
	3. Creación de contenido digital
	Competencias
	☐ Desarrollar contenido digital
	4. Seguridad
	Competencias
	☐ Proteger el medioambiente
	☐ Prevenir y reconocer las noticias falsas
	☑ Proteger la salud y el bienestar
	5. Resolución de problemas <u>Competencias</u>
	☐ Uso creativo de las tecnologías digitales
	El área de competencia principal del módulo "Seguridad: Proteger la salud y el bienestar" se mencionan con más detalle en el DigiComp 2.2. como puede ver en la imagen 1.

DIMENSION 1: COMPETENCE AREA 4. SAFETY explain ways to how to avoid threats to my physical and psychological health related with the use of technology. DIMENSION 2: COMPETENCE 4.3: PROTECTING HEALTH AND WELL-BEING To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies. To psychological well-being white using urginal recurring upon be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of digital As well as guiding others, I can: . apply different ways to protect myself and others from dangers in digital technologies for social well-being and social inclusion. DIMENSION 3: PROFICIENCY LEVEL At advanced level, according to my own needs and those of others, and in complex contexts At basic level and with guidance, I can: differentiate simple ways to avoid health risks and threats to physical and psychological well-being while using digital technologies.
 select simple ways to protect myself from possible danges in digital environments.
 identify simple digital technologies for social well-being and social inclusion. adapt the most appropriate ways to protect myself and others from dangers in digital Highly Specialised level 7 A basic level and with autonomy and appropriate guidance where needed, I can:

differentiate simple ways to avoid health risks and threats to physical and
psychological well-being while using digital technologies.

select simple ways to protect myself from possible dangers in digital environments. At highly specialised level. I can: create solutions to complex problems with limited definition that are related
 considered breakth winder, and threats to well-hains while using digital technologies. to avoiding health-risks and threats to well-being while using digital technologies, to protect self and others from dangers in digital environments, and to the use of digital technologies for social well-being aid social riskclaim.

Integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting health. identify simple digital technologies for social well-being and social inclusion. explain well-defined and routine ways to how to avoid health risks and threats to physical and psychological well-being while using digital technologies.
 select well-defined and routine ways to protect myself from dangers in digital Highly Specialised level 8 At the most advanced and specialised level, I can: create solutions to solve complex problems with many interacting factors Imagen 1. Área de competencia: Seguridad: Proteger la salud y el bienestar, 2022 Este módulo introduce los conceptos de seguridad, salud y bienestar al Descripción usar entornos digitales y tecnológicos. Además, el módulo se centra en la importancia del uso de los entornos digitales y tecnológicos y en cómo evitar no utilizar algunos entornos digitales y redes sociales. INTRODUCCIÓN Contenido UNIDAD 1. ¿Cómo estar seguro en Internet? ¿Qué es el bienestar en los entornos digitales y el ciberacoso? UNIDAD 2. ¿Qué es el ciberacoso? UNIDAD 3. ¿Cómo prevenir el ciberacoso? CONCLUSIÓN Unidades/Secci INTRODUCCIÓN El módulo desarrolla el área de competencia 4.3 de DigiComp2.2, ones proteger la salud y el bienestar evitando riesgos para la salud y el bienestar físico y psicológico al utilizar tecnologías digitales, identificar e indicar formas bien definidas y rutinarias de protegerse del peligro en entornos digitales y utilizando herramientas digitales para el bienestar y la inclusión social. En resumen, según DigComp2.2, la competencia 4.3 se refiere a una capacidad individual de mantener y promocionar la propia salud física, emocional y mental, así como la salud y el bienestar de los demás. En este contexto, "proteger" se refiere a las medidas adecuadas para prevenir daño, minimizar los riesgos, y promocionar resultados positivos para la salud. Eso puede implicar mantener hábitos de salud como hacer ejercicio regularmente, nutrición equilibrada y dormir suficientemente,

así cómo buscar atención médica cuando sea necesario y tomar medidas para prevenir la propagación de enfermedades.

Además, proteger la salud y el bienestar implica también promover un bienestar social y emocional positivo manteniendo relaciones sanas, buscando apoyo cuando se necesita y desarrollando habilidades de afrontamiento para gestionar el estrés y los retos.

El módulo pretende concienciar de que algunas herramientas digitales pueden crear oportunidades para participar en las sociedades que pueden contribuir al aislamiento y a la exclusión de la vida social de algunos grupos vulnerables (por ejemplo, ancianos, niños, personas con necesidades especiales, así como otros grupos que carecen de las competencias digitales). Por tanto, el módulo se centra en entender el uso de varios entornos digitales, saber cómo usar y seguir las instrucciones de seguridad y protegerse, por ejemplo, del ciberacoso, aprender cómo centrarse en el bienestar físico y mental y evitar los impactos negativos de los medios digitales.



Imagen 2. Seguridad: Día Internacional contra el ciberacoso, 2021.

UNIDAD 1. ¿Cómo estar seguro en Internet? ¿Qué es el bienestar en los entornos digitales y el ciberacoso?

Sección 1. Los conceptos básicos de seguridad, salud y bienestar en los entornos digitales y el ciberacoso

¿Cómo estar seguro en internet? Empezamos viendo un video sobre el tema proporcionado por el British Council:

Video 1. ¿Estás seguro en internet? https://www.youtube.com/watch?v=MH8myE0l2po

Cómo podemos ver en el video, las preguntas dirigidas a los profesores para estar seguros en internet son bastante cruciales, por ejemplo:

¿Has buscado a ti mismo en Google?

- ¿Cuántas imágenes publicas?
- ¿Aceptas las solicitudes de amistad de gente que no conoces?
- ¿Te has registrado en algún lugar usando las redes sociales?

¿Qué son la seguridad, la salud y el bienestar en los entornos digitales?

Protección y bienestar significan poder evitar riesgos para la salud y amenazas para el bienestar físico y psicológico mientras se utilizan las tecnologías digitales. Ser capaz de protegerse a sí mismo y a los demás de posibles peligros en los entornos digitales, como robo de identidad, ciberacoso, acoso, suplantación de identidad etc. y ser consciente de las tecnologías digitales para el bienestar social y la inclusión social.

En otras palabras, salud y bienestar significan:

- Proteger el entorno digital
- Prevenir y reconocer las noticias falsas
- Proteger la salud y el bienestar del entorno digital

El ciberacoso es una de las mayores amenazas que especialmente los jóvenes pueden encontrar online. Se analizará más en la Unidad 2.



Imagen 3. Día Internacional contra el acoso y el ciberacoso, 2021

En la imagen 3, podemos ver consejos de seguridad que los padres pueden comprobar para que sus hijos se sienten seguros en internet. Los consejos se dieron durante el Día Internacional contra el acoso escolar:

- Estar informado, al día y alerta
- Conocer las herramientas, los riesgos y las reglas
- Utilizar herramientas de protección online
- Fomentar el pensamiento crítico

- Configurar internet para un uso seguro
- Aprender sobre las redes sociales
- Entender los juegos y las aplicaciones
- Entender la violencia online
- Confiar, investir tiempo, monitorear y educar
- Practicar lo que se predica

Sección 2: ¿Qué es importante para mantener la seguridad y el bienestar tecnológico digital?

Es muy importante mantener la seguridad y el bienestar tecnológico digital porque 1) si se ignora, la situación empeorará, y 2) la responsabilidad de establecer medidas de seguridad y responder al uso inadecuado de la tecnología es de los padres, los educadores o las fuerzas del orden.

"En consecuencia, los incidentes de ciberacoso se tratan muchas veces de manera muy formal o informal y a veces se gestionan mal." (Patchin, J.W, Hinduja, S. 2021).

En base a estos hechos, necesitamos crear un entorno para que los jóvenes puedan hablar cómodamente con los adultos sobre los problemas de ciberacoso a que se enfrentan y que se sientan cómodos al trabajar juntos para resolver los problemas y obtener buenos resultados (Patchin, J.W, Hinduja, S. (2021).

Por tanto, lo más importante es que las escuelas eduquen la comunidad escolar sobre el uso responsable de internet, discutan los problemas relacionados con la comunicación online y utilicen regularmente la tecnología.

Además, el papel de los padres debería ser:

- Cultivar y mantener una línea de comunicación abierta con sus hijos
- Discutir los problemas y los retos
- Supervisar la situación y el comportamiento online tanto como offline, por ejemplo, controlar la experiencia en internet y el software
- Educar a sus hijos online tanto como offline

UNIDAD 2: ¿Qué es el ciberacoso?

El ciberacoso es el acoso que tiene lugar a través de dispositivos digitales, como móviles, ordenadores y tabletas. El ciberacoso puede ocurrir a través de SMS, textos, y aplicaciones, u online en las redes sociales, fórums, o juegos donde la gente puede ver, participar o compartir contenido.

El ciberacoso incluye enviar, postar o compartir contenido negativo, dañino, falso o mezquino sobre otra persona. Incluso se puede compartir información personal o privada sobre alguien más, causando vergüenza o humillación. Algunos ciberacosos cruzan la línea del comportamiento ilegal o criminal.

(Patchin, J.W, Hinduja, S. (2021)

Los entornos más comunes en los que ocurre el ciberacoso son:

- 1. Redes sociales, como Facebook, Instagram, Snapchat, Tik-Tok etc.
- 2. Mensajes de texto y aplicaciones de mensajería en los dispositivos móviles y tabletas
- 3. Mensajería instantánea, mensajes directos y chat online a través de internet
- 4. Fórums online, chats y tablones de anuncios, como Reddit
- 5. Correos
- 6. Comunidades de juegos online

Según el estudio sobre el ciberacoso de Patchin, J.W, y Hinduja, S. (2021), hay algunas razones más comunes por las que la gente acosa a los demás, por ejemplo:

- <u>Se utiliza como mecanismo de afrontamiento y respuesta a algo</u> estresante que está ocurriendo en sus vidas
- <u>Porque ellos son inseguros y están tratando de desviar la atención</u> de ellos mismos centrándose en alguien más
- <u>Pueden sentirse celosos, en lugar de entenderlo, se han convertido</u> en maltratadores
- Porque están preocupados que no vendrán aceptados por sus compañeros si no lo hacen

Algunas preguntas que considerar:

- ¿Cómo se puede diferenciar el ciberacoso de otras formas de acoso?
- ¿Alguien que conozcas o tú tenéis experiencias de ciberacoso?
- ¿Qué lo hace peor que otras formas de acoso?
- ¿Por qué la gente acosa o ciberacosa?

Veamos algunos videos sobre el ciberacoso:

https://www.stopbullying.gov/videos-social-media

Reflexiona sobre las siguientes preguntas:

- 1. ¿Qué piensas sobre los temas del video?
- 2. ¿Estás de acuerdo con las sugerencias que aporta?
- 3. ¿Es relevante para tus estudiantes? ¿Es un recurso útil para ser compartido con tus estudiantes?

4. ¿Querrías añadir algo al video?

En la práctica:

• Prueba Cyber Buddy – La aplicación contra el acoso

Cyber Buddy es una aplicación para el móvil que puede ser descargada en el Play Store (para Android) o en App Store (para iPhone). La aplicación ofrece información, enlaces a los recursos, videos y actividades en relación con el ciberacoso. Puedes buscar y descargar la aplicación para Android o iPhone:

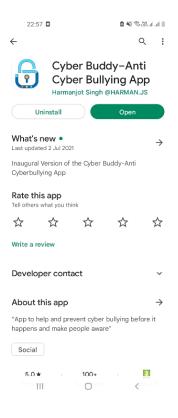
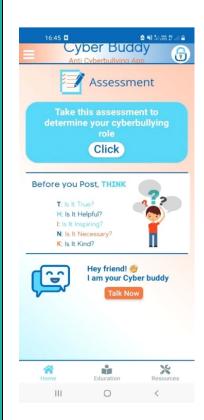


Imagen 4

Cuando empiezas a utilizar la aplicación, puedes realizar una evaluación sobre tu relación con el ciberacoso. Hay también mucha información sobre el ciberacoso en la sección sobre la educación y más recursos en la sección Recursos. Esta aplicación ofrece también actividades para ayudar a enfrentarse al ciberacoso.





Imágenes 4, 5, 6. La evaluación, Qué saber sobre el ciberacoso y los recursos de la aplicación Cyber Buddy.

Piensa en tu experiencia utilizando la aplicación:

- ¿La aplicación ha sido útil y fácil de usar?
- ¿Crees que entiendes qué es el ciberacoso?
- ¿Cuáles son las cosas principales que has aprendido sobre el ciberacoso?
- ¿Sabías que el ciberacoso es tan común?

UNIDAD 3. ¿Cómo prevenir el ciberacoso?

Hay una serie de medidas que la gente puede tomar para prevenir el ciberacoso y otras amenazas online. Lo más importante es establecer un control de privacidad, búscate en Google, nunca abras mensajes, correos etc. de fuentes que no conoces, crea una contraseña fuerte y no compartas tu contraseña con nadie, establezcas herramientas de seguridad y software que te ayuden a protegerte de las amenazas de ciberseguridad. (Patchin, J.W, Hinduja, S. 2021).

En caso de ciberacoso, no debes intentar enfrentarlo solo. Debes hablarlo con amigos, profesores o profesionales. Recuerda, no estás solo, mucha gente tiene experiencias relacionadas con el ciberacoso.

A continuación, hay unas reglas para prevenir el ciberacoso:

- 1. APRENDE. Para evitar que se produzca el ciberacoso debes entender qué es exactamente, investigar en qué consiste, al igual que cómo y dónde es más probable que se produzca. Entonces es bueno que hables con tus amigos sobre lo que estás viendo y experimentando.
- 2. PROTEGE TUS CONTRASEÑAS. Salvaguarda tus contraseñas y otra información privada de miradas indiscretas. Nunca dejes la contraseña u otros datos identificativos donde los demás puedan verlos. Además, nunca des esta información a nadie, ni siquiera a tu mejor amigo. Si otros la saben, itómate el tiempo de cambiarla ahora!
- 3. MANTEN FOTOS PG". Antes de postar o enviar esa imagen tuya, ten en cuenta si es algo que querrías que vieran tus padres, tus abuelos y el resto del mundo. Los que quieren hacerte daño, pueden utilizar esa imagen como munición para hacerte la vida imposible.
- 4. NUNCA ABRAS MENSAJES NO IDENTIFICADOS O NO SOLICITADOS. Nunca abras mensajes (correos, mensajes de texto, mensajes en Facebook, etc.) de gente que no conoces, o de los que sabes que a menudo acosan a los demás. Bórralos sin leerlos. Pueden contener virus que infectan tus dispositivos, si los abres. Además, nunca cliques en enlaces a las páginas enviados por personas que no conoces. Estos también pueden contener virus diseñados para recolectar tus informaciones privadas y personales, o instalar un backdoor en tu dispositivo.
- 5. CIERRA LA SESIÓN DE LAS CUENTAS ONLINE. No guardes las contraseñas en los campos de formularios de sitios web o en tu navegador por comodidad, y no permanezcas conectado cuando te alejes del ordenador o del móvil. No des a nadie la más mínima oportunidad de hacerse pasar por ti en internet a través de tu dispositivo. Si olvidas cerrar la sesión de Twitter cuando utilizas el ordenador de la biblioteca, la siguiente persona que utilice el ordenador podría entrar en tu cuenta y causarte problemas significativos.
- 6. HAZ UNA PAUSA ANTES DE PUBLICAR. No subas nada que pueda comprometer tu reputación. La gente te juzgará según cómo aparezcas online. Además, te darán o negarán oportunidades (trabajo, becas, prácticas) basándose en eso.

- 7. AUMENTA LA SENSIBILIZACIÓN. Inicia un movimiento, crea un club, haz una campaña u organiza un acto para concienciar sobre el ciberacoso. Aunque entiendes lo que es, sólo cuando los demás también lo sepan podremos evitarlo de verdad.
- 8. CONFIGURA LOS CONTROLES DE SEGURIDAD. Restringe el acceso a tu perfil online sólo a amigos de confianza. La mayoría de las redes sociales como Facebook e Instagram ofrecen la posibilidad de compartir cierta información sólo con los amigos, pero estos ajustes deben configurarse de manera que puedan garantizar la máxima protección. Además "no aceptes solicitudes de amistad de Snapchat de cualquiera".
- 9. BÚSCATE EN GOOGLE. Busca regularmente tu nombre en los principales motores de búsqueda (por ejemplo, Google, Bing, Yahoo). Si aparece alguna información o contenido personal que pueda ser utilizado por alguien para dirigirse a ti, toma medidas para eliminarlo antes de que se convierta en un problema.
- 10. NO ACOSES A LOS DEMÁS. Trata a los demás como te gustaría que te trataran a ti.

(Source: Hinduja, S. & Patchin, J.W. (2018). Preventing cyberbullying: Top ten tips for teens. Cyberbullying Research Center. Retrieved [10.08.2022], from https://cyberbullying.org/Top-Ten-Tips-Teens-Prevention.pdf)

Hoy en día, varias plataformas de redes sociales ofrecen y tienen integradas formas de proteger y minimizar los riesgos a los que las personas pueden enfrentarse online. Por ejemplo, la página web de HP ofrece información y formas de protegerte del ciberacoso: según la página principal de HP, las mejores formas para protegerse del ciberacoso son:

- 1. Gestiona los ajustes de privacidad,
- 2. Mantén registros claros,
- 3. Bloquea a los ciberacosadores mediante la configuración del usuario
- 4. Pregunta por sí mismo
- 5. Ponte en contacto con las fuerzas del orden si te sientes amenazado. (HP, 2023)

Para concluir, para prevenir el ciberacoso debe existir una comunicación clara y una supervisión online entre padres, hijos, educadores y otro personal escolar. Por tanto, los padres deben hablar con sus hijos, educarlos y controlar sus actividades online. Deben controlar también sus contraseñas online, los ajustes de seguridad y privacidad. Los niños

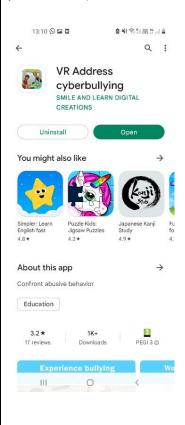
deben ser precavidos e informar de cualquier problema que tengan a sus padres, al personal de la escuela y a los profesores. Como resultado, podemos ayudar a los niños a prevenir el ciberacoso y a estar más seguros en la red, y animarlos a ser más empáticos y a desarrollar una inteligencia emocional más fuerte. (Universidad de Ohio, 2023).

Además, para que los adultos puedan prevenir el ciberacoso, deben ser conscientes de su comportamiento online y dedicar tiempo a reflexionar sobre el impacto de lo que publican y comparten en las redes sociales, así como tener presente el paso mencionado anteriormente.

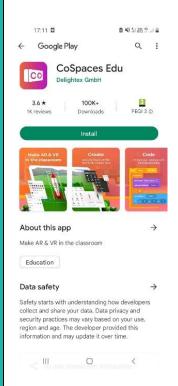
Herramientas y recursos sobre el ciberacoso

Además de los presentados anteriormente, hay muchas herramientas, juegos y recursos disponibles sobre el tema del ciberacoso.

VR Address Cyberbullying es un juego interactivo para móviles al que se puede acceder en un dispositivo móvil a través de Play Store (solo para Android). La idea del juego es seguir la trama e interactuar cuando se le pida. El jugador participa en la historia y puede tomar decisiones en función de la situación. Esto aumenta su empatía hacia los acosados, y en la última parte aprenden métodos para resolver situaciones de ciberacoso. También pueden moverse por el entorno de RA a través de su aplicación. Busca y descarga la aplicación para Android (no disponible para iPhone):



Cómo afrontar el ciberacoso es un juego interactivo online al que se puede acceder online o en un dispositivo móvil. El alumno debe registrarse primero en la plataforma CoSpaces Edu en su ordenador portátil o, si utiliza un dispositivo móvil, debe descargar la aplicación CoSpaces Edu en Play Store (para Android) o App Store (para iPhone).



Puedes jugar también en tu ordenador a través de este enlace: https://edu.cospaces.io/KTP-NBQ



A continuación, puedes encontrar información sobre como asistir a cursos sobre la seguridad en los entornos digitales:

https://www.coursera.org/learn/the-science-of-well-being

https://mydigiskills.eu/test/

https://www.alldigitalweek.eu/useful-tools/

Glosario

Ciberacoso: Daños intencionados y repetidos infligidos mediante el uso de ordenadores, teléfonos móviles y otros dispositivos electrónicos.

(5 términos del glosario)	Ciberespacio: El "universo" electrónico creado por las redes informáticas en el que los individuos interactúan. Ciberstalking: Acoso reiterado mediante dispositivos electrónicos y tecnología en red. Influencer: Persona capaz de convencer al público a través de una plataforma digital y del marketing en las redes sociales.
Autoevaluación (preguntas de elección múltiple)	 ¿Qué es el ciberacoso? a) Daños intencionados y repetidos infligidos mediante el uso de ordenadores, teléfonos móviles y otros dispositivos electrónicos. b) Daños involuntarios causados por el uso de ordenadores, teléfonos móviles y otros dispositivos electrónicos. ¿Qué es Cyber Buddy? a) Es una aplicación que ofrece información, enlaces a recursos, vídeos y actividades sobre el ciberacoso b) Se trata de una aplicación que ofrece información, enlaces a recursos, vídeos y actividades sobre diversas noticias c) Es un sitio web de noticias fiables ¿Dónde se produce principalmente el ciberacoso? a) Medios de comunicación, como los periódicos b) Redes sociales, como Facebook, Instagram, Snapchat y Tik-Tok c) Principalmente en Facebook ¿Cómo prevenir el ciberacoso y las amenazas online? a) Utiliza las mismas contraseñas en todas tus cuentas online b) Establezcas un control de privacidad, no abras nunca mensajes, correos electrónicos, etc., de fuentes que no reconozcas. c) Sólo aceptes solicitudes de amistad si tienes amigos en común
Recursos	Aquí puedes hacer otro cuestionario para mejorar tus conocimientos sobre el ciberacoso: https://cyberbullying.org/quiz-research 1. British Council homepage. A course on cybersecurity, 2022. https://study-uk.britishcouncil.org/plan-studies/choosing-course/subjects/cyber-security

2. British Council homepage. A course on data"You and your data".

PPT relacionado	
Material relacionado	Hinduja, S. and Patchin, J.W. (2021). Cyberbullying Identification, Prevention and Response. Cyberbullying Research Centre, 2021 Available in www format at: cyberbullying.org
	9. Vuorikari, R., Kluzer, S., Punie, Y. (2022). DigComp 2.2. The Digital Competence Framework for Citizens. With <i>new examples of knowledge, skills and attitudes.</i> Joint Research Center, 2022.
	8. Ohio University homepage, (2023). Available in www format at: https://onlinemasters.ohio.edu/online-msw-program/complete-guide-to-preventing-cyberbullying/
	7. International Day againsts byllying and cyberbullying at school. Picture 2, 2021. Available at: https://htxt.co.za/tag/international-day-against-violence-and-bullying-at-school-including-cyberbullying/
	6. Glossary: Social media, Cyberbullying and Online Safety glossary. Cyberbullying Research Centre. Available in www format: https://cyberbullying.org/social-media-cyberbullying-and-online-safety-glossary
	5. HP, homepage of HP. (2023). Available in www format at: https://www.hp.com/ca-en/shop/offer.aspx?p=best-ways-to-prevent-cyber-bullying-online
	4. Hinduja, S. & Patchin, J.W. (2018). Preventing cyberbullying: Top ten tips for teens. Cyberbullying Research Center. Retrieved [10.08.2022], from: https://cyberbullying.org/Top-Ten-Tips-Teens-Prevention.pdf
	3. Hinduja, S., Patchin J., W. 2021. Cyberbullying: Identification, Prevention and Response. 2021 Edition. Available in www format at: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
	2022 https://learnenglish.britishcouncil.org/general-english/magazine- zone/you-your-data