# CONSEJOS PARA LOS/AS FORMADORES/AS - PRIVACIDAD Y ÉTICA

## ORIENTAR

**Consejos para los/as formadores/as:** Esta actividad puede llevarse a cabo tanto directamente con estudiantes como con docentes. Las instrucciones para los formadores o docentes en esta parte considerarán ambos escenarios. Por lo tanto, en esta parte se puede referir a los/as alumnos/as como profesores/as participantes o estudiantes y el/la formador/a puede ser el propio docente cuando la actividad se realiza en un aula.

Al principio, se presenta el contexto de "Google nos espía". Pregunta a los/as participantes si han oído estas afirmaciones antes, y en qué contextos, y si tienen pruebas para creer en ellas. A continuación, presenta el caso del espionaje de Google a través de los routers no encriptados: *https://www.wired.com/2012/05/google-wifi-fcc-investigation/*, *https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data*

Puedes preguntar a los/as participantes si entienden el contenido y sus implicaciones preguntándoles qué saben sobre los routers y la encriptación. Proporciona las explicaciones adecuadas en caso de que sea necesario, según los conocimientos y la edad de los/as participantes (docentes o alumnos/as).

A continuación, pregunta a los/as participantes (docentes o alumnos/as) si saben a qué tipo de información se puede acceder desde las WiFis detectadas (como se hizo en las actividades Let's STEAM anteriores).

Puedes invitar a los/as participantes a realizar una pequeña lluvia de ideas sobre el tipo de información que comparten en línea. (*Opcional: Discute con los/as participantes cómo podrían evitar que alguien tenga acceso a la información que transfiere a través de su WiFi y presente brevemente los diferentes protocolos de cifrado. Intenta prever si el WiFi se ha detectado con actividades anteriores de Let's STEAM*).

## CONCEPTUALIZAR

**Consejos para los/as formadores**: El/a formador/a presenta a los/as participantes que la información que se comparte a través de los routers puede obtenerse a partir de la actividad de utilizar Internet con diferentes fines.

El/a formador/a puede plantear a los/as participantes diferentes preguntas para desencadenar el debate sobre los posibles riesgos del uso de Internet, como:

- **¿Para qué utilizas Internet? ¿Qué búsquedas haces? ¿Qué páginas visitas?**
- **¿Sueles aceptar las cookies? ¿Por qué? (si es necesario, explica brevemente a los/as participantes qué son las cookies y sus usos).**
- **¿Sabes qué tipo de información se comparte (y se puede almacenar sobre ti), cuando navegas por internet? (ejemplos: Ubicación, Fecha // Año de nacimiento, Número de móvil, Dirección de correo electrónico, Género, Información personal...)**
- **¿Cómo puedes saber qué datos sobre ti se han almacenado? Si los/as participantes son docentes, también se puedes orientar el debate hacia el tipo de datos que sus alumnos/as comparten en Internet.**

También se anima a los/as formadores a revisar la política de privacidad de los recursos de Internet que han utilizado en actividades anteriores de Let's STEAM, como Scratch. Intenta dirigir la discusión hacia si saben qué tipo de información se almacena y los propósitos del almacenamiento de esta información. También, si están de acuerdo o no con los propósitos del uso, cómo les hace sentir y qué acciones podrían considerar llevar a cabo en consecuencia. Después de unos minutos, intenta hacer una lista con los alumnos clasificando los tipos de información que se pueden almacenar al utilizar Internet en función de su riesgo potencial (daño/sensibilidad).

Esta hoja de actividades forma parte del proyecto Let's STEAM, financiado con el apoyo de la Comisión Europea a través del programa Erasmus + Asociación Estratégica. Su contenido refleja únicamente la opinión del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en ella. Esta obra está autorizada bajo la licencia Creative Commons Attribution-ShareAlike 4.0 International License.

Cofinanciado por el programa Erasmus+ de la Unión Europea

# CONSEJOS PARA LOS/AS FORMADORES/AS - PRIVACIDAD Y ÉTICA

## INVESTIGAR

**Consejos para los/as formadores**: Se pedirá a los/as participantes que busquen sus nombres completos en Internet. Ved los resultados que aparecen. Pregunta a los/as participantes (docentes o estudiantes): **¿Crees que los resultados reflejan quién eres y/o lo que haces? ¿Cómo? ¿Qué imagen de ti proyecta esa información? Invita a los/as participantes a buscar a uno o dos amigos/as cercanos/as (o compañeros que ya conozcan). Discute con ellos: ¿Crees que los resultados reflejan quiénes son y/o lo que hacen? ¿Has contribuido a que haya más información sobre ellos/as en Internet? ¿Cómo? ¿Qué información crees que comparten tus amigos/as sobre ti?** Los/as participantes pueden actualizar la lista de tipos de información y riesgos potenciales si es necesario. (opcional) Anima a los/as estudiantes a evaluar de nuevo el impacto de compartir información sensible que puede poner fácilmente en riesgo su privacidad y seguridad si se comparte por error, por desconsideración o por indicaciones engañosas. Sigue fomentando el debate con nuevas preguntas: **¿Crees que compartir información es bueno? ¿Hay algún ejemplo de intercambio positivo en Internet? ¿Y los negativos? ¿Crees que has dado tu consentimiento para compartir esta información? ¿Has recibido alguna vez un correo electrónico o una llamada de spam sin saber cómo tenían tus datos?** El objetivo es que los/as participantes sean más conscientes de los riesgos potenciales de compartir información, especialmente la sensible. También se pueden introducir retos y oportunidades más amplios a nivel social en relación con la privacidad y la seguridad en la era de la Internet de las cosas (internet of things), la comercialización de los datos, las necesidades de regulación y normalización de arriba a abajo y de abajo a arriba, etc. Internet lo sabe todo y nunca olvida, por lo que también es necesario contar con normas para el derecho al olvido. El contenido publicado en línea puede durar para siempre y puede ser compartido públicamente por cualquiera.

Siendo conscientes de la sobreexposición de los datos privados en los entornos online, se invitará a los/as participantes a identificar las mejores prácticas para reducir los riesgos a la hora de compartir información y mantener la privacidad de los datos personales online. Por ejemplo: ¿Qué acciones podríamos llevar a cabo para mantener nuestra información privada? (¿Es mejor tener un perfil público en las redes sociales o un perfil privado? // descargar cualquier aplicación de la AppStore // navegar en internet con la cuenta de Google...). Para ello, los/as participantes trabajarán en grupos de 3 o 4 personas identificando 10 acciones diferentes. Como formador/a, intenta fomentar el diálogo propiciando diferentes situaciones como, por ejemplo:

- **Quieres añadir a tu amigo/a íntimo/a a un chat de grupo.**
- **Haces una foto divertida del perro de tu vecino y quieres publicarla en Internet.**
- **Acabas de tener un/a nuevo/a novio/a y quieres cambiar el estado de tu relación.**
- **Ves a alguien dormido en el autobús y quieres hacer una foto y compartirla en línea.**
- **Quieres compartir tu ubicación y etiquetar a tus amigos/as.**
- **Encuentras una vieja foto tuya y de tu hermano/a y quieres compartirla en línea.**
- **Quieres desearle a tu amigo/a un feliz cumpleaños publicándolo en su cuenta de las redes sociales.**
- **Te envían una foto tuya y de un/a amigo/a y te ves muy bien en ella. A tu amigo/a no le gusta, pero tú quieres publicarla en línea de todos modos.**
- **Estás de vacaciones con tu familia y quieres compartir una foto y etiquetarlos en ella junto con el lugar donde os alojáis.**

Trainees can search on the Internet for other examples if needed it.

Después, el grupo de 3 o 4 participantes se fusionará con otro grupo pequeño, tratando de identificar qué directrices son similares entre los grupos y fusionarlas y discutir la relevancia de las diferentes directrices tratando de ordenarlas de más a menos relevantes. Este procedimiento puede repetirse en diferentes momentos para llegar a un consenso con todo el grupo.

## CONCLUIR

**Consejos para los/as formadores:** Discutir con todo el grupo las acciones/mejores prácticas más importantes para reducir la exposición de datos privados. Además, puedes pedir a los/as docentes que elaboren infografías con estas directrices para distribuirlas a otros/as compañeros/as de otros grupos.