



MÓDULO 5

CIBERSEGURIDAD Y SEGURIDAD EN LÍNEA



erasmediah.eu



**Co-funded by
the European Union**



Lección 5.2

Protección de la información personal y la privacidad en línea



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

Lección 5.2

Protección de la información personal y la privacidad en línea

Objetivos:

- Concientizar sobre los riesgos de compartir información personal en línea y cómo ésta puede ser utilizada indebidamente.
- Proporcionar a los estudiantes estrategias prácticas para controlar su huella digital, incluidas configuraciones de privacidad de datos, comunicación segura y evitar compartir información excesiva.
- Explorar ejemplos de violaciones de la privacidad, demostrando su impacto en las personas y cómo podrían haberse evitado.
- Inspirar un comportamiento proactivo mediante la creación de hábitos como revisar los permisos de las aplicaciones, comprender los términos del servicio y utilizar herramientas de privacidad.

Mensaje(s) clave:

- Toda la información que compartes en línea, desde fotos y "me gusta" hasta datos de ubicación, puede ser explotada por ciberdelincuentes o empresas. Saber cómo limitar el acceso es tu primera línea de defensa.
- Proteger tu privacidad no se trata de evitar internet; se trata de ser inteligente y premeditado. Herramientas y decisiones sencillas pueden mantener tus datos seguros sin sacrificar tu vida digital.



TIPO DE LECCIÓN:





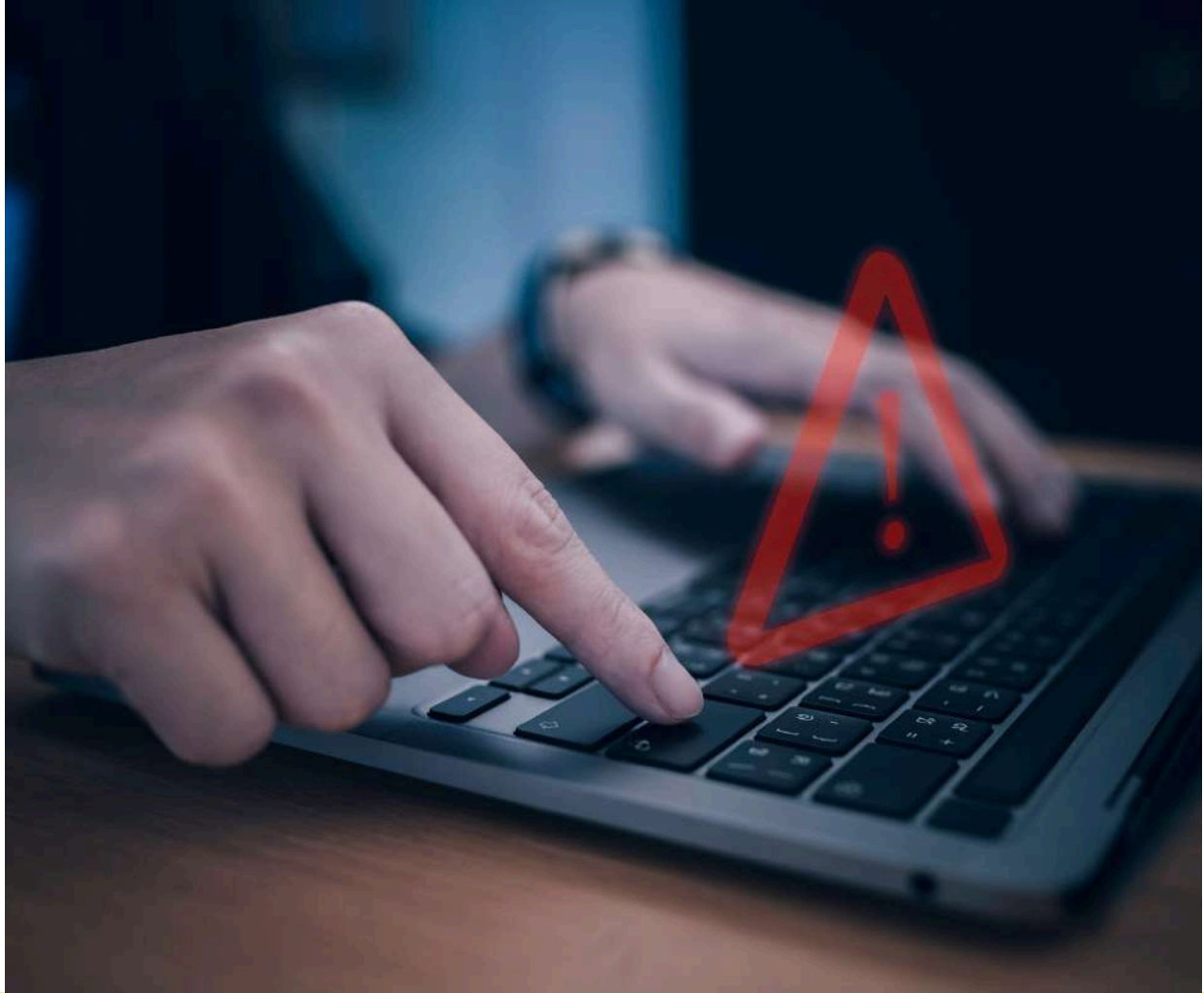
Descripción general de la lección

Con gran parte de nuestras vidas transcurriendo en línea, mantener la información personal segura nunca ha sido tan importante. Esta lección destaca la importancia de proteger tu privacidad.

Exploraremos cómo hábitos simples, como compartir demasiado en redes sociales o aceptar permisos de aplicaciones sin pensar, pueden exponer tus datos. Al reconocer estos riesgos y adoptar estrategias prácticas, obtendrás las herramientas para proteger tu identidad digital y tomar el control de tu seguridad en línea.

El taller está organizado en 4 pasos:

- 1: Introducción a los riesgos de la privacidad en línea (15 min)
- 2: Explorando violaciones de privacidad en el mundo real (10 min)
- 3: Estrategias prácticas para proteger la información personal (10 min)
- 4: Reflexión final y conclusiones clave (5 min)



Paso 1

Introducción a los riesgos de la privacidad en línea

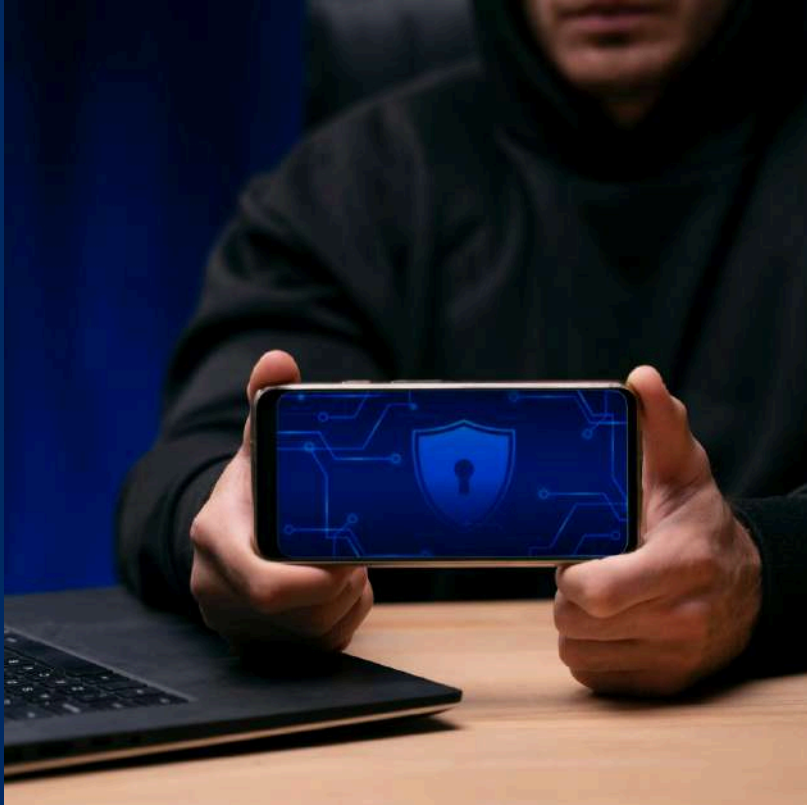
¿Alguna vez descargaste una nueva aplicación, aceptaste sus permisos y nunca te detuviste a pensar qué información está recopilando?

Cuando usamos internet, nuestros datos personales, como ubicación, contraseñas y hábitos de navegación, pueden quedar expuestos fácilmente. A continuación, exploraremos los riesgos de privacidad existentes y cómo podrían afectarte.

Como primer paso, lea la sección “Amenazas comunes a la privacidad en línea” de este artículo: builtin.com/articles

Mientras lee, escriba algunas palabras en una hoja de papel:

- La amenaza a la privacidad que le resulta más preocupante y por qué esta amenaza le resulta relevante o peligrosa.



Paso 1

Introducción a los riesgos de la privacidad en línea

Una vez que hayas terminado de leer, analicemos:

- ¿Qué amenaza a la privacidad te sorprendió más y por qué?
- ¿Cómo crees que estas amenazas afectan nuestra vida cotidiana?
- ¿Qué podría pasar si los ignoramos?

No dudes en compartir un ejemplo rápido de tu experiencia, ya sea sobre contraseñas débiles, rastreo de datos o cualquier otra cosa que hayas visto o escuchado. Si no estás seguro, ¡escuchar a otros te dará ideas!



Paso 2

Explorando violaciones de privacidad en el mundo real

Analicemos un ejemplo real de lo que sucede cuando no tenemos cuidado con nuestra información personal en línea.

Imagínate esto: A Sarah le encanta compartir su vida en redes sociales. Publica fotos de su nuevo apartamento, habla de sus rutinas diarias e incluso comparte su ubicación cuando está en su cafetería favorita. Un día, Sarah descubre que le han vaciado la cuenta bancaria. ¿Cómo? Un ciberdelincuente recopiló su información personal a partir de sus publicaciones públicas (su ubicación, sus hábitos de vida e incluso pistas sobre sus contraseñas) para acceder a sus cuentas. ¡Todo por compartir demasiado!

Ahora, piense en las siguientes preguntas:

- ¿Qué salió mal? ¿Qué acciones o hábitos provocaron la vulneración de la privacidad?
- ¿Cómo se podría haber evitado esta situación? ¿Qué cambios sencillos habrían marcado la diferencia?

Escribe tus respuestas y prepárate para compartirlas con el grupo.



Paso 2

Explorando violaciones de privacidad en el mundo real

Hablemos de ello juntos:

- ¿Qué cree usted que salió mal en la situación de Sarah?
- ¿Por qué cree usted que violaciones de la privacidad como ésta ocurren tan fácilmente?

Al final, tómate un momento para pensar:

- ¿Tú o alguien que conoces ha tenido algún problema de privacidad en línea? Podría ser un correo electrónico sospechoso, una cuenta pirateada o compartir demasiada información en redes sociales.
- ¿Cómo sucedió y cuál fue el resultado?

Si te sientes cómodo, comparte tu historia con el grupo. Si no, no hay problema: el simple hecho de escuchar te dará información valiosa.



Paso 3

Estrategias prácticas para proteger la información personal

Ahora que hemos explorado los riesgos de la privacidad y ejemplos del mundo real, centrémonos en los pasos prácticos para protegernos (nuestros datos) en línea.

Comenzaremos con un video rápido: <https://youtu.be/6WQzMAd6mJs>

Preste atención a los consejos clave compartidos.

Después de ver el video, anota tres acciones específicas que puedes tomar para mejorar tu privacidad en línea. Piensa en:

- Ajustar la configuración de privacidad en sus cuentas de redes sociales.
- Revisar los permisos de las aplicaciones en su teléfono.
- Ser cauteloso con la información personal que comparte en línea, especialmente en plataformas públicas.



Paso 3

Estrategias prácticas para proteger la información personal

Ahora, compartamos una estrategia que planeas implementar. Por ejemplo:

- “Esta noche revisaré todas las aplicaciones de mi teléfono y eliminaré las que no uso”
- Limitaré quién puede ver mis publicaciones de Facebook/Instagram y desactivaré la visibilidad pública de mi perfil.

Vamos a discutir:

1. ¿Qué hace que estos hábitos de privacidad parezcan fáciles o difíciles de adoptar?
 - ¿Nos sentimos demasiado cómodos compartiendo información en línea?
 - ¿Pensamos que las configuraciones de privacidad y los permisos son confusos o consumen mucho tiempo?
2. ¿Por qué tantas personas ignoran prácticas simples de privacidad, incluso cuando conocen los riesgos?
 - ¿Será porque no creen que les vaya a ocurrir una vulneración?
 - ¿Crees que es porque la gente no es consciente de las herramientas o hábitos que debería utilizar?
3. ¿Cómo puedes mantenerte motivado para mantener estos hábitos?
 - Por ejemplo, configurar recordatorios para actualizar las contraseñas o revisar periódicamente la configuración de las redes sociales.

Paso 4

Reflexión final y conclusiones clave

Para finalizar este taller, tomemos un momento para reflexionar sobre lo que hemos aprendido y pensar en cómo podemos aplicarlo en nuestra vida diaria.

Pregúntate: ¿Qué hábito puedes cambiar hoy para mejorar tu privacidad en línea? Podría ser algo sencillo, como desactivar la opción de compartir ubicación, revisar la configuración de privacidad de tus redes sociales o ser más precavido con lo que publicas. Ahora, piensa en cómo puedes ayudar a los demás: ¿Cómo compartirás lo que has aprendido hoy con un amigo, familiar o compañero? Incluso pequeños consejos, como explicar por qué es importante usar contraseñas seguras o enseñar a alguien a revisar los permisos de las aplicaciones, pueden marcar una gran diferencia.





Resumen de las conclusiones clave

- Tenga cuidado con lo que comparte en línea: los pequeños detalles, como ubicaciones o hábitos, pueden usarse incorrectamente si caen en las manos equivocadas.
- Revise y ajuste la configuración de privacidad: revise periódicamente sus redes sociales, los permisos de las aplicaciones y la configuración de la cuenta para limitar el intercambio innecesario de datos.
- Limite la información personal que publica públicamente: evite compartir detalles confidenciales como direcciones, rutinas o identificadores personales en las redes sociales u otras plataformas.
- Tenga cuidado con las aplicaciones y los enlaces: piense antes de hacer clic en enlaces, descargar aplicaciones u otorgar permisos: confíe solo en fuentes verificadas.
- Comience con pequeños pasos: hábitos simples, como desactivar el seguimiento de ubicación o limitar las publicaciones públicas, pueden tener un gran impacto en la protección de su privacidad.



Instrucciones para trabajadores juveniles, educadores y

Objetivo:

El objetivo de esta lección es brindar a los participantes habilidades y conocimientos prácticos para proteger su información personal y mantener su privacidad en línea. Mediante actividades interactivas, ejemplos reales y debates reflexivos, los participantes identificarán los riesgos comunes para la privacidad en línea, comprenderán el impacto de las violaciones de la privacidad y desarrollarán estrategias prácticas para proteger sus datos. Al finalizar la sesión, los participantes se sentirán más conscientes, preparados y comprometidos a adoptar hábitos que mejoren su seguridad digital.

Materiales necesarios:

- Conexión a Internet para reproducción de vídeo o artículos
- Proyector y pantalla
- Oradores
- Acceso a herramientas de ciberseguridad recomendadas
- Papel gráfico o marcadores de pizarra blanca
- Bolígrafos, lápices y hojas de notas





Paso 1: Introducción a los riesgos de la privacidad en línea (15 min)

1. Empieza con una pregunta que se relacione con tu experiencia: "¿Cuándo fue la última vez que descargaste una aplicación, aceptaste sus permisos o compartiste una publicación en línea? ¿Te detuviste a pensar en qué información personal podrías estar revelando?". Explica que estas pequeñas acciones cotidianas pueden exponer involuntariamente información privada como la ubicación, los hábitos de navegación o las rutinas personales a terceros o ciberdelincuentes.

2. Enfatiza que proteger tus datos personales es esencial en el mundo digital actual. Resalta que comportamientos aparentemente inofensivos, como compartir una foto o permitir que las aplicaciones accedan a tus contactos, pueden tener consecuencias imprevistas. Usa una analogía sencilla: «Tu información personal es como las piezas de un rompecabezas. Una sola pieza puede parecer inofensiva, pero al combinarse con otras, puede revelar mucho sobre ti».

3. Actividad: lectura de artículos y reflexión

Distribuya o comparta la sección "Amenazas comunes a la privacidad en línea" del artículo: ¿Qué es la privacidad en línea?

Pida a los participantes que:

- Identifique la amenaza a la privacidad que les resulta más preocupante.
- Reflexione sobre por qué esta amenaza parece especialmente peligrosa o sorprendente.

Anímelos a anotar ideas breves para preparar el debate grupal.





Paso 1: Introducción a los riesgos de la privacidad en línea (15 min)

4. Facilite una breve discusión utilizando estas indicaciones:

- “¿Qué amenaza a la privacidad le llamó más la atención y por qué?”
- ¿Cómo afectan estos riesgos a tu comportamiento o hábitos en línea?

Invite a algunos participantes a compartir sus reflexiones, reforzando que el conocimiento de estos riesgos es el primer paso para proteger mejor la información personal.

5. Resumen: resuma el punto clave de la discusión (por ejemplo: Al reconocer estos riesgos de privacidad, está tomando el control de su presencia en línea. El conocimiento le permite tomar decisiones más inteligentes sobre lo que comparte y cómo interactúa en línea).





Paso 2: Exploración de violaciones de privacidad en el mundo real (10 min)

1. Comience compartiendo una situación impactante y cercana para ilustrar cómo compartir información en línea puede provocar graves violaciones de la privacidad. Explique a los participantes que esta historia no es única. Muchas personas, sin saberlo, comparten información personal que los ciberdelincuentes o personas malintencionadas pueden usar para rastrearlas, hackear sus cuentas o incluso robar su identidad. Enfatice que las violaciones de la privacidad suelen comenzar con información pequeña y aparentemente inofensiva.

2. Muestre a los participantes un breve escenario escrito, ya sea basado en la historia de Sarah o en una situación hipotética similar:

Ejemplo de otro escenario:

Alex descargó una aplicación móvil gratuita sin leer los permisos. La aplicación tenía acceso a su ubicación, contactos y archivos multimedia. Poco después, notó que sus amigos recibían mensajes extraños. Resultó que la aplicación recopilaba sus datos y enviaba spam usando su cuenta.





Paso 2: Exploración de violaciones de privacidad en el mundo real (10 min)

3. Dar instrucciones a los participantes:

Trabajar individualmente o en pequeños grupos para analizar la situación.

- ¿Qué falló? ¿Qué acciones o comportamientos provocaron la vulneración?
- ¿Cómo se podría haber evitado esto? Identifique pasos o hábitos sencillos para proteger la información personal.

Escribe tus pensamientos brevemente.

4. Permita que los participantes compartan sus reflexiones, de la siguiente manera:

- ¿Usted o alguien que conoce se ha enfrentado a un problema similar, como phishing, piratería informática o uso excesivo de información?
- ¿Por qué la gente comparte tanta información personal sin considerar los riesgos?
- Posibles razones:
 - Confiar en aplicaciones o plataformas.
 - Sin darse cuenta de las consecuencias.
 - Configuraciones de privacidad confusas.

Fomentar el intercambio abierto y solidario de experiencias y conocimientos.





Paso 3: Estrategias prácticas para proteger la información personal (10 min)

1. Proyección del video: Muestre el video "Cómo proteger sus datos personales en línea". Anime a los participantes a prestar atención a las estrategias prácticas y viables que se comparten en el video. Enfatice que estos consejos son fáciles de implementar y pueden mejorar significativamente la privacidad en línea.

2. Actividad: "Plan de privacidad personal" Pida a los participantes que escriban tres acciones que tomarán para proteger su privacidad en línea.

Anímelos a considerar:

- Ajustar la configuración de privacidad de las redes sociales.
- Revisar los permisos de las aplicaciones en sus dispositivos.
- Ser conscientes de lo que publican públicamente.

3. Compartir en grupo. Invite a los participantes a compartir una acción que planean implementar con el grupo. Utilice las siguientes indicaciones para guiar la discusión:

- "¿Qué estrategia te resulta más fácil poner en marcha hoy y por qué?"
- ¿A qué desafíos podrías enfrentarte al intentar adoptar estos hábitos?
- ¿Cómo podemos superar barreras comunes, como olvidarnos de ajustar la configuración o encontrar confusas las herramientas de privacidad?

Anime al grupo a brindar consejos prácticos o compartir experiencias personales sobre cómo superaron desafíos similares. Enfatice que dar pequeños pasos de forma constante puede generar mejoras significativas en la privacidad en línea.

4. Además, puedes pedir a los participantes que piensen en cómo pueden compartir estas estrategias con amigos o familiares.





Paso 4 Reflexión final y conclusiones clave:

1. Pida a los participantes que reflexionen sobre:
 - “¿Qué hábito cambiarás para mejorar tu privacidad en línea a partir de hoy?”
 - “¿Cómo compartirás lo que has aprendido con tus amigos o familiares?”
2. Reforzar los puntos principales de la lección:
 - Pequeños cambios, como ajustar la configuración o limitar lo que compartes, tienen un gran impacto.
 - Proteger sus datos le brinda control sobre su identidad digital.
3. Finalice la sesión con una frase final. Por ejemplo: «Su información personal es valiosa. Tome pequeñas medidas inteligentes para protegerla y estará más seguro en línea».

Conclusiones clave:

Al finalizar la lección, los participantes deben comprender claramente que la privacidad en línea comienza con la concienciación y con pequeños pasos prácticos. Cambios sencillos, como ajustar los permisos de las aplicaciones, revisar la configuración de privacidad en redes sociales y ser consciente de lo que se comparte públicamente, pueden reducir significativamente los riesgos. Anime a los participantes a tomar el control de su comportamiento digital desarrollando hábitos como verificar quién tiene acceso a sus datos y ser cautelosos con los enlaces o mensajes sospechosos. Refuerce la idea de que proteger la información personal permite a las personas mantener el control sobre su identidad y seguridad digitales.





Seguimiento y actividades en casa

Pida a los participantes que dediquen los próximos días a implementar al menos una medida de privacidad que hayan identificado durante la sesión. Esto podría incluir revisar la configuración de privacidad en una red social, eliminar aplicaciones que no usan o compartir consejos de privacidad con amigos o familiares. Sugiera que documenten su progreso y reflexionen sobre cómo estos cambios los hacen sentir más seguros en línea. Además, anímelos a explorar herramientas como DuckDuckGo (un buscador privado) o Google Privacy Checkup para ver con qué facilidad pueden mejorar su seguridad en línea. Considere organizar una sesión de seguimiento donde los participantes puedan compartir sus experiencias y hablar sobre los desafíos que enfrentaron.

Consejos para profesores:

Se recomienda incluir ejemplos de la vida real en el debate para que el concepto de privacidad en línea sea comprensible. Utilice escenarios que incluyan compartir demasiado en redes sociales, filtraciones de datos o permisos de aplicaciones para mostrar cómo pequeños hábitos pueden tener grandes consecuencias. Cree un espacio propicio para que los participantes compartan sus experiencias sin ser juzgados. Para garantizar una participación continua, incorpore tareas prácticas breves en las clases, como mostrar cómo ajustar la configuración de privacidad o reconocer enlaces sospechosos. Revise el tema con regularidad para mantener la conciencia sobre la privacidad y animar a los estudiantes a considerar la protección de su información como un hábito para toda la vida.





Herramientas

PatoPatoGo



DuckDuckGo es un motor de búsqueda centrado en la privacidad que no rastrea tu historial de búsqueda ni recopila datos personales. Garantiza la privacidad de tus búsquedas y ayuda a minimizar la huella digital que dejas al navegar.

duckduckgo.com

Comprobación de privacidad de Google



La Comprobación de Privacidad de Google es una herramienta integrada que te ayuda a administrar la configuración de tu cuenta de Google. Te permite revisar y ajustar qué datos personales se recopilan, quién puede ver tu actividad y qué aplicaciones tienen acceso a tu información.

myaccount.google.com/privacycheckup



Referencias

- DuckDuckGo (s.f.). Recuperado de <https://duckduckgo.com>
- Farrier, E. (21 de agosto de 2024). Guía para proteger su información personal. Recuperado de <https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online>
- Glover, E. (24 de enero de 2024). ¿Qué es la privacidad en línea? Integrada. Recuperado de <https://builtin.com/articles/what-is-online-privacy>
- Comprobación de privacidad de Google (sin fecha). Recuperado de <https://myaccount.google.com/privacycheckup>
- Negrean, R. (s.f.). 10 consejos para proteger la privacidad en línea: Estrategias de seguridad digital. Privacy Tutor. Recuperado de <https://privacytutor.net/10-tips-for-protecting-online-privacy>
- Tech Implement Infra Pvt Ltd. (8 de diciembre de 2024). Consejos esenciales para la protección de datos personales y profesionales en línea. [Video]. YouTube. <https://youtu.be/6WQzMAAd6mJs?si=cq1NFnjxu7i8NRk5>
- Webb, M. (26 de noviembre de 2023). Cómo proteger su privacidad en línea: 7 prácticas recomendadas para implementar hoy. Techopedia. Recuperado de <https://www.techopedia.com/how-to/how-to-protect-your-privacy-online>



PRUEBA

1. ¿Cuál es una acción sencilla que puede realizar para limitar el uso indebido de datos personales en línea?
A. Evite crear cuentas en redes sociales por completo B. Desactive todas las notificaciones en sus dispositivos C. Acepte los permisos de las aplicaciones sin revisarlos D. Ajuste su configuración de privacidad en redes sociales regularmente

2. ¿Cuál de los siguientes es un ejemplo de compartir información en exceso que podría conducir al robo de identidad?
A. Compartir una foto de vacaciones solo con amigos cercanos. B. Publicar tu ubicación y rutinas diarias públicamente. C. Enviar fotos de tus mascotas por mensaje privado. D. Usar emojis para describir tu estado de ánimo en línea.

3. ¿Cómo puede la revisión de los permisos de las aplicaciones mejorar tu privacidad en línea?
A. Le permite restringir que las aplicaciones accedan a datos personales innecesarios. B. Le ayuda a descargar aplicaciones más rápido al omitir las verificaciones de permisos. C. Garantiza que todas las aplicaciones en su dispositivo se actualicen automáticamente.
D. Permite que las aplicaciones se ejecuten con mayor fluidez en su dispositivo.





PRUEBA

4. ¿Por qué muchas personas no protegen su información personal en línea?

A. Las herramientas de privacidad no están disponibles para los usuarios habituales. B. Las personas confían en que las empresas mantendrán sus datos seguros. C. Las configuraciones y herramientas de privacidad a menudo se pasan por alto o se consideran confusas. D. La mayoría de las personas creen que no tienen datos personales que valga la pena proteger.

5. ¿Cuál es un buen hábito a desarrollar para proteger la información personal?

A. Usar la misma contraseña por conveniencia B. Permitir que las aplicaciones rastreen tu ubicación en todo momento C. Ignorar los términos de los acuerdos de servicio D. Ser cauteloso al compartir información sensible en plataformas públicas





Soluciones

Pregunta 1: D

Pregunta 2: B

Pregunta 3: A

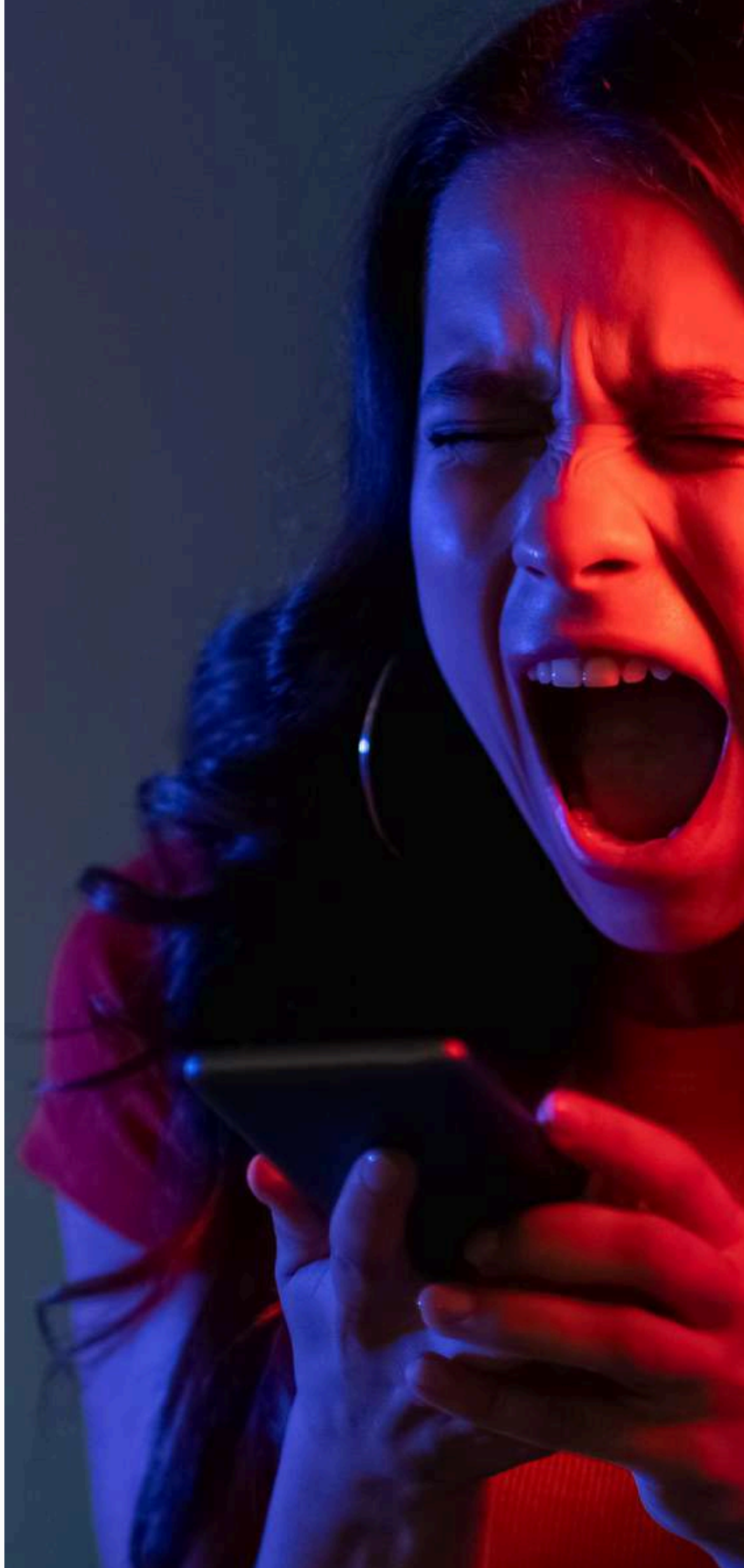
Pregunta 4: C

Pregunta 5: D





Centrum Wspierania
Edukacji
i Przedsiębiorczości



**Co-funded by
the European Union**

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados son, sin embargo, responsabilidad exclusiva del/de los autor(es) y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA se hacen responsables de ellas.