RASMEDIAH – REFUERZO EDUCATIVO CONTRA LA HIPERCONECTIVIDAD DE LAS REDES SOCIALES. NÚMERO DE PROYECTO: 2023-1-HU01-KA220-YOU-000161173

MÓDULO 5

CIBERSEGURIDAD Y SEGURIDAD EN LÍNEA

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

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.

Lección 5.6

Herramientas prácticas para la seguridad en línea

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

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.

Duración: 40 minutos

Lección 5.6

Herramientas prácticas para la seguridad en línea

Objetivos:

- Equipar a los participantes con herramientas y técnicas prácticas para identificar y mitigar amenazas comunes en línea, incluido el phishing, el malware y las estafas.
- Desarrollar competencias en el uso de recursos de ciberseguridad, como administradores de contraseñas, VPN y navegadores seguros, al tiempo que se fomenta la comprensión de la gestión de la privacidad en línea.
- Promover prácticas en línea seguras y responsables a través de la evaluación crítica de las plataformas digitales, reconociendo las señales de advertencia de amenazas cibernéticas y adoptando hábitos de protección como informar actividades sospechosas.

Mensaje(s) clave:

- La concientización y la preparación son su primera línea de defensa. Comprender las amenazas en línea y contar con las herramientas adecuadas le permite navegar con seguridad en el mundo digital.
- Tu seguridad está en tus manos. Aprovechar herramientas prácticas como VPN, navegadores seguros y configuraciones de privacidad te permite proteger tus datos personales y mantener el control de tu presencia en línea.

TIPO DE LECCIÓN:

Descripción general de la lección

La seguridad en línea depende en gran medida de la capacidad de usar eficazmente herramientas diseñadas para proteger la información personal y prevenir amenazas digitales. Esta lección se centra en la interacción práctica con herramientas clave de ciberseguridad, como administradores de contraseñas, VPN y configuraciones de privacidad. Los participantes explorarán activamente cómo funcionan estas herramientas, probarán sus funciones y aprenderán estrategias para incorporarlas a sus rutinas digitales diarias. Mediante actividades guiadas, desarrollarán confianza en la aplicación de estas herramientas para proteger su presencia en línea y responder a los riesgos con soluciones prácticas.

El taller está organizado en 4 pasos:

1: Introducción a las herramientas de seguridad en línea (10 min)

2: Exploración práctica de herramientas (15 min)

3: Gestión de riesgos basada en escenarios (10 min)

4: Reflexiones finales (5 min)

Paso 1

Introducción a las herramientas de seguridad en línea

¿Alguna vez te has encontrado con algo sospechoso en línea? ¿Quizás un correo electrónico extraño pidiéndote que restablezcas tu contraseña, una ventana emergente que ofrece un premio gratis o un sitio web que solicita demasiada información personal? Estas situaciones pueden parecer arriesgadas, y a menudo lo son.

La buena noticia es que existen herramientas prácticas que puedes usar para protegerte en momentos como estos. Al finalizar esta actividad, sabrás reconocer estos riesgos y usar herramientas como administradores de contraseñas, VPN y configuraciones de privacidad para mantenerte seguro en línea. ¡Profundicemos y veamos cómo estas herramientas pueden ayudarte!

Paso 1

Introducción a las herramientas de seguridad en línea

Aquí hay tres herramientas sencillas que pueden hacer que tu vida en línea sea mucho más segura:

- **Administradores de contraseñas: te ayudan a crear y almacenar contraseñas seguras y únicas para que no tengas que recordarlas todas.**
- **VPN (redes privadas virtuales): protegen tu actividad en línea, especialmente en redes Wi-Fi públicas, manteniendo tu conexión segura.**
- **Configuración de privacidad del navegador: le permiten controlar qué información pueden recopilar los sitios web sobre usted, como su ubicación o hábitos de navegación.**

Hoy nos centraremos en estas herramientas porque pueden marcar una gran diferencia a la hora de mantenernos seguros en línea.

Piensa en la última vez que te topaste con algo en línea que te pareció extraño, tal vez un sitio web que no parecía confiable. ¿Cómo lo gestionaste? ¿Lo ignoraste, investigaste más a fondo o incluso hiciste clic?

Hagamos una lluvia de ideas juntos:

- ¿Qué tipos de amenazas o riesgos en línea ha notado antes?
- ¿Qué herramientas o estrategias utilizas ya para mantenerte seguro en línea?

Nos tomaremos unos minutos para compartir ideas en grupo. No te preocupes si no lo has vivido en primera persona: las historias de tus compañeros podrían inspirar nuevas ideas.

Paso 2

Exploración práctica de herramientas

Ahora es el momento de profundizar y explorar cómo herramientas sencillas pueden hacer tu presencia en línea más segura. En esta actividad, probarás la configuración de privacidad del navegador y pondrás a prueba tus habilidades para crear contraseñas con el Medidor de Contraseñas. ¡Comencemos!

Parte 1: Configuración de privacidad del navegador

Tu navegador puede controlar cuánta información recopilan los sitios web sobre ti. Revisemos y ajustemos tu configuración de privacidad:

1. Abra la configuración de privacidad de su navegador (busque "Configuración" o "Preferencias" y luego "Privacidad" o "Seguridad").
2. Revise estas áreas clave:

- **Prevención de seguimiento: ¿está activada?**
- **Cookies: ¿Se bloquean las cookies de terceros?**
- **Permisos: ¿Qué sitios web pueden acceder a tu ubicación, cámara o micrófono?**

Paso 2 oración práctica de herramientas

3. Realice ajustes: active cualquier configuración de privacidad que crea que ayudará a proteger sus datos.

Por ejemplo:

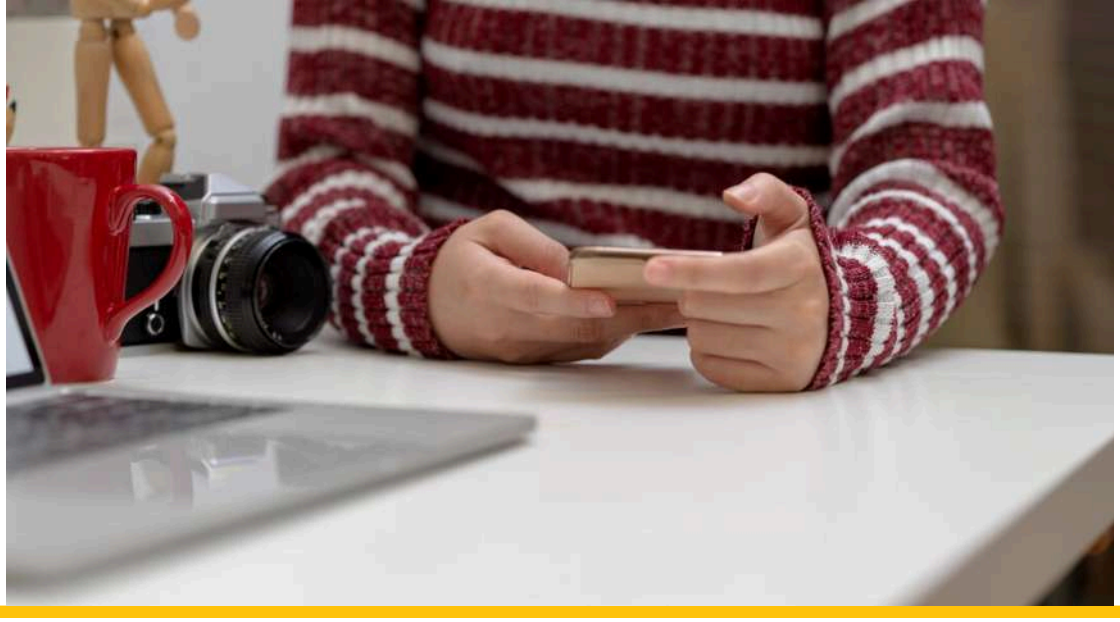
- Bloquear las cookies de seguimiento.
- Desactiva la función de compartir ubicación para sitios web en los que no confías.

Reflexión rápida: ¿Qué te sorprendió de tu configuración actual? ¿Hiciste algún cambio?

Parte 2: Prueba de la seguridad de la contraseña con The Password Meter

Crear una contraseña segura es una de las maneras más fáciles de proteger tus cuentas. Veamos qué tan seguras son tus contraseñas:

1. Vaya al medidor de contraseñas.
2. Piensa en una nueva contraseña (¡no uses una que ya tengas!).



Paso 2 Exploración práctica de herramientas

3. Introdúzcalo en The Password Meter y mire los comentarios:
   - ¿Qué tan segura es tu contraseña?
   - ¿Qué sugerencias da para hacerlo más fuerte?

4. Experimenta cambiando tu contraseña según los comentarios (por ejemplo, añade símbolos, alargándola o combinando mayúsculas y minúsculas). ¡Observa cómo mejora tu puntuación!

Reflexión rápida: ¿Qué tan fácil o difícil fue crear una contraseña segura? ¿Qué harás diferente al configurar contraseñas en el futuro?

¡Al finalizar esta actividad, habrás mejorado la configuración de privacidad de tu navegador y habrás aprendido a crear contraseñas más seguras!

Paso 3

Gestión de riesgos basada en escenarios

Tras analizar algunas herramientas prácticas, veamos cómo se pueden aplicar a situaciones reales. Trabajarán en grupos pequeños para analizar escenarios, identificar riesgos y decidir cómo abordarlos utilizando las herramientas presentadas.

Lean el escenario que se les presenta a sus grupos. Aquí tienen algunos ejemplos:

1. Recibes un correo electrónico diciendo que has ganado un premio, pero el enlace parece sospechoso. ¿Qué haces?
2. *Una aplicación de redes sociales te pide acceder a tu ubicación, cámara y micrófono al instalarla. ¿Deberías permitirlo?*
3. *Estás usando una red wifi pública en una cafetería y te piden que inicies sesión en un sitio web desconocido. ¿Cómo te proteges?*

Hablen con su grupo sobre los riesgos de su escenario. Pregúntense:

- *¿Qué podría salir mal si no actúas con cuidado?*
- *¿Por qué esta situación parece insegura?*

Decide cómo podrías usar herramientas prácticas para gestionar el riesgo. Por ejemplo:

- *Utilice la configuración de privacidad del navegador para bloquear permisos innecesarios.*
- *Evite hacer clic en enlaces sospechosos y revise sus correos electrónicos para detectar señales de phishing.*
- *Activa una VPN para proteger tu conexión en redes Wi-Fi públicas.*

Paso 3

Gestión de riesgos basada en escenarios

Después de varios minutos, cada grupo compartirá:

- *¿Qué riesgos detectaste en el escenario?*
- *¿Qué herramientas o pasos usaste para mantenerte seguro?*

Piénsalo: ¿Cómo podrían estas herramientas ayudarte en tus propias actividades en línea?

Herramientas prácticas como la configuración de privacidad del navegador, las VPN y la detección de phishing pueden simplificar las situaciones de riesgo. ¡Usarlas regularmente facilita enormemente la seguridad en línea!

Paso 4

Reflexiones finales

Reflexionemos sobre lo que has aprendido y cómo lo utilizarás para mantenerte seguro en línea.

Paso 1: Reflexionar

Piense en estas preguntas:

- ¿Qué herramienta (por ejemplo, la configuración de privacidad del navegador, las VPN o los administradores de contraseñas) te resultó más útil? ¿Por qué?
- ¿Cómo ha cambiado tu visión sobre la seguridad en línea después de utilizar estas herramientas?

Paso 2: Planifica tu próximo paso

Escribe una acción que llevarás a cabo para mejorar tu seguridad en línea.

- ¿Qué harás? (p. ej., «Usaré un gestor de contraseñas para crear contraseñas seguras»).
- ¿Cuándo lo harás? (por ejemplo, “A finales de la semana”).

Las herramientas prácticas son el primer paso: ¡sea constante para mantener sólida su seguridad en línea!

Resumen de las conclusiones clave

- La configuración de privacidad del navegador, los administradores de contraseñas y las VPN son herramientas simples pero poderosas para mejorar su seguridad en línea.
- Administre activamente qué información comparte en línea ajustando la configuración de privacidad y limitando los permisos innecesarios.
- Actualice periódicamente la configuración de privacidad, cree contraseñas seguras y revise los permisos de las aplicaciones para hacer de la seguridad en línea una parte rutinaria de su vida digital.
- Manténgase proactivo: combinar herramientas con pensamiento crítico y mantenerse informado le garantiza estar preparado para las amenazas en línea en evolución.
- Intenta también probar otras herramientas prácticas en línea para entender y mejorar tu seguridad digital: ¡cuantas más herramientas sepas utilizar, más aumentarás tu seguridad!

Instrucciones para trabajadores juveniles, educadores y

Objetivo:
Esta lección se centra en dotar a los participantes de las habilidades prácticas necesarias para usar herramientas básicas de seguridad en línea. Mediante ejercicios y debates individuales y grupales, adquirirán la capacidad de identificar y abordar amenazas comunes en línea, fortalecer su protección digital con recursos como administradores de contraseñas, VPN y configuraciones de privacidad, e integrar hábitos más seguros en sus actividades diarias en línea.

Materiales necesarios:

- Acceso a Internet para herramientas de prueba (por ejemplo, VPN, administradores de contraseñas)
- Computadoras portátiles, tabletas o teléfonos inteligentes para ejercicios prácticos.
- Pizarra o rotafolio para generar ideas y resumir debates
- Hojas de papel en blanco para tomar notas
- Bolígrafos, lápices o rotuladores de colores

Paso 1: Introducción a las herramientas de seguridad en línea (10 min)

1. Comience por involucrar a los participantes con una pregunta que les resulte familiar: "¿Alguna vez se han encontrado con algo en línea que les pareció sospechoso, como un correo electrónico extraño, una ventana emergente que ofrece un premio o un sitio web que solicita demasiada información personal?". Explique brevemente que estas situaciones pueden parecer riesgosas y a menudo lo son, pero existen herramientas prácticas para abordarlas.
2. Presente el enfoque de la sesión en tres herramientas esenciales: administradores de contraseñas, VPN y la configuración de privacidad del navegador. Resalte su importancia explicando que los administradores de contraseñas ayudan a crear y almacenar contraseñas seguras y únicas, las VPN protegen la actividad en línea en redes wifi públicas y la configuración de privacidad del navegador controla qué información pueden recopilar los sitios web, como la ubicación o los hábitos de navegación.
3. Anime a los participantes a reflexionar sobre sus propias experiencias con los riesgos en línea preguntándoles: «Piensen en la última vez que se encontraron con algo sospechoso en línea. ¿Cómo lo manejaron?».
4. Facilite un breve debate con preguntas como: "¿Qué tipos de amenazas en línea han detectado?" y "¿Qué herramientas o estrategias utilizan ya para mantenerse seguros?". Invite a los participantes a compartir sus historias o ideas, enfatizando que aprender unos de otros puede generar nuevas perspectivas.
5. Concluya reforzando la importancia de estas herramientas para gestionar los riesgos en línea, afirmando: «Al usar herramientas como administradores de contraseñas, VPN y configuraciones de privacidad, puede navegar con confianza por el mundo digital mientras protege su información personal». Mantenga la conversación interactiva y motivadora, asegurándose de que los participantes se sientan motivados a compartir sus ideas y aprender del grupo.

Paso 2: Exploración práctica de herramientas (15 min)

1. Comience explicando el objetivo de esta actividad: explorar herramientas prácticas que mejoran la seguridad en línea a través de la configuración de privacidad del navegador y las pruebas de fortaleza de las contraseñas.
2. Divida la actividad en dos partes para garantizar un enfoque estructurado.

Parte 1: Configuración de privacidad del navegador (8 minutos)

1. Indique a los participantes que abran la configuración de privacidad de su navegador (vayan a "Configuración" o "Preferencias" y luego busquen "Privacidad" o "Seguridad"). Pídales que revisen las áreas clave:
   - Prevención de seguimiento: asegúrese de que esté habilitada.
   - Cookies: Comprueba si las cookies de terceros están bloqueadas.
   - Permisos: revise qué sitios web pueden acceder a su ubicación, cámara o micrófono.
2. Anime a los participantes a realizar ajustes, como bloquear las cookies de seguimiento o deshabilitar el uso compartido innecesario de la ubicación.
3. Después, invite a una breve reflexión: "¿Qué les sorprendió de su configuración actual? ¿Hicieron algún cambio?". Esto ayuda a los participantes a conectar sus descubrimientos con el valor de estas herramientas.

Parte 2: Prueba de fortaleza de la contraseña (5 minutos)

1. Indique a los participantes que accedan al Medidor de Contraseñas. Pídales que creen una nueva contraseña (no la que usan actualmente) y que comprueben su seguridad.
2. Anímelos a analizar los comentarios y experimentar con cambios, como agregar símbolos, mezclar mayúsculas y minúsculas o aumentar la longitud, para ver cómo mejora la puntuación.
3. Concluye con una reflexión: "¿Qué tan fácil o difícil fue crear una contraseña segura? ¿Qué harás diferente al configurar contraseñas en el futuro?"
4. Concluya la actividad reforzando su valor práctico.
5. Mantenga la sesión práctica y atractiva, ofreciendo orientación según sea necesario mientras los participantes exploran y aplican estas herramientas.

Paso 3: Gestión de riesgos basada en escenarios (10 min)

1. Esta actividad ayuda a los participantes a aplicar herramientas de seguridad en línea a situaciones reales. Divida a los participantes en grupos pequeños y asigne a cada grupo una situación, como por ejemplo:
   - Un correo electrónico sospechoso con un enlace a un premio.
   - Una aplicación de redes sociales que solicita permisos excesivos.
   - Estoy usando una red Wi-Fi pública y me encuentro con un mensaje de inicio de sesión desconocido.
2. Instruya a los grupos para que discutan los riesgos, considerando:
   - "¿Qué podría salir mal si no actúas con cuidado?"
   - "¿Por qué esta situación parece insegura?"
3. Pídales que identifiquen cómo manejar el riesgo utilizando herramientas como la configuración de privacidad del navegador, evitando enlaces de phishing o habilitando una VPN.
4. Posteriormente, cada grupo comparte los riesgos que identificaron y las herramientas que utilizaron para abordarlos.
5. Concluya destacando: «Herramientas como la configuración de privacidad, las VPN y la detección de phishing facilitan la gestión de riesgos en línea. El uso regular de estas herramientas refuerza la seguridad en línea». Mantenga la sesión enfocada y fomente ideas prácticas y viables.

Paso 4: Reflexiones finales (5 min)

1. Concluya la sesión guiando a los participantes a través de un ejercicio reflexivo para consolidar su aprendizaje. Comience pidiéndoles que consideren:
   - ¿Qué herramienta (p. ej., configuración de privacidad del navegador, VPN, gestores de contraseñas) te resultó más útil? ¿Por qué?
   - ¿Cómo ha cambiado tu visión de la seguridad en línea después de usar estas herramientas?
2. Anime a los participantes a compartir sus pensamientos brevemente, fomentando un ambiente propicio para el debate.
3. A continuación, pídeles que planifiquen una acción concreta para mejorar su seguridad en línea, como por ejemplo:
   - "¿Qué harás?" (p. ej., "Usaré un administrador de contraseñas para crear contraseñas seguras").
   - “¿Cuándo lo harás?” (por ejemplo, “A finales de la semana”).
4. Concluya enfatizando la importancia de la constancia y recordando a los participantes: "Las herramientas prácticas son el primer paso: ¡sean constantes para mantener una seguridad en línea sólida!". Mantenga un tono motivador y concéntrese en aplicar las lecciones aprendidas a sus prácticas diarias en línea.

Conclusiones clave:

Tras completar la lección, los participantes comprenderán claramente cómo usar herramientas básicas como administradores de contraseñas, VPN y la configuración de privacidad del navegador para mejorar su seguridad en línea. Aprenderán a identificar amenazas comunes, como el rastreo de datos, y a tomar medidas proactivas para proteger su información personal. Al integrar estas herramientas y estrategias en su rutina diaria, podrán desenvolverse en el mundo digital con confianza, minimizando las posibles amenazas. Para comunicar eficazmente estas lecciones, utilice situaciones reales y ejemplos claros para demostrar el impacto real de estas herramientas en la seguridad en línea.

Seguimiento y actividades en casa:

Incentive a los participantes a analizar con más detalle sus prácticas actuales en línea revisando y ajustando la configuración de privacidad de su navegador, probando la seguridad de sus contraseñas con herramientas como The Password Meter y explorando las funciones de VPN. Pídales que evalúen los permisos de las aplicaciones que usan con frecuencia, identificando los posibles riesgos e implementando alternativas más seguras. Finalmente, pídales que compartan un consejo de seguridad recién aprendido con un amigo o familiar para reforzar sus conocimientos y crear conciencia sobre la seguridad digital.

Consejos para profesores:

Puede usar ejemplos prácticos del mundo real y otros ejercicios interactivos para demostrar cómo herramientas como administradores de contraseñas, VPN y configuraciones de privacidad pueden usarse eficazmente para mejorar la seguridad en línea. Muestre a los participantes paso a paso cómo navegar y configurar estas herramientas, haciendo que la sesión sea práctica y práctica. Cree un ambiente abierto y propicio donde los participantes se sientan cómodos para compartir sus experiencias con las amenazas en línea y hacer preguntas. Resalte la importancia de usar estas herramientas regularmente e integrarlas en sus rutinas diarias en línea para garantizar una protección digital consistente y proactiva.

Herramientas

Manténgase seguro en línea

Un sitio web completo que ofrece consejos gratuitos y directos sobre una amplia gama de temas de seguridad en línea. Incluye guías prácticas para proteger la información personal, evitar estafas y comunicarse en línea de forma segura. El contenido es intuitivo y está diseñado para personas con conocimientos técnicos mínimos.

www.getsafeonline.org

El medidor de contraseñas

Una herramienta gratuita que evalúa la seguridad de las contraseñas y ofrece consejos para mejorarlas. Los estudiantes pueden experimentar creando contraseñas y recibir información instantánea sobre su nivel de seguridad, lo que les permite comprender de forma interactiva la importancia de las contraseñas seguras.

passwordmeter.com

Referencias

- Alice. (3 de octubre de 2022). 5 herramientas que ayudan a mantener la seguridad en línea. Ryadel. Recuperado de https://www.ryadel.com/en/5-privacy-data-protection-security-tools
- Navega con seguridad en línea. (s.f.). Recuperado de https://www.getsafeonline.org
- Equipo Goodwall. (24 de marzo de 2022). Las 7 mejores herramientas de seguridad en línea y configuraciones de privacidad para protegerte. Recuperado de https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings
- Lakhwani, S. (19 de junio de 2024). Fundamentos de ciberseguridad [Guía para principiantes 2024]. Blog de upGrad KnowledgeHut. Recuperado de https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- El medidor de contraseñas. (s.f.). Recuperado de https://passwordmeter.com
- Vodafone. (s.f.). Uso de herramientas de seguridad y bienestar en línea. Recuperado de https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools

PRUEBA

1. ¿Cuál es la función principal de una red privada virtual (VPN)?
A. Proporcionar protección antivirus automática
B. Aumentar la velocidad de Internet
C. Evitar anuncios emergentes en todos los sitios web
D. Cifrar la actividad en línea, especialmente en redes Wi-Fi públicas

2. ¿Qué comportamiento podría poner en riesgo tu seguridad en línea?
A. Usar contraseñas seguras y únicas para cada cuenta.
B. Ajustar la configuración de privacidad de su navegador regularmente.
C. Usar un administrador de contraseñas para almacenar las credenciales de inicio de sesión.
D. Hacer clic en todos los enlaces de correos electrónicos no solicitados.

3. ¿Cuál es un paso recomendado para mejorar la configuración de privacidad de su navegador?
A. Usar la configuración predeterminada sin modificaciones
B. Bloquear las cookies de seguimiento y deshabilitar permisos innecesarios
C. Desactivar las cookies para todos los sitios web
D. Permitir que todos los sitios web accedan a su ubicación

PRUEBA

4. ¿Cuál es el propósito de la configuración de privacidad del navegador?

A. Para acelerar la experiencia de navegación del usuario

B. Para almacenar las contraseñas del usuario de forma segura

C. Para controlar qué información pueden recopilar los sitios web sobre el usuario

D. Para evitar anuncios emergentes en todos los sitios web

5. ¿Cómo puedes mejorar la seguridad de tu contraseña?

A. Incluyendo símbolos, mezclando mayúsculas y minúsculas y aumentando la longitud.

B. Utilizando frases comunes que sean fáciles de recordar.

C. Evitando el uso de números y caracteres especiales.

D. Probando la misma contraseña repetidamente

Soluciones

Pregunta 1: D
Pregunta 2: D
Pregunta 3: B
Pregunta 4: C
Pregunta 5: A

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

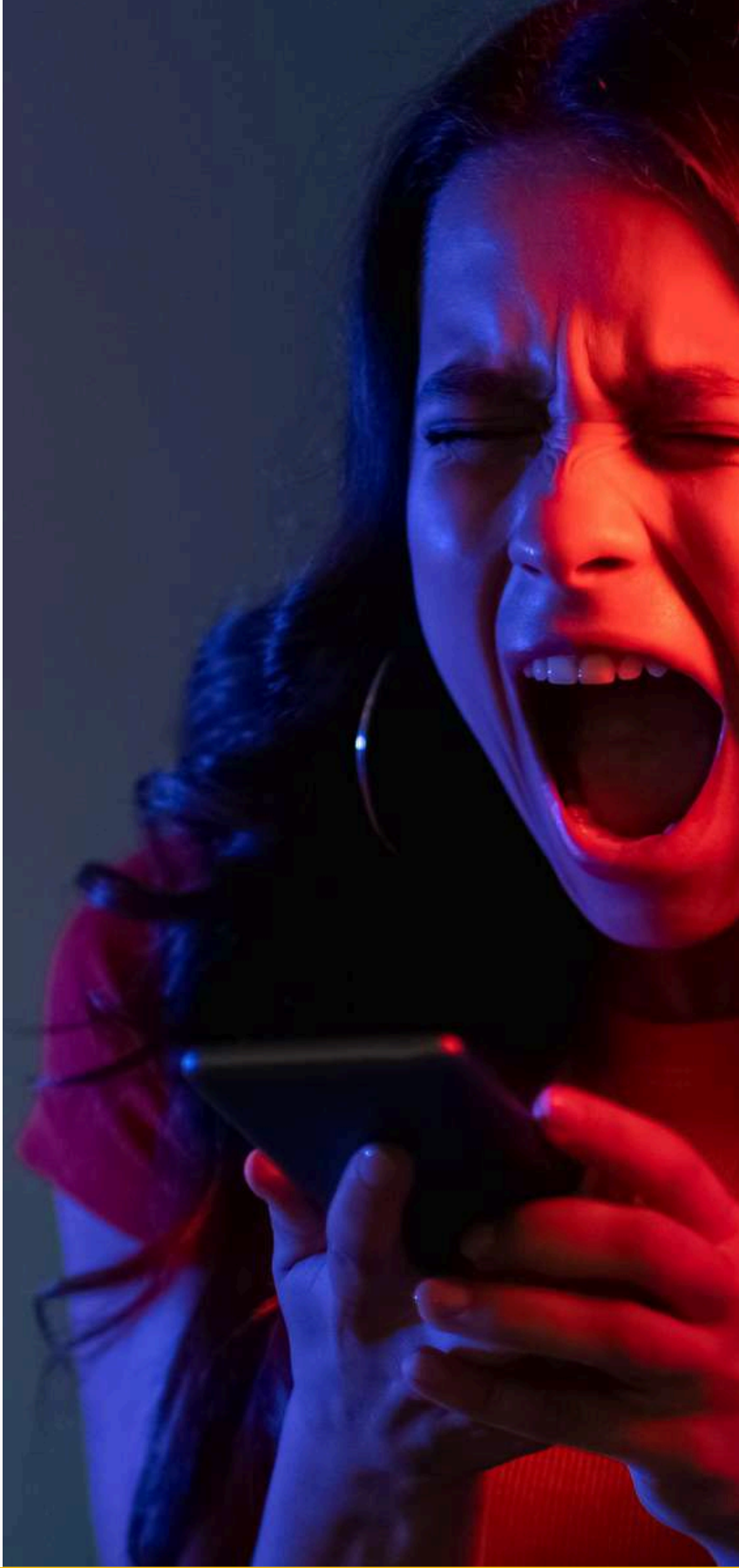
LABC

CWEP Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



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.