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 5.4

Reconocimiento de amenazas cibernéticas y estrategias para prevenir la exposición a contenido inapropiado

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 5.4

Reconocimiento de amenazas cibernéticas y estrategias para prevenir la exposición a contenido inapropiado

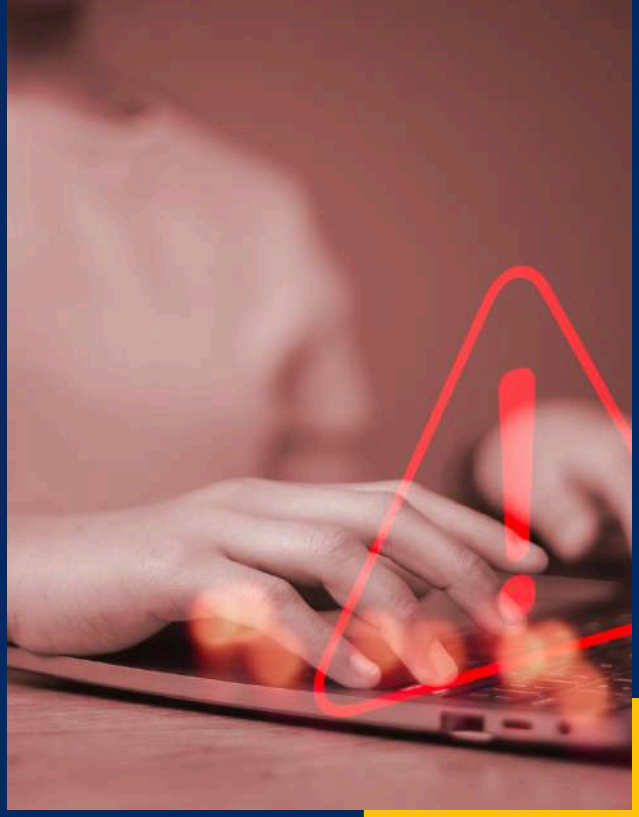
Objetivos:

- Desarrollar conciencia sobre los riesgos prevalentes en línea, como la exposición a contenido inapropiado, el acoso cibernético y el acoso escolar, especialmente dirigidos a usuarios vulnerables como niños y adolescentes.
- Proporcionar a los estudiantes habilidades críticas para reconocer señales de advertencia de amenazas cibernéticas, como enlaces sospechosos, comportamiento depredador en línea y contenido manipulador.
- Fomentar hábitos proactivos en la gestión de las interacciones en línea fomentando el pensamiento crítico, identificando espacios digitales seguros y manteniendo una comunicación abierta sobre las experiencias en línea.

Mensaje(s) clave:

- Las amenazas en línea suelen esconderse tras plataformas o interacciones aparentemente inocentes. Reconocer las señales es clave para mantenerse a salvo.
- Prácticas simples como usar filtros de contenido y mantener una comunicación sólida pueden ayudar a prevenir la exposición a contenido dañino y amenazas cibernéticas.

TIPO DE LECCIÓN:



Descripción general de la lección

En el entorno digital hiperconectado actual, la exposición a contenido inapropiado y ciberamenazas es un riesgo constante. Esta lección está diseñada para brindar una comprensión integral de la naturaleza y los riesgos de estas amenazas, herramientas prácticas para mitigarlas y estrategias para fomentar interacciones en línea más seguras. Mediante ejercicios interesantes y consejos prácticos, terminará la sesión mejor preparado para navegar por el mundo digital de forma segura y responsable.

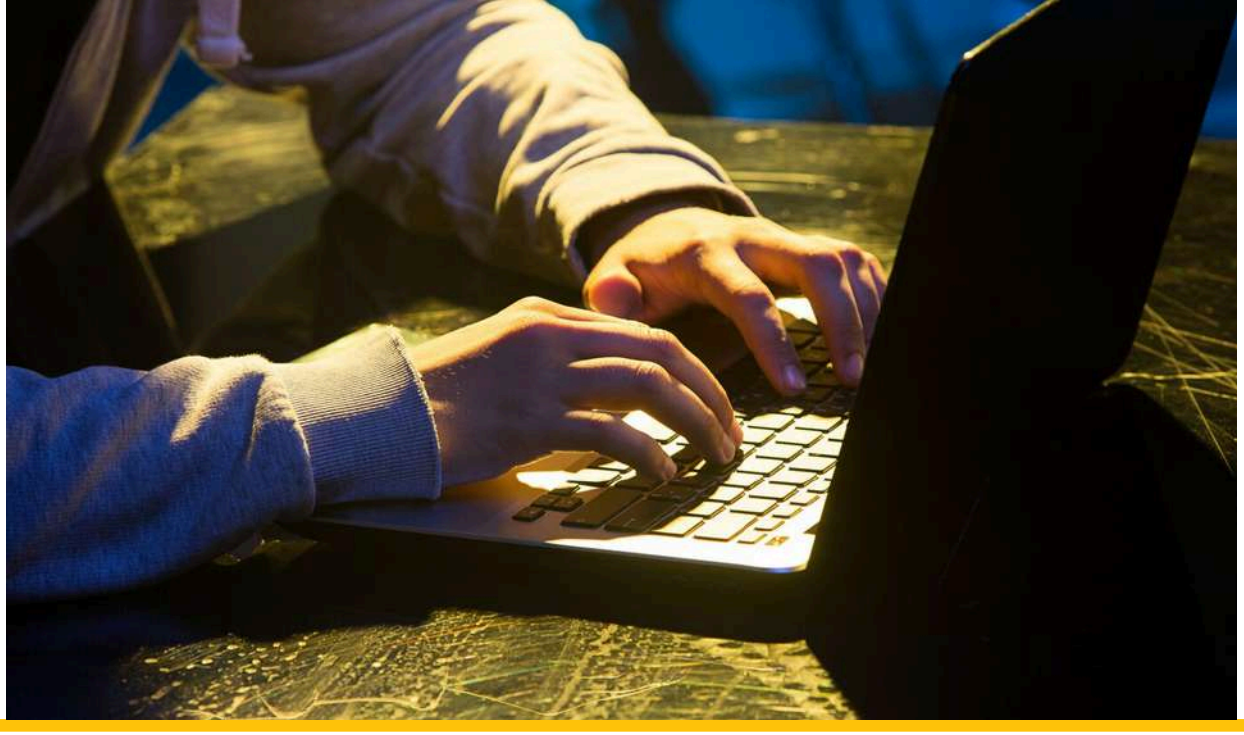
El taller está organizado en 4 pasos:

1: Fundamentos de las ciberamenazas y el contenido inapropiado (10 min)

2: Reconocer señales de advertencia y riesgos (15 min)

3: Enfoques de prevención y mitigación (10 min)

4: Reflexión y aplicación (5 min)



Paso 1

Conceptos básicos sobre amenazas cibernéticas y contenido inapropiado

¿Alguna vez te has encontrado con algo en línea que te hizo sentir incómodo o inseguro?

Las ciberamenazas son actividades dañinas que atacan a personas o sistemas en línea, con el objetivo de robar información, causar daños o explotar vulnerabilidades. Algunos ejemplos incluyen:

- Ciberacoso: uso de plataformas en línea para acosar o intimidar.
- Phishing: Envío de mensajes engañosos para engañar a las personas y que revelen información personal.
- Grooming: construir una relación con alguien en línea para explotarlo más tarde, a menudo de manera inapropiada.

¿Qué constituye contenido inapropiado?

Contenido que sea dañino, explícito o inadecuado para ciertos grupos de edad, como:

- Imágenes o vídeos explícitos.
- Mensajes manipuladores o depredadores.
- Material violento o de odio.

Paso 1

Conceptos básicos sobre amenazas cibernéticas y contenido inapropiado

La exposición a dicho contenido puede causar angustia emocional, dañar las relaciones y generar consecuencias a largo plazo como el robo de identidad o la explotación.

Actividad

Ahora, nos dividiremos en equipos pequeños. Cada grupo recibirá un escenario para analizar:

Escenario 1: Recibes un correo electrónico de un extraño que te pide información personal Escenario 2: Ves un enlace sospechoso en un correo electrónico Escenario 3: Te encuentras con un comentario inapropiado en las redes sociales

Tu tarea es responder las preguntas en tu grupo:

- ¿Qué hay de riesgoso en esta situación?
- ¿Cómo puedes responder de forma segura?

Una vez que los grupos hayan terminado, compartan las conclusiones entre todos.

Paso 2

Reconocer señales de advertencia y riesgos

Observa los ejemplos a continuación y piensa si alguna vez has visto algo similar en internet. Durante la lluvia de ideas, discutan en grupo cuáles de estas señales de advertencia son las más comunes y cómo pueden responder a ellas.

1. Remitente desconocido o sospechoso

- Recibes un mensaje de alguien que no conoces, pidiéndote información personal o invitándote a hacer clic en un enlace.
- La dirección de correo electrónico parece inusual, como "bank123random@mail.com" en lugar de una dirección oficial.
- *Pregunta para debate: “¿Qué haces cuando recibes un mensaje de alguien que no reconoces?”*

2. Errores ortográficos o gramaticales

- El mensaje está lleno de errores ortográficos o frases extrañas.
- Ejemplo: "¡Tu cuenta está bloqueada! Haz clic aquí para reactivarla".
- *Pregunta de debate: "¿Los errores en un mensaje te hacen sospechar? ¿Por qué sí o por qué no?"*

Paso 2

econocer señales de advertencia y riesgos

3. Solicitudes urgentes o amenazas

- Mensajes como: "¡Si no pagas en 24 horas, tu cuenta será desactivada!"
- El contenido intenta asustarte o presionarte para que actúes rápidamente.
- *Pregunta para debate: "¿Cómo puedes diferenciar entre una advertencia real y una estafa?"*

4. Ofertas demasiado buenas para ser verdad

- Anuncios que prometen recompensas increíbles: "¡Ganaste un iPhone nuevo! Haz clic aquí para reclamar tu premio".
- Sitios web que ofrecen beneficios poco realistas con poco esfuerzo.
- *Pregunta de debate: "¿Por qué son peligrosas este tipo de ofertas?"*

Paso 2

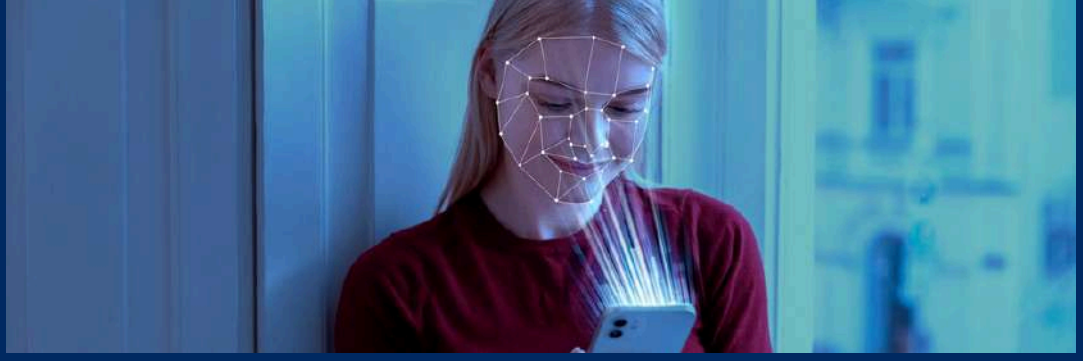
Reconocer señales de advertencia y riesgos

5. Enlaces o archivos adjuntos desconocidos

- Recibes un enlace que no parece confiable, como "www.freegift.now".
- Archivos adjuntos de remitentes desconocidos que podrían contener virus.
- *Pregunta de debate: "¿Cómo puedo comprobar si un enlace o archivo adjunto es seguro?"*

En grupo, elijan una de estas señales de advertencia y analicen cómo manejarían la situación.

Al final, cada grupo compartirá sus conocimientos e ideas sobre cómo evitar estos riesgos en las actividades cotidianas en línea.



Paso 3

Enfoques de prevención y mitigación

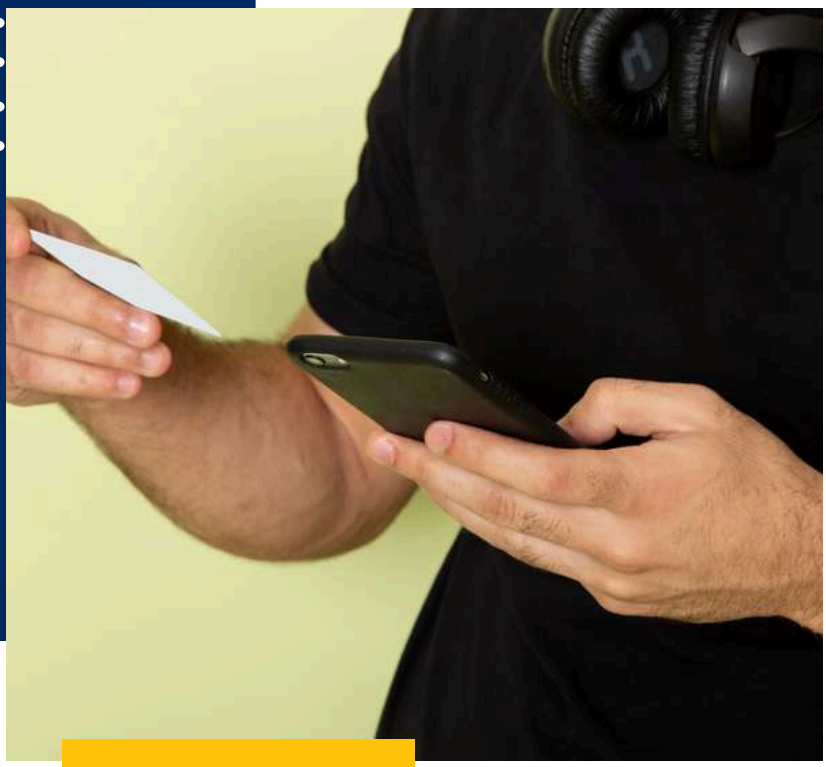
La mejor manera de mantenerse seguro en línea es tomar medidas proactivas que protejan sus datos y prevengan riesgos antes de que ocurran. Exploremos estrategias sencillas que puede empezar a usar de inmediato.

Mantengámonos en los mismos grupos. Lea la siguiente lista de acciones sencillas que puede tomar para reducir los riesgos en línea:

- **Utilice contraseñas fuertes y únicas y actualícelas periódicamente.**
- **Habilite la autenticación multifactor (MFA) para cuentas importantes.**
- **Evite enlaces y archivos adjuntos sospechosos: verifique siempre la fuente.**
- **Revise la configuración de privacidad en las redes sociales y aplicaciones para controlar quién ve su información.**
- **Mantenga el software actualizado para corregir vulnerabilidades de seguridad.**

En grupo, analicen cuáles de estas acciones ya practican y cuáles les resultaría difícil implementar.
Respondan estas preguntas juntos:

- ¿Qué estrategia crees que es la más eficaz para mantenerte seguro en línea?



Paso 3

Enfoques de prevención y mitigación

"¿Cómo puedes recordarte a ti mismo que debes desarrollar mejores hábitos, como revisar la configuración de privacidad o evitar enlaces peligrosos?". Tras una lluvia de ideas, cada grupo comparte una nueva estrategia que planea adoptar y explica brevemente por qué es importante.

Como reflexión final, tómate un momento para pensar en un hábito o herramienta específica que te comprometerás a usar de inmediato para mejorar tu seguridad en línea. Escríbelo en una nota adhesiva y piensa cómo puedes ayudar a otros a adoptar los mismos hábitos. Al compartir tus conocimientos, puedes crear un entorno en línea más seguro no solo para ti, sino también para tus amigos, familiares y la comunidad.

Paso 4

Reflexión y aplicación

Ahora que hemos explorado los riesgos en línea y las estrategias de prevención, es hora de reflexionar sobre lo que has aprendido y pensar en cómo puedes aplicarlo en tu vida digital cotidiana.

Tómate un momento para responder la pregunta en silencio:

- "¿Qué hábito tienes actualmente que podría ponerte en riesgo en línea?"

Escribe tu respuesta en una nota adhesiva.

Como siguiente paso, forme pareja con un compañero y compartan sus reflexiones:

- Explique el hábito riesgoso que identificó y por qué podría ser un problema.
- Comparte la acción o herramienta que planeas adoptar para mitigar este riesgo.
- Ofrézcanse mutuamente comentarios o ideas adicionales para fortalecer sus planes.
- Analice cómo se pueden aplicar estas estrategias en diferentes situaciones, como usar Wi-Fi público, compartir información personal o evitar el acoso y el phishing.

Resumen de las conclusiones clave

- La concientización es el primer paso hacia la protección.
- Las señales de advertencia están en todas partes, pero una vez que aprendes a reconocerlas y responder adecuadamente, ¡puedes mejorar significativamente tu seguridad en línea!
- Comprender las amenazas cibernéticas y el contenido inapropiado le permitirá identificar riesgos potenciales y responder con confianza.
- Reconocer los riesgos en situaciones cotidianas en línea le permite actuar rápidamente y evitar peligros.
- Al difundir la concienciación, estás ayudando a crear una comunidad en línea más segura para todos.

Instrucciones para trabajadores juveniles, educadores y

Objetivo:

Esta lección está diseñada para concientizar sobre los riesgos en línea, incluyendo las ciberamenazas y el contenido inapropiado, y para brindar a los participantes estrategias prácticas para fomentar interacciones en línea más seguras. Mediante el análisis de situaciones reales, los participantes aprenderán a identificar riesgos, reconocer señales de alerta y adoptar medidas preventivas.

Materiales necesarios:

- Rotafolio o herramienta de presentación digital para resumir conceptos clave
- Bolígrafos y marcadores
- Hojas de papel en blanco para tomar notas o completar actividades.
- Acceso a herramientas como CyberWise o Malwarebytes Browser Guard (en caso de presentarlas a los participantes)
- Notas adhesivas de colores para la lluvia de ideas

Paso 1: Fundamentos de las ciberamenazas y el contenido inapropiado (10 min)

1. Comience preguntando a los participantes: "¿Alguna vez se han encontrado con algo en línea que les haya parecido inseguro o sospechoso?". Anime a algunos a compartir sus experiencias o a dar un breve ejemplo, como recibir un correo electrónico sospechoso o ver un comentario ofensivo. Utilice esto para enfatizar la importancia de comprender y abordar los riesgos en línea.
2. Miniconferencia: explique las principales ciberamenazas: phishing, acoso, etc. Defina el contenido inapropiado, incluyendo:
   - Material explícito: imágenes y vídeos dañinos o gráficos.
   - Mensajes depredadores: comunicación manipuladora o dañina.
   - Contenido inapropiado para la edad: material no apto para determinados grupos de edad.
3. Actividad: Divida a los participantes en grupos de 3 a 5 y asigne uno de tres escenarios diferentes a cada grupo.

Instrucciones para grupos:

1. Analizar el riesgo: Analice qué hace que el escenario sea riesgoso (por ejemplo, remitente desconocido, tono urgente o enlace sospechoso).
2. Sugerir acciones seguras: Piense en respuestas prácticas:
   - Para correos electrónicos: evite hacer clic en enlaces, verifique el remitente a través de canales oficiales o repórtelo como spam.
   - Para comentarios inapropiados: bloquear al usuario, reportar el comentario y evitar responder.
   - Para enlaces sospechosos: pase el cursor para verificar la URL, no haga clic si no está seguro y consulte una fuente confiable.
3. Compartir hallazgos: Los grupos resumen su análisis y lo comparten con la clase. Destacan las estrategias comunes y analizan su eficacia.

4. Finalice reforzando los puntos clave y vinculando la actividad con estrategias más amplias de seguridad en línea que se explorarán en los pasos posteriores.

Paso 2: Reconocer señales de advertencia y riesgos (15 min)

1. Presente a los participantes las señales de advertencia comunes de amenazas cibernéticas utilizando ejemplos claros:

- Enlaces sospechosos o remitentes desconocidos: mensajes de contactos desconocidos con enlaces o archivos adjuntos (por ejemplo, "www.freeprizes.xyz").
- Errores ortográficos o urgencias: Mensajes como "¡Tu cuenta está bloqueada! Reactívala ahora", a menudo mal redactados para crear urgencia.
- Ofertas demasiado buenas para ser verdad: promesas de recompensas o promociones, como "¡Ganaste un iPhone gratis!"

También puede utilizar elementos visuales, como capturas de pantalla de intentos de phishing, y alentar a los participantes a compartir ejemplos para lograr una mejor participación.

2. El siguiente paso es realizar un ejercicio grupal. Divida a los participantes en grupos pequeños y asigne a cada grupo una señal de alerta específica para analizar (por ejemplo, mensajes urgentes o enlaces sospechosos). Indique estos pasos:

1. Analice la advertencia: analice qué hace que la amenaza sea convincente (por ejemplo, la urgencia o el engaño).
2. Proponer soluciones: haga una lluvia de ideas sobre respuestas, como verificar fuentes, evitar enlaces sospechosos o denunciar estafas.
3. Resumir los hallazgos: preparar consejos prácticos para evitar la amenaza asignada.

3. Al final, cada grupo presenta sus ideas y estrategias. Resúmelas en una lista consolidada de buenas prácticas en una pizarra o rotafolio. Concluye enfatizando la importancia de la precaución, la verificación y el pensamiento crítico para mantenerse seguro en línea.

Paso 3: Enfoques de prevención y mitigación (10 min)

1. Comience enfatizando la importancia de tomar medidas proactivas para proteger los datos personales y reducir los riesgos en línea. Presente una lista de acciones sencillas que los participantes puedan adoptar de inmediato, como:

- Usar contraseñas fuertes y únicas y actualizarlas periódicamente.
- Habilitación de la autenticación multifactor (MFA) para cuentas críticas.
- Evitar enlaces y archivos adjuntos sospechosos verificando sus fuentes.
- Revisar la configuración de privacidad en redes sociales y aplicaciones.
- Mantener el software actualizado para abordar vulnerabilidades de seguridad.

Explique cómo estas acciones pueden mitigar eficazmente los riesgos comunes en línea.

2. Mantenga a los participantes en sus grupos y proporcióneles la lista de acciones. Pídales que analicen y completen las siguientes tareas:

1. Discusión en grupo:

- Identifique qué acciones ya practican y cuáles les resultan desafiantes.
- Analice por qué ciertas estrategias podrían ser más difíciles de implementar y proponga ideas para superar estos desafíos.

2. Responder preguntas clave:

- ¿Qué estrategia crees que es la más eficaz para mantenerte seguro en línea?
- “¿Cómo puedes recordarte a ti mismo que debes desarrollar mejores hábitos, como revisar periódicamente la configuración de privacidad o evitar enlaces peligrosos?”

3. Compartir nuevas estrategias:

- Cada grupo selecciona una nueva estrategia que planea adoptar, explica por qué es importante y la comparte con los demás.

Paso 3: Enfoques de prevención y mitigación (10 min)

3. Concluya la actividad pidiendo a cada participante que reflexione individualmente sobre un hábito o herramienta que se comprometerá a usar de inmediato para mejorar su seguridad en línea. Pídales que lo escriban en una nota adhesiva. Anime a los participantes a pensar en cómo pueden compartir este hábito con amigos, familiares o colegas para promover un entorno en línea más seguro de forma colectiva.

Paso 4: Reflexión y aplicación (5 min)

1. Reflexión individual:
   - Pregunte a los estudiantes: "¿Qué hábito en línea puedes cambiar para mejorar la seguridad?"
   - Los participantes escriben sus respuestas en notas adhesivas.
2. Discusión entre pares:
   - Forme parejas con los participantes para que compartan sus objetivos y sugieran pasos viables.
3. Resumen:
   - Concluya con una conclusión motivadora. Podría ser, por ejemplo: «Pequeños cambios en tu comportamiento en línea pueden marcar una gran diferencia en tu seguridad y la de tu comunidad».

Conclusiones clave:
Los participantes deben finalizar la sesión con una comprensión clara de cómo identificar ciberamenazas y contenido inapropiado, como intentos de phishing, mensajes manipuladores o enlaces sospechosos. Resalte la importancia de estrategias prácticas de seguridad, como el uso de contraseñas seguras, la activación de la autenticación multifactor y la personalización de la configuración de privacidad para proteger la información personal.
Invite a los participantes a adoptar una mentalidad proactiva, fomentando el pensamiento crítico y manteniendo conversaciones abiertas sobre los riesgos en línea. Refuerce estos principios mediante la práctica regular y compartiendo conocimientos, creando un efecto dominó que promueva hábitos en línea más seguros en sus comunidades.

Seguimiento y actividades en casa:
Pida a los participantes que:

- Revise su configuración personal de redes sociales.
- Pruebe herramientas como Malwarebytes Browser Guard o filtros de contenido.
- Comparte una estrategia aprendida con un amigo o familiar.

Consejos para profesores:
Haga que las lecciones sean atractivas utilizando ejemplos reales y recursos visuales claros para explicar los riesgos en línea y las estrategias prácticas de seguridad. Fomente debates interactivos para que los participantes conecten con el material. Las actividades prácticas, como la creación de guías de seguridad, ayudan a consolidar los conceptos. Mantenga un ambiente de apoyo y apertura donde se abran las preguntas y destaque los beneficios a largo plazo de los hábitos seguros en línea. Refuerce las lecciones clave mediante tareas de seguimiento o reflexiones grupales para asegurar que los participantes retengan y apliquen lo aprendido.

Seguimiento y actividades en casa:

Pida a los participantes que:

- Revise su configuración personal de redes sociales.
- Pruebe herramientas como Malwarebytes Browser Guard o filtros de contenido.
- Comparte una estrategia aprendida con un amigo o familiar.

Consejos para profesores:

Haga que las lecciones sean atractivas utilizando ejemplos reales y recursos visuales claros para explicar los riesgos en línea y las estrategias prácticas de seguridad. Fomente debates interactivos para que los participantes conecten con el material. Las actividades prácticas, como la creación de guías de seguridad, ayudan a consolidar los conceptos. Mantenga un ambiente de apoyo y apertura donde se abran las preguntas y destaque los beneficios a largo plazo de los hábitos seguros en línea. Refuerce las lecciones clave mediante tareas de seguimiento o reflexiones grupales para asegurar que los participantes retengan y apliquen lo aprendido.

Herramientas

CyberWise

CyberWise es una plataforma educativa que ofrece herramientas, recursos y guías para ayudar a las personas, especialmente a padres, educadores y estudiantes, a comprender la seguridad en línea. Ofrece módulos para reconocer ciberamenazas como el phishing, el ciberacoso y el contenido inapropiado, además de estrategias para mitigar los riesgos.

www.cyberwise.org

Malwarebytes Browser Guard

Esta extensión gratuita para navegadores protege a los usuarios contra phishing, estafas, malware y contenido inapropiado. Bloquea activamente sitios web y anuncios dañinos, garantizando una navegación más segura para todos los usuarios, no solo para los niños.

www.malwarebytes.com

Referencias

- CyberWise. (s.f.). Recuperado de https://www.cyberwise.org
- Dalby, J. (15 de enero de 2021). Cómo evitar contenido inapropiado. Gabb Now. Recuperado de https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (25 de septiembre de 2023). Evolución de la amenaza a la ciberseguridad: Panorama general de la escala de la ciberamenaza. Recuperado de https://figshare.com/ndownloader/files/42443952
- Lynch, M. (5 de abril de 2024). 19 maneras sencillas de bloquear contenido inapropiado. The Tech Edvocate. Recuperado de https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (21 de febrero de 2024). Navegando el panorama de la ciberseguridad: Una revisión exhaustiva de ciberataques, tendencias emergentes y desarrollos recientes. Recuperado de https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (s.f.). Recuperado de https://www.malwarebytes.com/browserguard
- Roy, R. (23 de agosto de 2021). ¿Qué es una ciberamenaza? Definición, tipos, búsqueda, mejores prácticas y ejemplos. Recuperado de https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (s.f.). 10 tipos de amenazas y soluciones a la ciberseguridad. Recuperado de https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

PRUEBA

1. ¿Cuál es una señal clave de un intento de phishing?
A. Recibir un mensaje de una cuenta previamente desconocida pero verificada
B. Un correo electrónico sin enlaces, imágenes ni archivos adjuntos
C. Un correo electrónico que lo insta a actuar de inmediato, a menudo con mala gramática
D. Un mensaje de un remitente conocido que solicita información de rutina

2. ¿Qué comportamiento podría aumentar el riesgo de amenazas cibernéticas?
A. Actualizar regularmente sus dispositivos y aplicaciones
B. Hacer clic en enlaces en correos electrónicos sin verificar al remitente
C. Usar autenticación de dos factores para cuentas en línea
D. Revisar la configuración de privacidad en las redes sociales una vez al mes

3. ¿Qué hábito ayuda a evitar ser víctima de amenazas cibernéticas?
A. Usar un administrador de contraseñas para crear y almacenar contraseñas únicas
B. Aceptar todos los permisos al instalar aplicaciones para mayor comodidad
C. Compartir contraseñas con amigos o familiares de confianza para tener una alternativa en caso de olvidarlas
D. Ignorar las advertencias de seguridad de su navegador

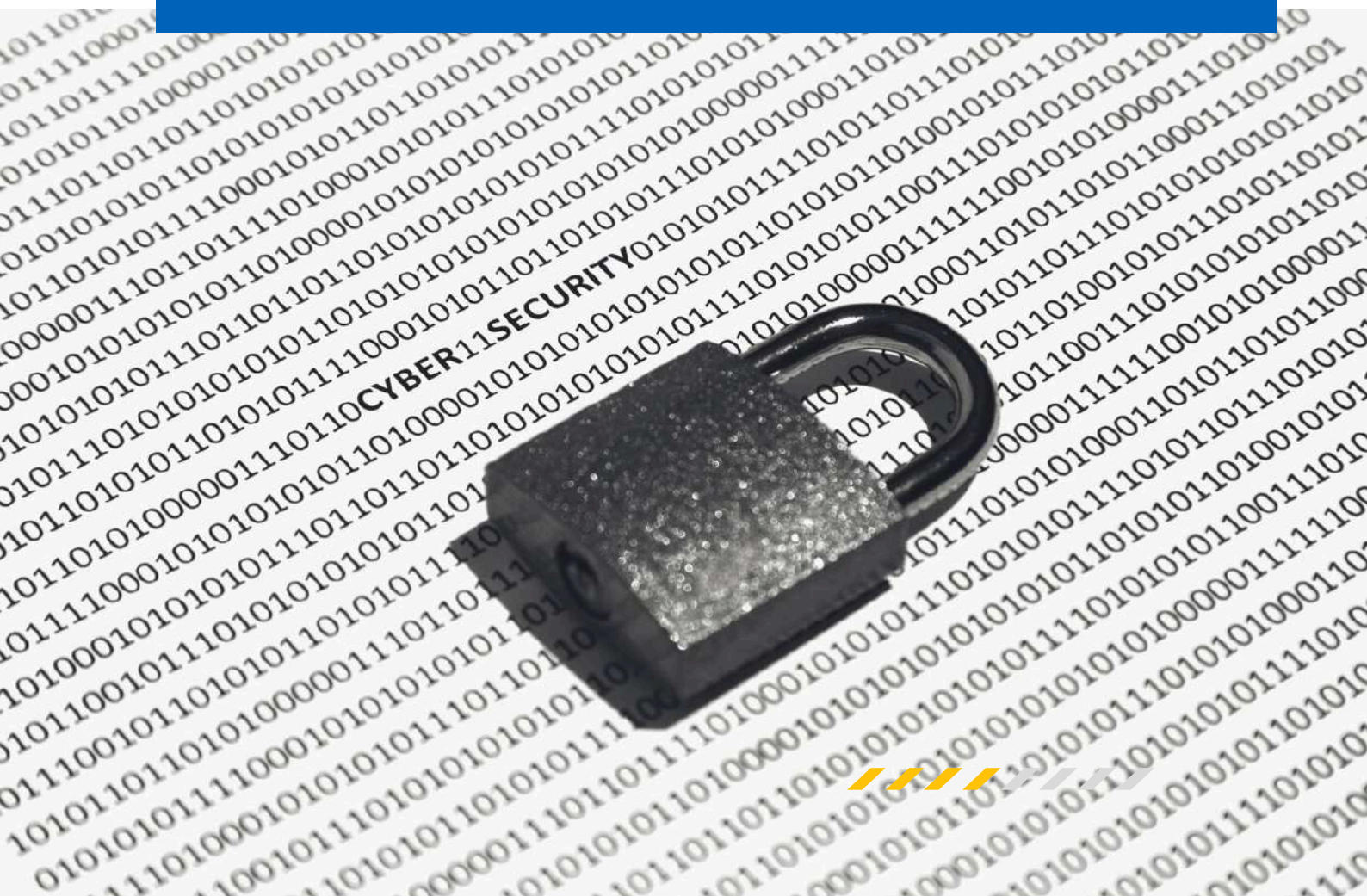
PRUEBA

4. ¿Qué hace que un enlace sea sospechoso y potencialmente dañino?
A. Utiliza cifrado HTTPS
B. Redirige a otro sitio web
C. Contiene caracteres o dominios inusuales
D. Lo comparte un amigo en un mensaje directo

5. ¿Cuál estrategia es la más efectiva para prevenir la exposición a contenido inapropiado?
A. Mantener al mínimo cualquier interacción en línea
B. Desactivar todas las notificaciones en sus dispositivos
C. Confiar únicamente en el software antivirus
D. Uso de filtros de contenido y ajuste de la configuración de privacidad

Soluciones

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



ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

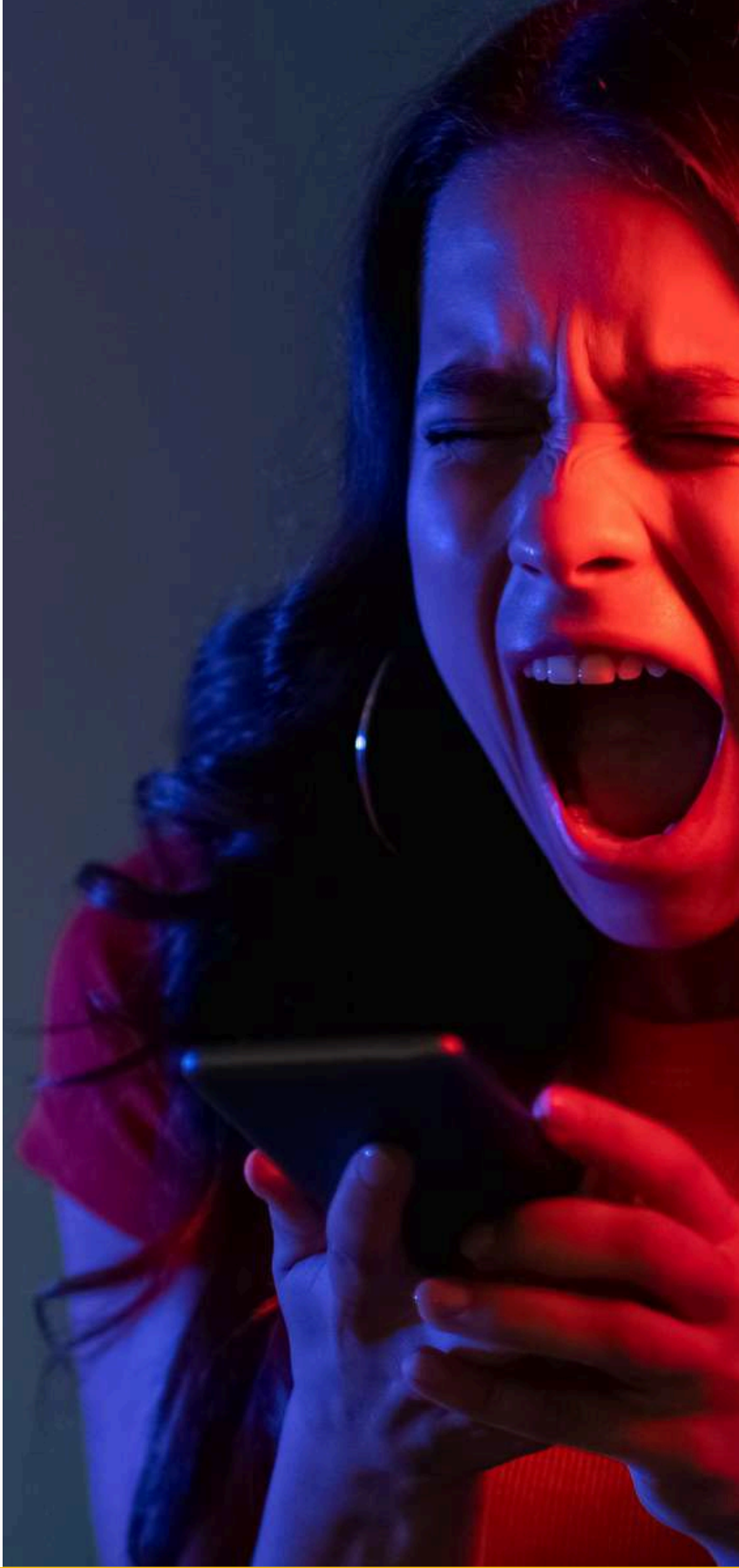
LABC

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.