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 5.1

Introducción a los fundamentos de la ciberseguridad

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 5.1

Introducción a los fundamentos de la ciberseguridad

Objetivos:

- Desarrollar una comprensión clara de los conceptos centrales de la ciberseguridad, incluidos términos clave como amenazas, vulnerabilidades y riesgos.
- Identificar amenazas en línea predominantes, como phishing, malware, ransomware y ataques de ingeniería social, y comprender su impacto.
- Fomentar una mentalidad proactiva para identificar y responder a posibles incidentes de ciberseguridad.

Mensaje(s) clave:

- Ya sea que usted sea un individuo, una pequeña empresa o una empresa global, comprender las prácticas básicas de ciberseguridad es esencial para proteger su huella digital.
- Implementar medidas preventivas simples puede ahorrar mucho tiempo, dinero y estrés en comparación con la recuperación de un ciberataque.

TIPO DE LECCIÓN:

Descripción general de la lección

En el mundo digital actual, comprender los fundamentos de la ciberseguridad ya no es opcional: es una necesidad. Esta lección te presenta los principios básicos de la ciberseguridad, las amenazas comunes y maneras prácticas de mejorar la seguridad en línea. Juntos, exploraremos cómo proteger los activos digitales personales y profesionales, fomentando una cultura de ciberconciencia y resiliencia.

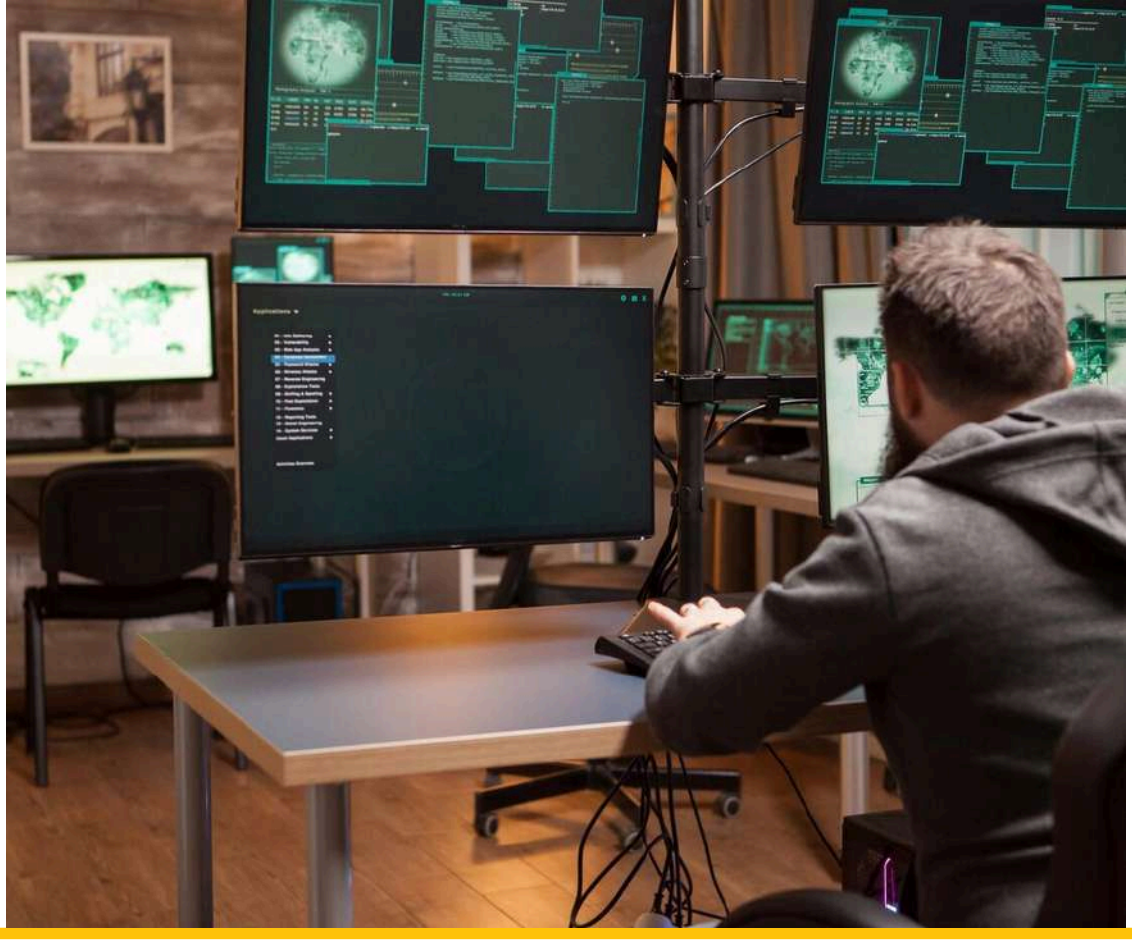
El taller está organizado en 4 pasos:

1: Introducción a los conceptos básicos de ciberseguridad (15 min)

2: Identificación de amenazas cibernéticas comunes (10 min)

3: Estrategias para las mejores prácticas de ciberseguridad (10 min)

4: Reflexión final y conclusiones clave (5 min)



Paso 1

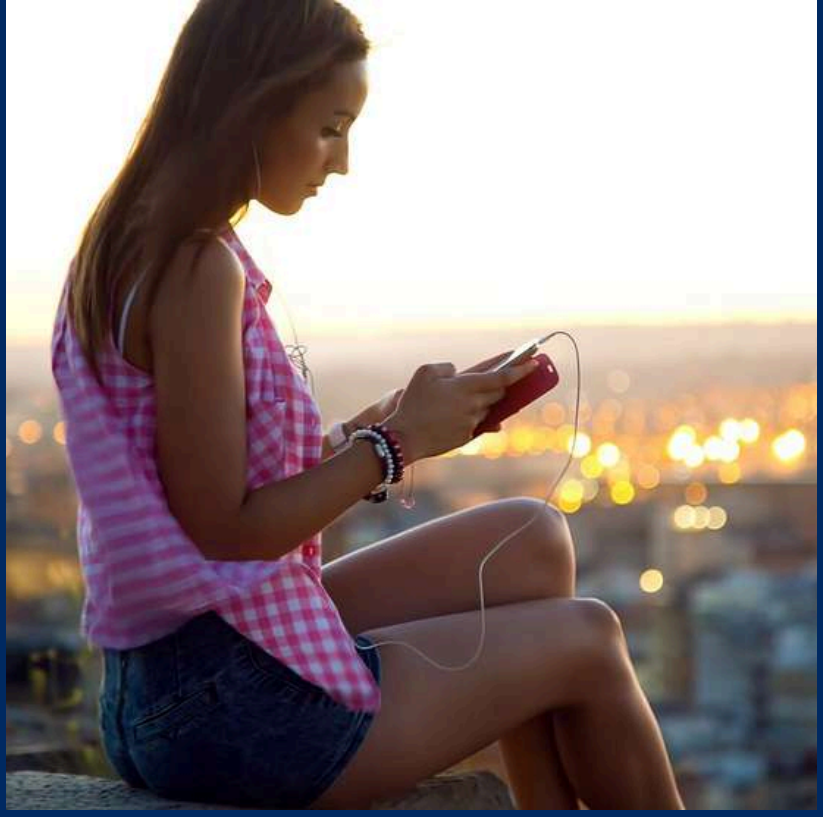
Introducción a los conceptos básicos de ciberseguridad

Comencemos con un breve video que presenta el concepto de ciberseguridad. En nuestra vida diaria, usamos constantemente herramientas digitales, pero ¿con qué frecuencia nos detenemos a considerar su seguridad? La ciberseguridad es esencial para mantenernos seguros, tanto a nosotros mismos como a nuestra información personal, en el mundo digital. Hoy profundizaremos en los fundamentos de la ciberseguridad y exploraremos su importancia.

Veamos este vídeo juntos: https://youtu.be/inWWhr5tnEA?si=Pxp1YyvjrFdLoo38

Ahora que hemos visto el vídeo, analicemos:

1. ¿Qué fue lo que más te llamó la atención sobre la ciberseguridad en el vídeo?
2. ¿Por qué crees que la ciberseguridad es importante en nuestra vida diaria?



Paso 1

Introducción a los conceptos básicos de ciberseguridad

La ciberseguridad no se trata solo de proteger sistemas; también implica comprender nuestro propio comportamiento en línea. La forma en que interactuamos con las herramientas digitales puede fortalecer nuestra seguridad o hacernos vulnerables a las amenazas.

Ahora es el momento de tomarnos un momento para reflexionar sobre nuestra vida digital.

Escriba las respuestas a las siguientes preguntas:

1. ¿Con qué frecuencia piensas en la seguridad de tus actividades en línea?
2. ¿Puedes identificar algún hábito que pueda poner en riesgo tu información personal?

¡Prepárate para compartir tus pensamientos!

Paso 2

Identificación de amenazas cibernéticas comunes

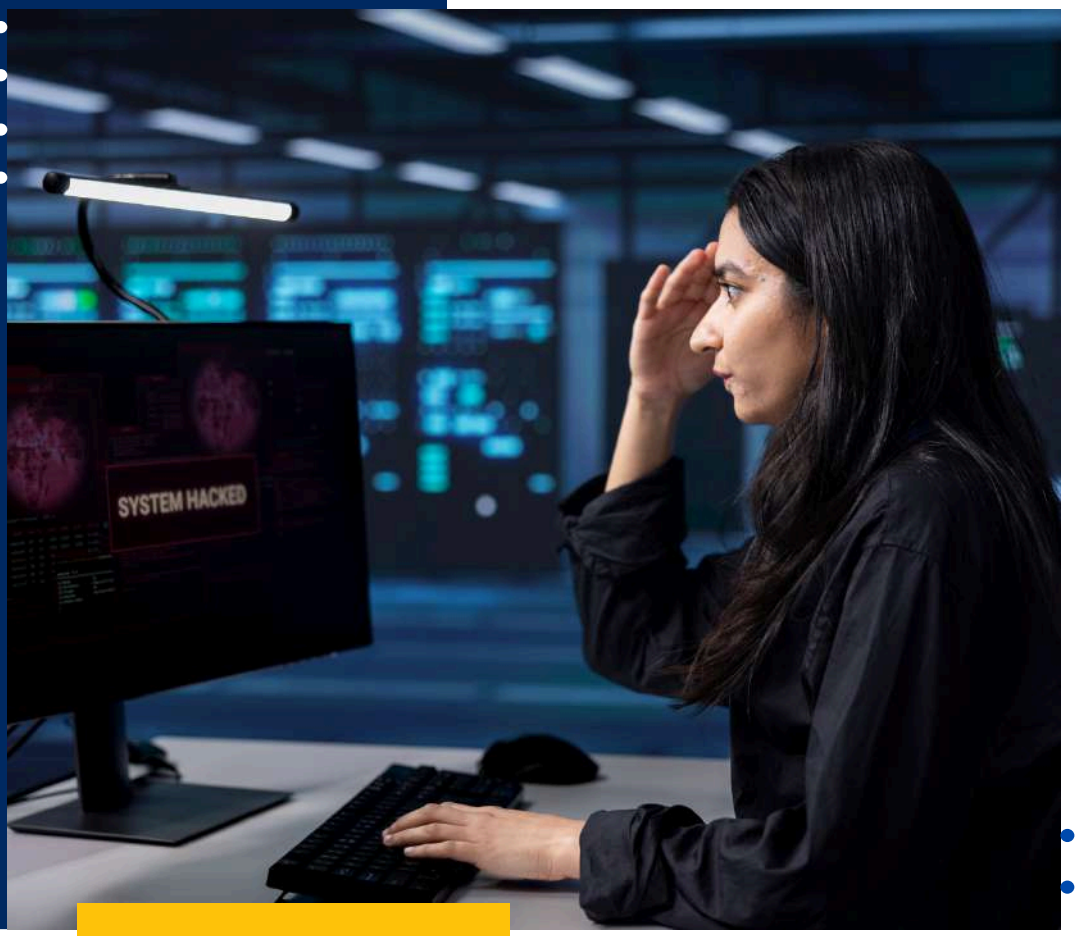
Analicemos con más detalle los tipos de amenazas cibernéticas que podríamos encontrar.

Internet es un espacio vasto y lleno de oportunidades, pero también conlleva riesgos. Las ciberamenazas pueden afectar a cualquier persona, en cualquier lugar, por lo que es crucial comprender su naturaleza e impacto. En este paso, exploraremos los distintos tipos de amenazas y cómo pueden afectarnos.

Lea el artículo: IBM: Tipos de ciberamenazas

El artículo destaca:

- Los diferentes tipos de amenazas cibernéticas, incluidos el phishing, el ransomware y el malware.
- Cómo operan estas amenazas y a quién se dirigen.
- Ejemplos de los daños que pueden causar.



Paso 2

Identificación de amenazas cibernéticas comunes

Después de leer el artículo, considere lo siguiente:

1. ¿Qué tipo de amenaza cibernética le resultó más preocupante y por qué?
2. ¿Usted o alguien que conoce ha experimentado alguna de estas amenazas?
3. ¿Cómo cree usted que comprender estas amenazas puede ayudar a prevenirlas?

Después de eso, escribe un ejemplo o escenario de la vida real (puede ser hipotético) donde podría ocurrir una de estas amenazas cibernéticas mencionadas en el artículo.

¡Prepárate para compartir tu ejemplo y discutirlo con el grupo!

Paso 3

Estrategias para las mejores prácticas en ciberseguridad

Ahora, centrémonos en protegernos en línea.

Si bien las ciberamenazas evolucionan constantemente, existen medidas sencillas y eficaces que podemos tomar para proteger nuestra información y mantener la seguridad. Al adoptar las mejores prácticas de ciberseguridad, podemos minimizar los riesgos y mantenernos más seguros en nuestra vida digital.

La ciberseguridad no requiere habilidades técnicas avanzadas: pequeñas acciones intencionales pueden marcar una gran diferencia en su protección y la de sus datos.

Paso 3

Estrategias para las mejores prácticas en ciberseguridad

A continuación se presentan algunas prácticas clave a tener en cuenta:

- Cree contraseñas fuertes y únicas y cámbielas periódicamente.
- Habilite la autenticación multifactor (MFA) para mayor seguridad.
- Tenga cuidado con los enlaces y archivos adjuntos, especialmente si provienen de fuentes desconocidas.
- Mantenga el software y los dispositivos actualizados para corregir vulnerabilidades.
- Utilice conexiones Wi-Fi seguras, evitando redes públicas siempre que sea posible.

Actividad: Lista de verificación de mejores prácticas de ciberseguridad

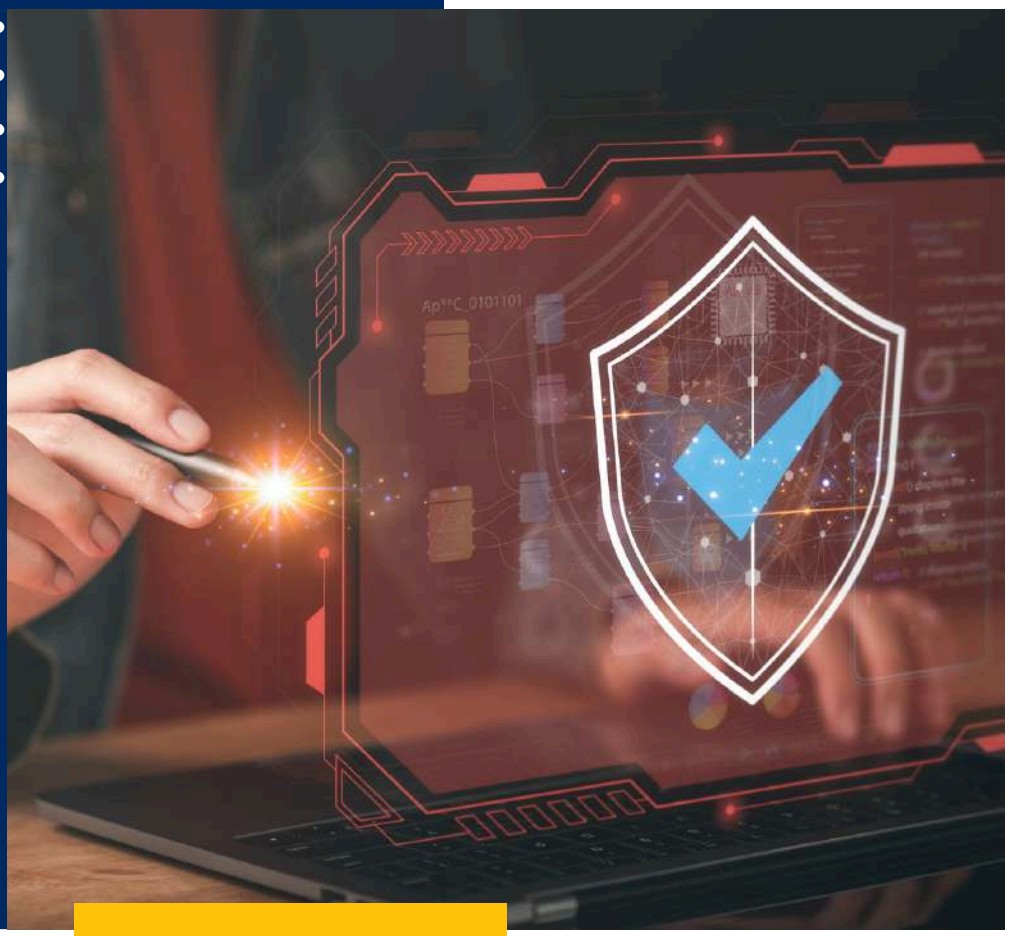
Paso 1: Evalúa tus hábitos actuales

- Reflexiona sobre tus comportamientos y hábitos actuales en línea. ¿Existen áreas en las que podrías estar poniéndote en riesgo?

Ejemplo: “Uso la misma contraseña en varias cuentas” Paso 2: Crear un plan

- Anote un paso viable para cada concepto clave mencionado anteriormente. Por ejemplo:

Contraseñas seguras: “Instalaré un administrador de contraseñas para generar y almacenar contraseñas seguras”, etc.



Paso 3

Estrategias para las mejores prácticas en ciberseguridad

Paso 3: Compartir en grupo

- Comparte una de tus acciones planificadas con un compañero o con el grupo.
- Analice cómo estos pasos podrían ayudarle a mejorar su seguridad digital.
- Ofrecer consejos o sugerencias sobre medidas adicionales que otros pueden tomar.

Al final, responde mentalmente la pregunta clave de reflexión: ¿Qué hábito o estrategia puedes comenzar a practicar hoy para mejorar de inmediato tu seguridad en línea?

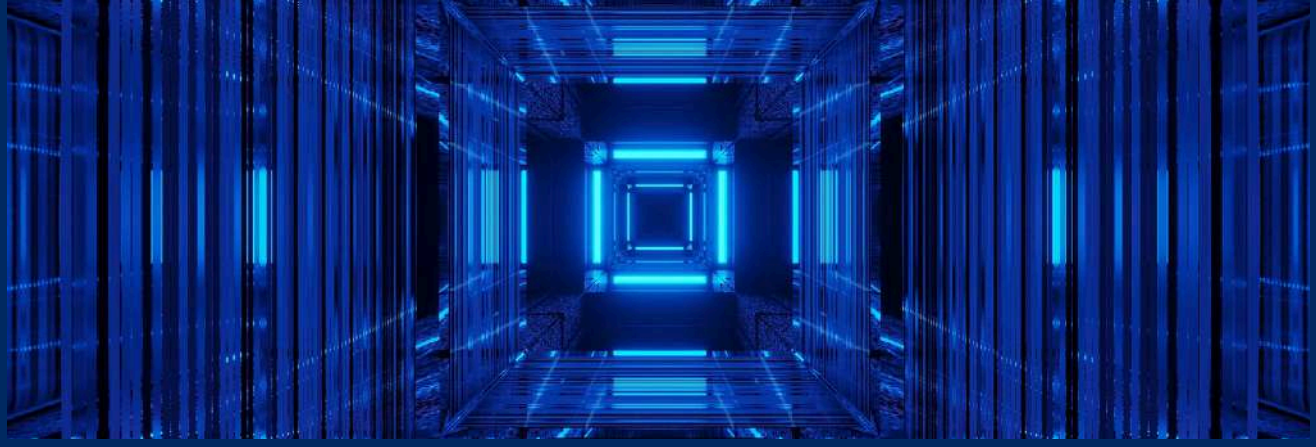
Paso 4

Reflexión final y conclusiones clave

Para terminar, tomémonos un momento para reflexionar sobre todo lo que hemos cubierto en esta lección y cómo podemos usar este conocimiento en el futuro.

Piensa en tus hábitos en línea: ¿te inspira algún cambio después de la charla de hoy? Si es así, ¿cuál sería el primer paso que darías para mejorar tu ciberseguridad?
Ahora, piensa en cómo podemos ayudar a los demás. ¿Qué consejo o hábito sencillo de este taller podrías compartir con un amigo o colega para ayudarle a mantenerse seguro en línea?

¡Gracias a todos por su participación activa y sus reflexivas contribuciones de hoy!



Resumen de las conclusiones clave

- La ciberseguridad es para todos. Comprender las amenazas y adoptar las mejores prácticas nos ayuda a mantenernos seguros en línea.
- Los pequeños pasos marcan una gran diferencia. Herramientas como los administradores de contraseñas y las actualizaciones periódicas pueden mejorar significativamente tu seguridad.
- Manténgase informado. Las ciberamenazas evolucionan constantemente, por lo que mantenerse al día con los últimos consejos y herramientas es esencial para la seguridad a largo plazo.
- Sé proactivo. Cuanto más adoptes hábitos seguros, más seguros estarán tú y quienes te rodean.

Instrucciones para trabajadores juveniles, educadores y

Objetivo:

Esta lección tiene como objetivo ayudar a trabajadores juveniles, educadores y docentes a dotar a los jóvenes de conocimientos esenciales sobre ciberseguridad. Mediante interesantes debates, actividades y reflexiones, los participantes comprenderán las ciberamenazas comunes, aprenderán las mejores prácticas de seguridad en línea y crearán planes de acción para protegerse en el mundo digital.

Materiales necesarios:

- Conexión a Internet para reproducción de vídeos o artículos
- Proyector y pantalla
- Oradores
- Acceso a herramientas de ciberseguridad recomendadas
- Papel gráfico o marcadores de pizarra blanca
- Bolígrafos o lápices
- Hojas de papel

Paso 1: Introducción a los conceptos básicos de ciberseguridad (15 min)

1. Comience por involucrar a los participantes con un ejemplo que se pueda relacionar con ellos: "Piense en la última vez que usó una aplicación nueva o visitó un sitio web. ¿Se detuvo a pensar en cuán seguros están sus datos?"

2. Resalte la relevancia de la ciberseguridad: Explique que la ciberseguridad no es solo para profesionales de TI; es una habilidad fundamental para todos en la era digital actual. Enfatice cómo la ciberseguridad ayuda a proteger la información personal, profesional y organizacional.

3. Describa claramente los objetivos de la sesión.

4. Actividad: Proyección de vídeo y debate:

- Reproduce el vídeo: “¿Qué es la ciberseguridad?” (mira aquí).
- Proporcione a los participantes preguntas orientadoras después de mirar.

5. Después del vídeo, dirija una discusión:

- ¿Qué fue lo que más te sorprendió de la ciberseguridad?
- ¿Crees que la ciberseguridad es importante para todos? ¿Por qué sí o por qué no?
- ¿Cuáles son los riesgos de no prestar atención a la seguridad en línea?

Paso 1: Introducción a los conceptos básicos de ciberseguridad (15 min)

6. Reflexión personal: Pida a los participantes que se tomen unos minutos para escribir sus pensamientos:

- ¿Con qué frecuencia considera la seguridad de sus actividades en línea?
- ¿Puedes identificar uno o dos hábitos que podrían poner en riesgo tu información personal?
- ¿Qué cambios crees que podrías hacer para mejorar tu seguridad en línea?

7. Fomentar el intercambio en parejas o grupos pequeños:

- Opción 1: Comparte un hábito que consideres riesgoso y pide consejos a tu grupo sobre cómo mejorarlo.
- Opción 2: Analice si alguna vez ha experimentado o escuchado sobre una amenaza cibernética y cómo se manejó.

8. Si los participantes prefieren no compartir en grupos, permítales escribir un cambio que se comprometen a realizar y enviarlo de forma anónima al facilitador para su posterior discusión.

Paso 2: Identificación de amenazas cibernéticas comunes (10 min)

1. Comparta el artículo IBM: Tipos de amenazas cibernéticas o un resumen impreso de sus puntos clave.
2. Permita que los participantes tengan cinco minutos para leer y anotar las amenazas que les resulten más preocupantes, centrándose en su funcionamiento y su impacto potencial.
3. Discusión:
Facilitar una conversación grupal:
- "¿Qué ciberamenaza le parece más preocupante y por qué?"
- ¿Usted o alguien que conoce ha sufrido alguna de estas amenazas? ¿Qué ocurrió?

4. Agregue información si es necesario:
Resalte estadísticas o ejemplos para enriquecer la discusión, como correos electrónicos de phishing o ataques de ransomware.
5. Actividad de escenario:
Pídeles a los participantes que escriban un ejemplo breve, real o hipotético, que involucre una amenaza cibernética, como por ejemplo:
- Phishing: "Un correo electrónico fraudulento engañó a alguien para que compartiera los datos de acceso de su cuenta"
- Malware: "Al hacer clic en un enlace sospechoso, se descargó un virus y se bloquearon los archivos"

6. Comparta escenarios en el grupo y facilite una discusión en torno a:
- "¿Qué salió mal en el escenario?"
- "¿Cómo se podría haber evitado la situación?"
- ¿Qué medidas preventivas habrían ayudado?

7. Opcionalmente, puede contribuir al debate resaltando estrategias preventivas del mundo real para cada tipo de amenaza.

Paso 3: Estrategias para las mejores prácticas de ciberseguridad (10 min)

1. Resumen de las mejores prácticas:
    - Presentar estrategias sencillas y efectivas:
    - Utilice contraseñas fuertes y únicas.
    - Habilitar la autenticación multifactor (MFA).
    - Evite enlaces y archivos adjuntos sospechosos.
    - Mantenga el software y los dispositivos actualizados.
    - Utilice una red Wi-Fi segura o una VPN.
- Utilice ejemplos de la vida real o demostraciones breves para mostrar el impacto de cada estrategia.

2. Si es posible, demuestre o explique la configuración de una herramienta (incluida en la sección “Herramientas” para que sea más fácil de entender).

3. Actividad: lista de verificación de ciberseguridad:

- Distribuya una plantilla de lista de verificación simple con las estrategias enumeradas.
- Pídeles a los participantes que escriban un paso viable para cada uno.
- Ejemplo: “Habilitaré MFA en mi correo electrónico”.
- Anime a los participantes a centrarse en acciones simples e inmediatas y ayude a aclarar los pasos si es necesario.

4. Compartir en grupo:

- Los participantes comparten un paso que planean dar.
- Ofrezca comentarios rápidos y fomente el debate sobre los beneficios de estos cambios.
- Anime a los participantes a revisar periódicamente su lista de verificación para actualizar sus hábitos.

Paso 4 Reflexión final y conclusiones clave (5 min)

1. Reforzar el aprendizaje y motivar a los participantes a aplicar lo aprendido.

2. Pregunte a los participantes:

- "¿Qué hábito planeas cambiar o adoptar a partir de hoy?"
- "¿Cómo compartirás lo que has aprendido con los demás?"

3. Compartir en grupo:

    - Invite a voluntarios a compartir sus reflexiones o una conclusión clave.

4.Mensaje de cierre:

- Recuerde a los participantes: «La ciberseguridad es responsabilidad de todos. Pequeñas acciones intencionadas pueden marcar una gran diferencia para mantenerse seguros en línea».
- Agradezca a todos por su participación activa y anímelos a actuar de inmediato.

Conclusiones clave:

Enfatice a los participantes que la ciberseguridad es una habilidad que todos necesitan, independientemente de su experiencia técnica. Utilice los puntos clave de la lección para destacar cómo comprender las amenazas comunes y adoptar medidas preventivas, como usar contraseñas seguras o habilitar la autenticación multifactor (MFA), puede reducir drásticamente los riesgos en línea. Anime a los participantes a adoptar una mentalidad proactiva estableciendo objetivos sencillos y alcanzables para mejorar sus hábitos en línea. Refuerce estas conclusiones mediante debates o actividades de seguimiento que repasen estos conceptos, asegurando que los participantes se mantengan alerta y motivados para mantener prácticas sólidas de ciberseguridad.

Seguimiento y actividades en casa

Anime a los participantes a practicar lo aprendido mediante el seguimiento de sus actividades en línea durante la próxima semana. Pueden identificar las áreas donde se sienten más vulnerables e implementar una nueva estrategia de ciberseguridad cada día. Además, sugiérales que prueben herramientas como LastPass o Bitdefender en casa y compartan sus experiencias con el grupo en una sesión de seguimiento.

Consejos para profesores:

Integre temas de ciberseguridad en las conversaciones o clases diarias utilizando ejemplos reales relacionados con las experiencias de los estudiantes, como la seguridad en redes sociales o estafas comunes. Utilice métodos interactivos, como debates en grupo o juegos de rol, para que el tema sea atractivo y práctico. Revise regularmente el progreso y brinde apoyo para reforzar la importancia de desarrollar hábitos sólidos de ciberseguridad.

Herramientas

LastPass

LastPass es una potente herramienta de gestión de contraseñas diseñada para mejorar la ciberseguridad mediante la generación y el almacenamiento seguro de contraseñas seguras y únicas para todas las cuentas en línea. Elimina la necesidad de recordar múltiples contraseñas complejas, almacenándolas en una bóveda digital cifrada, accesible solo con una contraseña maestra.

www.lastpass.com

Bitdefender

Bitdefender es una herramienta avanzada de ciberseguridad que ofrece protección integral contra malware, phishing, ransomware y otras amenazas en línea. Combina un potente software antivirus con medidas inteligentes antiphishing para brindar seguridad multicapa para uso personal y profesional.

www.bitdefender.com

Referencias

- Bitdefender. (s.f.). Recuperado de https://www.bitdefender.com
- Academia de Redes de Cisco. (s.f.). Fundamentos de Ciberseguridad. Academia de Redes de Cisco: Aprenda Ciberseguridad, Python y más. Recuperado de https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US
- IBM. (25 de marzo de 2024). Tipos de ciberamenazas. Recuperado de https://www.ibm.com/think/topics/cyberthreats-types
- 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
- LastPass. (s.f.). Recuperado de https://www.lastpass.com
- Simplilearn. (10 de junio de 2020). ¿Qué es la ciberseguridad? | ¿Cómo funciona? | Ciberseguridad en 7 minutos | Ciberseguridad | Simplilearn. [Video]. YouTube. https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo

PRUEBA

1. ¿Cuál es uno de los principales objetivos de la ciberseguridad?
A. Garantizar que nadie pueda acceder a Internet sin permiso. B. Permitir que las empresas monitoreen la actividad de los usuarios. C. Proteger los activos digitales mediante la gestión de riesgos y vulnerabilidades. D. Bloquear todos los correos electrónicos de remitentes desconocidos.

2. ¿Cuál de las siguientes opciones demuestra el uso de la autenticación multifactor (MFA)?
A. Iniciar sesión respondiendo una pregunta de seguridad B. Usar su contraseña de correo electrónico y un correo electrónico de respaldo para la recuperación C. Combinar una contraseña con un código temporal enviado a su teléfono D. Guardar contraseñas en un archivo cifrado en su computadora

3. ¿Qué hace que el phishing sea diferente de otras amenazas en línea?
A. Implica hackear directamente los sistemas sin interacción del usuario. B. Utiliza tácticas engañosas para engañar a los usuarios y lograr que compartan información confidencial. C. Se propaga a través de dispositivos físicos como unidades USB.
D. Funciona exclusivamente instalando malware en un ordenador.

PRUEBA

4. ¿Cómo mejora la ciberseguridad la actualización de su software?
A. Mejora el diseño y la usabilidad de sus aplicaciones. B. Reduce las posibilidades de que los errores interfieran con sus tareas. C. Cierra las vulnerabilidades de seguridad que los atacantes podrían explotar. D. Permite una mejor compatibilidad con hardware más antiguo.

5. ¿Por qué es beneficioso utilizar un gestor de contraseñas?
A. Garantiza que todas sus contraseñas estén respaldadas en un servidor compartido. B. Cierra su sesión de cuentas automáticamente después de un tiempo establecido. C. Crea y almacena de forma segura contraseñas complejas para cada cuenta.
D. Te avisa cuando alguien accede a tu correo electrónico sin permiso.

Soluciones

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

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

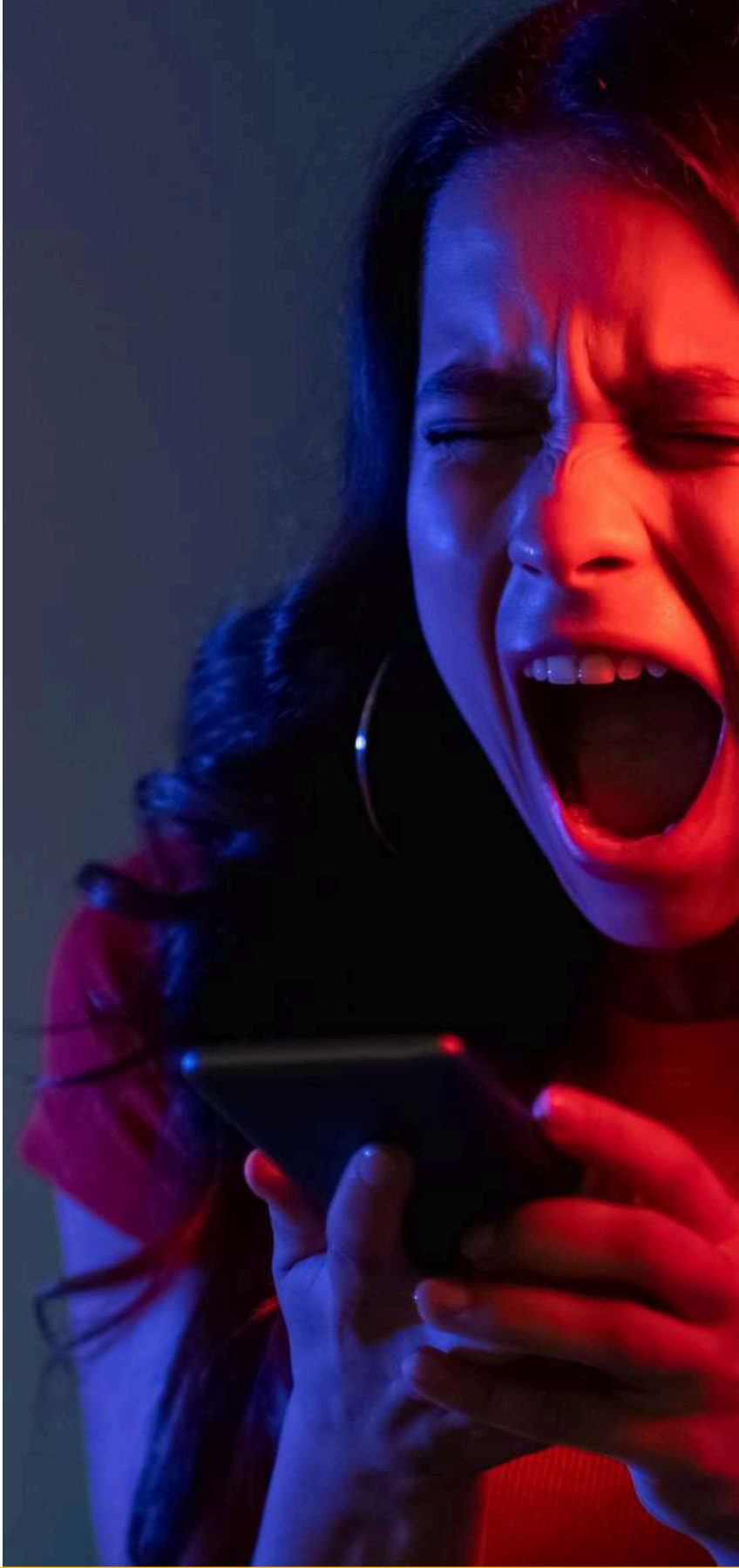
LABC

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.