13+

IDENTIFICAR Y EVITAR LOS RIESGOS EN LÍNEA: PHISHING, MALWARE Y ESTAFAS

TEMA: Navegación segura por Internet

TEMA DE LA LECCIÓN: Concienciación sobre ciberseguridad

DURACIÓN: 45 minutos (1 Lección); 1-1.5 horas (Preparación)

OBJETIVOS DE APRENDIZAJE:

Objetivo principal de la lección

Educar a los alumnos sobre los distintos riesgos en línea, en concreto el phishing, el malware y las estafas, y dotarles de los conocimientos y habilidades necesarios para identificar y evitar estas amenazas con el fin de garantizar su seguridad en línea.

Competencias que adquirirán los alumnos

Los estudiantes adquirirán un pensamiento crítico y habilidades analíticas para identificar y mitigar las amenazas en línea, competencia técnica en el uso de herramientas de ciberseguridad y una mejor alfabetización digital. También desarrollarán la responsabilidad personal para la seguridad en línea, habilidades de comunicación eficaces para informar de incidentes, y un enfoque proactivo para mantener la ciberseguridad.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MATERIALES/RECURSOS NECESARIOS:

- Module 2 (https://www.digi-civis.eu/e-learning)
- Canva Presentation (https://www.canva.com/design/DAGWuXDxmtY/ldGBbQBs9TK1hm_FYYv_3Q/edit)
- 10 question Quiz on Cybersecurity Practices.
- Preparation of sets of printed emails, including both phishing and legitimate ones (these emails can be sourced from Google or created by teacher for educational purposes).
- Caulfield, M., & Wineburg, S. (2024). Verified: How to Think Straight, Get Duped Less, and Make Better Decisions about What to Believe Online.
- Kallen, S. A. (2023). Spotting Online Scams and Fraud.

MÉTODOS/TÉCNICAS:

- **Presentación:** El profesor realizará una presentación para introducir el tema, explicar los conceptos clave y proporcionar ejemplos reales de phishing, malware y estafas en línea.
- **Trabajo en grupo:** Los alumnos participarán en una actividad de grupo en la que analizarán e identificarán correos electrónicos de phishing. Este ejercicio colaborativo fomentará el debate, el pensamiento crítico y el trabajo en equipo a medida que determinan qué correos electrónicos son intentos de phishing.
- **Trabajo individual:** Los alumnos completarán un cuestionario para evaluar su comprensión de las prácticas de ciberseguridad tratadas en la lección. Esta actividad permite a los alumnos aplicar individualmente lo que han aprendido y reforzar sus conocimientos sobre cómo identificar y evitar los riesgos en línea.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

RESUMEN DEL PLAN DE CLASES

PREPARACIÓN:

- Repasar a fondo el Módulo 2 de Digi-Civis para comprender los conceptos fundamentales de los riesgos en línea, incluidos el phishing, el malware y las estafas.
- Examinar los libros y vídeos recomendados para recopilar información detallada y ejemplos de la vida real que mejoren el contenido de la lección.
- Los profesores deben preparar conjuntos de correos electrónicos impresos, tanto de phishing como legítimos. Estos correos pueden ser ejemplos reales recopilados (con la información sensible eliminada) o falsos creados con fines educativos. Asegúrese de que los correos electrónicos estén en el idioma local o en inglés, en función de los conocimientos de los alumnos y del idioma de enseñanza.
- Revise la presentación de Canva proporcionada para asegurarse de que se cubren todos los puntos clave y de que los elementos visuales son atractivos e informativos.
- Imprima el cuestionario proporcionado o, si es posible, facilite el cuestionario como archivo digital para que los estudiantes lo completen utilizando dispositivos y bolígrafos digitales.

IMPLEMENTACIÓN:

1. Introducción (10 minutos)

Visión general del tema:

- Explique brevemente qué son el phishing, el malware y las estafas en línea.
- Comente por qué es importante comprender y evitar estos riesgos en línea.
- Muestre un breve videoclip que ilustre ejemplos reales de intentos de phishing y otros.

2. Actividad en grupo (15 minutos)

Simulación de phishing:

- Divida a los alumnos en pequeños grupos.
- Proporcione a cada grupo un conjunto de correos electrónicos de phishing impresos y correos electrónicos legítimos.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Pídeles que identifiquen qué correos electrónicos son intentos de phishing y que expliquen su razonamiento.
- Cada grupo presenta sus conclusiones y razonamientos a la clase.

3. Debate en clase (10 minutos)

- Haga preguntas a los alumnos sobre sus propias experiencias con correos electrónicos o actividades en línea sospechosos. Por ejemplo, comente las características comunes de los correos electrónicos de phishing (por ejemplo, saludos genéricos, lenguaje urgente, enlaces sospechosos).
- Destaque las estafas en línea más comunes (estafas de lotería, estafas de soporte técnico, estafas de compras en línea).

4. Actividad individual (10 minutos)

- Test de 10 preguntas sobre prácticas de ciberseguridad.

- Proporcionar a los alumnos un cuestionario para evaluar su comprensión de la lección.

INFORMACIÓN ADICIONAL:

- Phishing Explained In 6 Minutes https://www.youtube.com/watch?v=XBkzBrXlle0
- Ransomware In Cybersecurity https://www.youtube.com/watch?v=-KL9APUjj3E
- More New Clever Email Scams to Watch Out For https://www.youtube.com/watch?v=xEKY7lZStE4

ANEXOS:

- Presentación de Canva (https://www.canva.com/design/DAGWuXDxmtY/ldGBbQBs9TK1hm_FYYv_3Q/edit?utm_content=DAGWuXDxmtY&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton)

TAREAS:

No se requieren deberes formales para esta lección. Sin embargo, puede animar a los alumnos a que hablen con sus familiares sobre cualquier experiencia que hayan tenido con mensajes o correos electrónicos fraudulentos. Pida a los alumnos que averigüen cómo sus familiares detectaron estas estafas y qué consejos pueden ofrecer para ayudar a los alumnos a evitar riesgos similares.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

EVALUACIÓN:

Utilice estas 10 preguntas para evaluar o inspírese en ellas para crear su propio cuestionario sobre prácticas de ciberseguridad.

Cuestionario sobre prácticas de ciberseguridad

Responda a las siguientes preguntas de opción múltiple para evaluar su comprensión de las prácticas de ciberseguridad.

1. ¿Qué es el phishing?

- A) Un tipo de malware
- **B) Un método para engañar a la gente para que facilite información personal**
- C) Una forma legítima de proteger tu cuenta

2. ¿Cuál de los siguientes es un signo común de un correo electrónico de phishing?

- **A) Saludos genéricos como «Estimado cliente**
- B) Información personalizada
- C) Ortografía y gramática correctas

3. ¿Qué es el malware?

- A) Un programa informático seguro
- **B) Software dañino que puede dañar tu ordenador**
- C) Un tipo de estafa por correo electrónico

4. ¿Cuál de los siguientes es un tipo de malware?

- A) Correo electrónico de phishing
- **B) Virus**
- C) Contraseña segura

5. ¿Cómo puedes proteger tu ordenador del malware?

- **A) Mantén actualizado tu software antivirus**
- B) Haz clic en todos los enlaces de correo electrónico
- C) Comparte tus contraseñas

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

EVALUACIÓN:

6. ¿Qué debe hacer si recibe un correo electrónico de un remitente desconocido pidiéndole información personal?

- A) Responder con tus datos
- **B) Ignorar y borrar el correo**
- C) Reenviarlo a tus amigos

7. ¿Cuál de las siguientes es una estafa habitual en Internet?

- A) Ayuda genuina de soporte técnico
- **B) Premios de lotería falsos**
- C) Compras seguras en línea

8. ¿Por qué es importante utilizar contraseñas seguras y únicas para las distintas cuentas?

- **A) Para proteger cada cuenta por separado y evitar que varias cuentas se vean comprometidas**
- B) Para que sea más fácil recordar todas las contraseñas
- C) Para compartirlas fácilmente con amigos

9. ¿Qué pasos debes seguir si crees que tu dispositivo está infectado con malware?

- A) Ignorarlo
- **B) Ejecutar un escaneo de virus con un software antivirus actualizado**
- C) Seguir utilizando el dispositivo con normalidad

10. ¿Cómo puedes ayudar a tus amigos y familiares a estar seguros en Internet?

- A) Compartiendo tus contraseñas con ellos
- **B) Enseñándoles a reconocer y evitar las amenazas online**
- C) Ignorando los consejos de seguridad online

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.