PROTEGER LA INFORMACIÓN PERSONAL Y FINANCIERA

16+

TEMA: Alfabetización digital, Educación del consumidor

TEMA DE LA LECCIÓN: Cómo proteger la información personal y financiera en Internet

DURACIÓN: 60 minutos

OBJETIVOS DE APRENDIZAJE:

Objetivo principal de la lección: Enseñar a los alumnos la importancia de salvaguardar la información personal y financiera en línea, comprender las amenazas potenciales y aprender estrategias eficaces para protegerse del fraude y el robo de identidad en línea.

Competencias que adquirirán los alumnos:

- Conocimiento de las principales amenazas a la ciberseguridad (por ejemplo, phishing, malware, violación de datos).
- Capacidad para reconocer actividades, correos electrónicos y sitios web sospechosos.
- Conciencia de las prácticas seguras en línea a la hora de compartir información personal o financiera.

MATERIALES/RECURSOS NECESARIOS:

Módulo 5 (https://www.digi-civis.eu/e-learning); Proyector y ordenador para la presentación; Internet; Ejemplos de correos electrónicos de phishing, sitios web falsos.

MÉTODOS/TÉCNICAS:

- Debates en pequeños grupos
- Reflexión personal y autoevaluación
- Debate en clase y retroalimentación
- Ejercicio de role-playing

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.

PLAN GENERAL DE LA LECCIÓN

PREPARACIÓN:

- Prepare las diapositivas de la presentación del MÓDULO 5 de DIGI-CIVIS.
- Recopilar ejemplos de correos electrónicos de phishing, sitios web fraudulentos y sitios seguros para mostrarlos durante la clase.
- Crear hojas de trabajo que guíen a los alumnos en la creación de contraseñas seguras y en la identificación de intentos de phishing.

PUESTA EN PRÁCTICA:

- Introducción a las amenazas en línea (10 minutos): Explicar las amenazas online más comunes (phishing, malware, violación de datos) y por qué es crucial proteger la información personal y financiera.
- Reconocer los ataques de phishing (10 minutos): Mostrar ejemplos de correos electrónicos de phishing y sitios web fraudulentos. Hable de las señales de advertencia, como las URL sospechosas y las solicitudes urgentes de información.
- Buenas prácticas de protección (15 minutos): Enseñe a crear contraseñas seguras, a utilizar la autenticación de dos factores y a evitar las redes Wi-Fi públicas para transacciones confidenciales. Demuestre cómo comprobar la seguridad de un sitio web (por ejemplo, «https», icono de candado).
- Actividad práctica «Creación de contraseñas seguras» (10 minutos): Guíe a los alumnos en la creación de contraseñas seguras y muéstreles cómo evaluar su seguridad.
- Debate sobre un caso práctico (10 minutos): Repase una violación de datos de la vida real, discutiendo su impacto y cómo unas mejores prácticas de seguridad podrían haberla evitado.
- Reflexión (5 minutos): Los alumnos identifican una medida que tomarán para mejorar su propia seguridad 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.

INFORMACIÓN ADICIONAL:

EU OP, Shopping online within EU

EU E-Commerce Report 2023

DMA scheme

Be safe out there

ANEXOS:

Data Protection in EU (Video)

Financial literacy (video)

TAREAS:

Los alumnos deben realizar una auditoría de seguridad de sus propias cuentas en línea. Redactar una reflexión de una página sobre lo que han descubierto y las medidas que han tomado para mejorar su seguridad en línea.

EVALUACIÓN:

Revisión de los deberes para evaluar la capacidad del alumno para aplicar los principios de seguridad 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.