13+

PROTECCIÓN DE LA INFORMACIÓN PERSONAL EN PLATAFORMAS DIGITALES (CONFIGURACIÓN DE SEGURIDAD)

TEMA: Navegación segura por Internet

TEMA DE LA LECCIÓN: Ajustes de seguridad

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

OBJETIVOS DE APRENDIZAJE:

Objetivo principal: Los alumnos aprenderán a proteger la información personal confidencial en las plataformas digitales, incluida la información de identidad, los datos de las tarjetas de crédito, la información sanitaria, la dirección del domicilio, los números de teléfono y otros identificadores personales más allá del mero uso de contraseñas seguras.

Competencias adquiridas:

- Los alumnos comprenderán la importancia de proteger diversos tipos de información personal en línea.
- Aprenderán las mejores prácticas para proteger datos sensibles como la información del DNI, los datos de la tarjeta de crédito, los historiales médicos, las direcciones y los números de teléfono.
- Serán conscientes de los riesgos potenciales asociados a una protección inadecuada de la información personal y de cómo mitigarlos.

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:

- Módulo 2 (https://www.digi-civis.eu/e-learning)
- Un dispositivo con acceso a Internet (si está disponible) para demostrar la configuración de seguridad relacionada con la información personal.
- Escenarios y ejemplos preparados de antemano (a continuación) para debatir durante la clase.
- Preguntas del cuestionario (a continuación).

MÉTODOS/TÉCNICAS:

- **Presentación:** El profesor ofrece una visión general concisa y atractiva de los temas clave, haciendo hincapié en la importancia de proteger diversos tipos de información personal en línea.
- **Trabajo en grupo** (análisis de casos hipotéticos): Los alumnos se dividen en pequeños grupos para debatir y resolver situaciones concretas relacionadas con la protección de la información personal.
- **Cuestionario:** Un breve cuestionario para evaluar la comprensión por parte de los alumnos de los conceptos clave tratados durante la lección. Esto ayuda a reforzar el aprendizaje y a identificar las áreas que pueden necesitar más aclaraciones.

PLAN GENERAL DE LA LECCIÓN

PREPARACIÓN:

- Repasar a fondo el Módulo 2 que cubre los fundamentos de la configuración de seguridad en las plataformas digitales.
- Familiarizarse con las configuraciones de seguridad específicas relacionadas con la información personal, como la protección del DNI, la seguridad de las tarjetas de crédito y la salvaguarda de la información sanitaria, las direcciones particulares y los números de teléfono.
- Imprime y recorta los escenarios para la actividad de trabajo en grupo.
- Imprime las preguntas del cuestionario que se utilizará para evaluar la comprensión de los alumnos al final de la lección.

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.

IMPLEMENTACIÓN:

1. Introducción/Presentación breve (15 minutos):

Visión general del tema: Explicar los conceptos esenciales relacionados con la información del DNI, los datos de las tarjetas de crédito, las fechas de nacimiento, los historiales médicos y las direcciones particulares.

Explicación: La información de identidad incluye identificadores personales como los números de la Seguridad Social (SSN), los números del carné de conducir y los números de pasaporte. Estos datos son fundamentales para verificar la identidad de una persona y pueden utilizarse para cometer un robo de identidad si caen en las manos equivocadas. El robo de identidad se produce cuando alguien utiliza ilegalmente la información personal de otra persona para obtener beneficios económicos u otras ventajas.

Por qué es importante: la información de identidad es un objetivo primordial para los ciberdelincuentes porque puede utilizarse para abrir cuentas bancarias, solicitar préstamos o cometer fraudes.

Buenas prácticas:

o Nunca comparta su SSN, número de licencia de conducir o número de pasaporte a menos que sea absolutamente necesario.

o Guarde copias físicas de estos documentos en un lugar seguro (por ejemplo, un cajón cerrado con llave o una caja fuerte).

o Cuando proporcione información de identificación en línea, asegúrese de que el sitio web es seguro (busque «https» y el icono de un candado).

o Controle su informe de crédito con regularidad para detectar cualquier uso no autorizado de la información de su documento de identidad.

Explicación: Los datos de la tarjeta de crédito incluyen el número de la tarjeta, la fecha de caducidad, el CVV (Valor de Verificación de la Tarjeta) y la dirección de facturación. Esta información es sensible porque permite a otros realizar compras o retirar dinero de su cuenta**.**

Por qué es importante: el fraude con tarjetas de crédito es una forma habitual de delito financiero en el que los ladrones utilizan información robada de la tarjeta para realizar compras no autorizadas.

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.

Buenas prácticas:

o Introduzca la información de su tarjeta de crédito únicamente en sitios web seguros y de confianza.

o Utilice números de tarjeta de crédito virtuales o monederos digitales (por ejemplo, Apple Pay, Google Pay) para las transacciones en línea.

o Establezca alertas con su banco o compañía de tarjetas de crédito para que le notifiquen cualquier actividad inusual.

o Revise regularmente sus extractos bancarios para detectar transacciones no autorizadas.

Explicación: Los delincuentes pueden utilizar identificadores personales como fechas de nacimiento, direcciones de correo electrónico e incluso nombres de usuario para adivinar contraseñas, responder a preguntas de seguridad o crear un perfil para el robo de identidad.

Por qué es importante: las fechas de nacimiento se utilizan a menudo en combinación con otros datos para restablecer contraseñas o verificar identidades.

Buenas prácticas:

o Sea prudente a la hora de compartir su fecha de nacimiento completa en Internet; considere la posibilidad de compartir sólo el mes y el día si es necesario.

o Utiliza direcciones de correo electrónico diferentes para cada tipo de cuenta (por ejemplo, una para la banca y otra para las redes sociales).

o Evite utilizar el mismo nombre de usuario en varias plataformas para dificultar que alguien relacione sus cuentas.

o Ten cuidado con la cantidad de información personal que compartes en los perfiles de las redes sociales.

Explicación: La información sanitaria incluye historiales médicos, datos del seguro y cualquier dato relacionado con la salud física o mental de una persona. Con el auge de los servicios sanitarios en línea y los historiales médicos electrónicos, proteger esta información es cada vez más importante.

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.

Buenas prácticas:

o Utilice canales de comunicación seguros y cifrados cuando comparta información sanitaria Verifique la seguridad de los portales sanitarios en línea antes de introducir cualquier dato sanitario personal.

o Tenga cuidado al compartir información sanitaria en las redes sociales o en foros públicos.

o Habilite la autenticación de dos factores en los portales de salud siempre que sea posible.

Explicación: La dirección es un dato personal que puede revelar dónde vives. Si se expone en Internet, puede dar lugar a diversos riesgos, como acoso, robos y estafas.

Por qué es importante: conocer el domicilio de una persona puede permitir a los delincuentes atacarla físicamente (por ejemplo, para robarle) o utilizar la información para estafarla (por ejemplo, timos de entregas falsas).

Buenas prácticas:

o Evita compartir públicamente la dirección de tu domicilio en Internet, por ejemplo en redes sociales o foros públicos.

o Utiliza un apartado de correos para las entregas si sueles comprar o vender artículos por Internet.

o Asegúrese de que las plataformas que requieran su dirección particular (por ejemplo, mercados en línea) tengan una buena configuración de privacidad.

o Ten cuidado con las peticiones no solicitadas de tu dirección, especialmente por teléfono o correo electrónico.

Explicación: Los números de teléfono se utilizan a menudo con fines de verificación y contacto. Sin embargo, si no se protegen adecuadamente, también pueden utilizarse para estafas, robos de identidad o marketing no deseado.

Por qué es importante: Los números de teléfono pueden utilizarse en ataques de intercambio de SIM, en los que un pirata informático toma el control de su número de teléfono para acceder a sus cuentas 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.

Buenas prácticas:

o Evita compartir tu número de teléfono públicamente en Internet, especialmente en las redes sociales.

o Utiliza aplicaciones de autenticación de dos factores en lugar de SMS siempre que sea posible para reducir el riesgo de intercambio de SIM.

o Considera la posibilidad de utilizar un número de teléfono secundario o un número basado en una aplicación para servicios no esenciales.

o Ten cuidado con las llamadas o mensajes de texto no solicitados que te pidan información personal.

2. Trabajo en grupo sobre casos hipotéticos (20 minutos):

Escenario 1: Un estudiante recibe un mensaje de texto que dice ser de su banco, pidiéndole que verifique su dirección y número de teléfono. ¿Qué debe hacer?

Soluciones esperadas (Para el profesor: no lo comparta con los alumnos)

1.No responder al mensaje de texto.

2.Contactar directamente con el banco utilizando un número de teléfono conocido para verificar si la solicitud es legítima.

3. Denuncie el mensaje sospechoso al departamento de fraudes del banco.

Escenario 2: Un usuario comparte con frecuencia su ubicación y fotos de su casa en las redes sociales. Hable de los riesgos que esto conlleva y de las medidas que debería tomar para proteger su privacidad.

Soluciones esperadas (Para el profesor: no comparta esto con los alumnos)

1.Evitar compartir detalles específicos de la ubicación en tiempo real.

2.Ajustar la configuración de privacidad para limitar quién puede ver las publicaciones.

3.Ten cuidado a la hora de etiquetar ubicaciones o mencionar detalles de la casa en los mensajes.

Escenario 3: Una persona recibe una llamada telefónica no solicitada de alguien que dice ser de su proveedor de atención sanitaria y le pide su número de seguro médico y otros datos personales. ¿Cómo debe responder?

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.

Soluciones esperadas (Para el profesor: no lo comparta con los alumnos)

1. No facilite ninguna información por teléfono.
2. Cuelgue y póngase en contacto directamente con el profesional sanitario utilizando un número de teléfono verificado.
3. Denuncie la llamada al departamento de fraudes del proveedor de asistencia sanitaria.

Escenario 4: Una persona indica su dirección particular y su número de teléfono en el perfil de un mercado en línea para facilitar la venta de artículos. Discuta los riesgos potenciales y cómo mitigarlos.

Soluciones previstas (Para el profesor: no comparta esto con los alumnos)

1. Utilizar el sistema de mensajería privada de la plataforma en lugar de compartir información de contacto personal.
2. Considera la posibilidad de utilizar un apartado de correos o un número de teléfono temporal.
3. Quedar con los compradores en lugares públicos en lugar de dar la dirección de su casa.

Cada grupo (de 3 a 5 estudiantes) analiza el escenario que se le ha asignado y presenta sus soluciones propuestas a la clase, explicando la lógica que subyace a cada paso.

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:

- 11 consejos de seguridad en Internet para su seguridad en línea https://www.youtube.com/watch?v=aO858HyFbKI&t=21s
- Privacidad y seguridad en línea 101: ¿Cómo protegerse realmente? https://www.youtube.com/watch?v=qZE45J-MIUg

ANEXOS:

- Quiz de Evaluación

TAREAS:

Tarea: Los alumnos deben revisar y proteger la información personal que comparten en Internet, incluida la dirección, el número de teléfono, la fecha de nacimiento y otros datos personales. Deben aplicar al menos una nueva medida de seguridad que se haya discutido en clase.

Reflexión: Escribe un breve párrafo sobre los cambios que han realizado y cómo creen que estos cambios protegerán mejor su información personal.

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:

- Evalúe a los alumnos en función de su participación en los debates de grupo y de la calidad de las soluciones que presenten.
- Califique las respuestas del cuestionario para garantizar la comprensión de los conceptos clave.
- Anime a los alumnos a compartir una nueva medida que piensen adoptar para proteger su información personal en Internet, explicando por qué es necesario.

Cuestionario (15 minutos):

Prueba escrita:

1. Pregunta: ¿Por qué es importante no compartir públicamente la dirección de tu casa en Internet?

(Respuesta: Compartir públicamente la dirección de tu casa puede convertirte en objetivo de robos, estafas y visitas no deseadas).

2. Pregunta: ¿Qué debe hacer si recibe una llamada sospechosa en la que le piden sus datos personales?

(Respuesta: No facilite ninguna información; cuelgue y póngase en contacto directamente con la organización utilizando un método de contacto verificado).

3. Pregunta: ¿Cómo puede ponerle en peligro compartir su número de teléfono en Internet?

(Respuesta: Tu número de teléfono puede ser utilizado para el robo de identidad, ataques de intercambio de SIM y marketing no deseado).

4. Pregunta: ¿Cuáles son los riesgos de compartir su información sanitaria a través de canales no seguros?

(Respuesta: La información sanitaria puede ser interceptada, dando lugar a violaciones de la privacidad o robos de identidad).

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.