UNA GUÍA DE COMPONENTES PARA EL MAESTRO

Cómo proteger su identidad en línea

Los estudiantes responden preguntas de cierto o falso sobre los comportamientos seguros en línea y consideran formas de protegerse en línea.

Metas de aprendizaje

Idea principal

El fraude y el robo de identidad perjudican a millones de estadounidenses cada año..

Preguntas esenciales

- ¿Por qué es importante proteger mi identidad cuando estoy en línea?
- ¿Qué puedo hacer para protegerme del fraude y el robo de identidad cuando estoy en línea?

Objetivos

- Comprender por qué el fraude y el robo de identidad son un riesgo
- Revisar las prácticas que pueden ayudar a proteger a las personas del fraude y el robo de identidad

Lo que harán los estudiantes

- Responder preguntas de cierto o falso sobre comportamientos seguros en línea.
- Explorar formas de protegerse en línea.

INFORMACIÓN CLAVE

Elemento Fundamental:

Función ejecutiva

Estándares y hábitos financieros

Rango de edad: Escuela Secundaria (6-8)

Rango de edad: 11–14

Tema: Proteger (Prevención de fraude y robo de identidad)

Asignatura escolar: CTE (Educación técnica y profesional), inglés o lenguaje y humanidades, Bellas artes y artes escénicas

Estrategia de enseñanza: Ludificación

Nivel de taxonomía de Bloom: Comprender, Crear

Duración de la actividad: 45-60 minutos

ESTÁNDARES

Consejo de Educación Económica
Estándar VI. Proteger y asegurar

Coalición Jump$tart
Toma de decisiones financieras - Estándares 2 y 3

Cómo prepararse para esta actividad

- [ ] Completar la actividad de "Actuando el fraude" antes de realizar esta actividad puede hacer que sea más significativa, aunque no es necesario.
- [ ] Imprima copias de todos los materiales estudiantiles o prepárelos para que los estudiantes puedan acceder a ellos electrónicamente.
- [ ] Imprima una copia de las declaraciones sobre "Cómo estar seguro en línea" de esta guía para leer en voz alta.
- [ ] Los estudiantes necesitarán papel en blanco para hacer letreros de "cierto" y "falso".

Lo que necesitará

ESTA GUÍA DEL MAESTRO

- **Cómo proteger su identidad en línea** (guía) cfpb_building_block_activities_como-proteger-su-identidad-en-linea_guia.pdf
- **Declaraciones sobre "Cómo estar seguro en línea"** (en esta guía)

MATERIALES ESTUDIANTILES

- **Cómo proteger su identidad en línea** (hoja de trabajo) cfpb_building_block_activities_como-proteger-su-identidad-en-linea_tabla.pdf
- **Papel en blanco para los letreros de "cierto" y "falso"**

Cómo explorar conceptos financieros clave

Millones de estadounidenses son víctimas de fraude o robo de identidad cada año. Algún día puede verse afectado por estos delitos sin importar en dónde viva o qué edad tenga. El robo de identidad puede ocurrir por teléfono al responder preguntas personales o en línea al hacer clic en enlaces sospechosos o al abrir correos electrónicos de fuentes desconocidas en su computadora o teléfono. Saber cómo identificar el fraude y el robo de identidad lo ayuda a mejor protegerse a sí mismo y a su dinero.

CONSEJO

Debido a que los tipos de fraude y las leyes sobre el fraude y el robo de identidad cambian, se les debe animar a los estudiantes a siempre buscar la información más actualizada

Cómo enseñar esta actividad

Introducción para la clase

- Dígales a los estudiantes que explorarán comportamientos seguros en línea.
- Asegúrese que los alumnos entiendan el vocabulario clave:
  - **Fraude:** un acto ilegal que ocurre cuando las personas intentan engañarlo para obtener su información personal y su dinero.
  - **Robo de identidad:** el uso de su información personal, como su nombre, número de Seguro Social o número de tarjeta de crédito, sin su permiso.
- Distribuya la hoja de trabajo "Cómo proteger su identidad en línea" y asegúrese que los estudiantes tengan papel en blanco para las señales de "cierto" y "falso".
- Explíqueles que responderán preguntas sobre cómo proteger su identidad en línea.

Trabajo individual

- Los estudiantes deberán trabajar individualmente para completar sus hojas de trabajo.
- Pídales que formen dos letreros en el papel blanco después de completar su hoja de trabajo, uno que diga "Cierto" y otro que diga "Falso".
- Cuando todos los estudiantes hayan terminado, lea cada declaración en voz alta.
- Pídales a los estudiantes que indiquen si creen que la declaración es cierta o falsa haciendo que sostengan el letrero apropiado.
- Mientras los alumnos comparten sus respuestas, lleve la cuenta en el pizarrón o en un cartel.

Conclusión

- Cuando se haya hecho el conteo de todas las respuestas, repase cada pregunta nuevamente y use la guía de respuestas para compartir la respuesta correcta.
- Puede utilizar la sección de "Cómo ampliar la comprensión" de la guía de respuestas para contribuir al debate.
- Anime a los estudiantes a que compartan sus pensamientos sobre la razón por la cual respondieron a cada pregunta de la forma en que lo hicieron.
- Pídales a los estudiantes que compartan sus respuestas a las preguntas de reflexión.

Siguientes pasos recomendados

Considere buscar otras actividades que hablen sobre el tema de la protección, que incluye las actividades sobre la gestión de riesgos y la prevención del fraude y robo de identidad.

Cómo medir el aprendizaje de los estudiantes

La guía de respuestas en la siguiente página describe posibles respuestas para la hoja de trabajo sobre "Cómo proteger su identidad en línea".

Tenga en cuenta que las respuestas de los estudiantes para las preguntas de reflexión podrían variar, ya que no hay respuesta correcta o incorrecta. Lo importante es que los estudiantes tengan una explicación razonable para sus respuestas.

Guía de respuestas y declaraciones sobre cómo saber de estar seguro en línea

Respuesta	Respuesta	[Información para] ampliar la comprensión
1. Está bien dar información personal si alguien le envía un correo electrónico diciendo que usted tiene una cuenta con esa persona y él/ella parece saber algunas cosas sobre usted.	Falso	Asegúrese de saber quién obtiene su información personal y no la proporcione por correo electrónico o por Internet a menos que sepa con quién está tratando. Si una compañía le envía un correo electrónico y le dice que usted tiene una cuenta con ellos, no haga clic en ningún enlace en el correo. Mejor comuníquese con el servicio de atención al cliente a través de su sitio web y pregunte si enviaron una solicitud.
2. Es seguro abrir o descargar cualquier archivo adjunto siempre y cuando lo haga desde la seguridad de su cuenta de correo electrónico.	Falso	Siempre debe tener cuidado al abrir o descargar cualquier archivo adjunto en los correos electrónicos que reciba, sin importar quién los envió. Los archivos inesperados pueden tener software que puede dañar su computadora.

Respuesta	Respuesta	[Información para] ampliar la comprensión
3. Hacer clic en los enlaces en los mensajes es peligroso solo si proporciona su información personal.	Falso	No abra archivos, haga clic en enlaces ni descargue programas que vienen de extraños. Esto podría exponer su computadora a un virus o programa espía que roba sus contraseñas u otra información que escriba.
4. El gobierno federal exige que los sitios y servicios destinados a cualquier persona de 13 años o menos notifiquen a los padres directamente y obtengan su aprobación antes de juntar, usar o divulgar la información personal de un niño.	Cierto	El congreso promulgó la ley de protección de la privacidad infantil en Internet (COPPA, por sus siglas en ingles) en 1998. La ley COPPA exigió que la Comisión Federal de Comercio emitiera y aplicara reglamentos sobre la privacidad de los niños en línea. El objetivo de COPPA es que los padres estén en control sobre qué información se recopila de sus hijos pequeños en línea.
5. Es más seguro permanecer conectado permanentemente a las cuentas.	Falso	Si permanece conectado a cuentas que tienen su información personal o que usan la función de inicio de sesión automático (que guarda su nombre de usuario y contraseña), su información personal está en riesgo si pierde o le roban su computadora.
6. La "s" en https en una dirección web significa seguro.	Cierto	Si ve que https es parte del URL de un sitio web, esto significa que puede comunicarse de forma segura con el servidor web. Estos sitios utilizan un programa que distorsiona su información para que otras personas no puedan acceder a ella a través del Internet.
7. Evite conectarse a redes de wifi que no requieren una contraseña para iniciar sesión.	Cierto	Las conexiones inalámbricas públicas (wifi) no son seguras. Siempre debe usar las redes públicas con cuidado. Si conecta su computadora portátil o teléfono inteligente al wifi de una cafetería, biblioteca u otro lugar público, asegúrese de estar usando un sitio web encriptado.

Respuesta	Respuesta	[Información para] ampliar la comprensión
8. Es importante tener protección antivirus en su computadora y actualizarla con frecuencia.	Cierto	Es importante asegurarse que sus computadoras estén protegidas con un software de seguridad confiable. Mantenga su software actualizado para protegerlo de las últimas amenazas. Esto incluye su sistema operativo, los navegadores web que utiliza para conectarse al Internet y sus aplicaciones. Es más fácil para los delincuentes ingresar a un programa anticuado.
9. Es mejor usar la misma contraseña para varias de sus cuentas porque es muy difícil acordarse de varias contraseñas.	Falso	Es una buena práctica utilizar contraseñas seguras para el correo electrónico y otras cuentas en línea. Una contraseña segura incluye una combinación de letras mayúsculas y minúsculas, números y símbolos. También debe proteger sus contraseñas. Mientras más larga sea la contraseña, más difícil será descifrarla. La información personal, su nombre de inicio de sesión, las palabras comunes o las teclas contiguas en el teclado no son contraseñas seguras.
10. El hecho de compartir sus contraseñas con alguien que no sea un miembro de la familia proporciona una capa adicional de protección para su cuenta.	Falso	Las personas pueden proteger sus contraseñas mientras no las compartan con nadie, incluyendo con sus amigos.