

Cómo proteger su identidad en línea

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

Metas de aprendizaje

Gran idea

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?
- ¿Cuáles son algunas de las cosas que puedo hacer para protegerme del fraude y el robo de identidad cuando estoy en línea?

Objetivos



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

NOTA:

Por favor recuerde tomar en cuenta las necesidades y adaptaciones de sus estudiantes para garantizar que todos los estudiantes puedan participar de manera significativa.

INFORMACIÓN CLAVE

Cimientos:

-  Función ejecutiva
-  Hábitos y normas financieras

Nivel de grado: Escuela intermedia (6-8)

Rango de edad: 11-14

Tema: Proteger (Manejo de riesgo, Prevención de fraude y robo de identidad)

Asignatura: CTE (Educación profesional y técnica), inglés o lengua y literatura, bellas artes y artes escénicas

Estrategia de enseñanza: Gamificación

Nivel de taxonomía de Bloom:
Entender, crear

Duración de la actividad: 45-60 minutos

Estándares Nacionales para la Educación Financiera Personal, 2021

Manejo de riesgo: 4-1, 4-2, 8-1, 8-5, 8-7, 12-11

Estos estándares son acumulativos y los temas no se repiten en cada nivel de grado. Esta actividad puede incluir información que los estudiantes necesitan comprender antes de explorar este tema con más detalle.

Qué harán los estudiantes

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

Preparación para esta actividad

- Si bien no es necesario, completar la actividad “Representar el fraude y robo de identidad” primero puede hacer que esta actividad sea más significativa.
- Imprima copias de todos los materiales de los estudiantes o prepárelos para que los estudiantes accedan a ellos electrónicamente.
- Imprima una copia de las afirmaciones de “Saber cómo estar seguro en línea” de esta guía para leer en voz alta.
- Los estudiantes necesitarán papel en blanco para hacer letreros de “verdadero” y “falso”.

Qué necesitará

ESTA GUÍA DEL MAESTRO

- Proteger tu identidad en línea (guía)
[cfpb_building_block_activities_como-proteger-su-identidad-en-linea_guia.pdf](#)
- Afirmaciones de “Saber cómo estar seguro en línea” (en esta guía)

MATERIALES DE LOS ESTUDIANTES

- Proteger tu identidad en línea (hoja de trabajo)
[cfpb_building_block_activities_como-proteger-su-identidad-en-linea_tabla.pdf](#)
- Papel en blanco para hacer letreros de “verdadero” y “falso”

Exploración de conceptos financieros clave

Millones de estadounidenses son víctimas de fraude o robo de identidad cada año. No importa dónde vivas o qué edad tengas, algún día podrías verte afectado por estos delitos. El robo de identidad puede ocurrir por teléfono al responder preguntas personales o en línea haciendo clic en enlaces sospechosos o al abrir correos electrónicos de fuentes desconocidas en tu computadora o teléfono. Saber cómo identificar el fraude y el robo de identidad te ayuda a proteger mejor tu dinero.

CONSEJO

Debido a que los tipos de fraude y las leyes sobre fraude y robo de identidad cambian, motive a los estudiantes a que siempre busquen la información más actualizada..

Cómo enseñar esta actividad

Introducción para la clase

- Dígales a los estudiantes que explorarán comportamientos seguros en línea.
- Asegúrese de que los estudiantes entiendan el vocabulario clave:
 - **Fraude:** Un acto ilegal que ocurre cuando las personas intentan engañarte para robarte tu información personal y tu dinero.
 - **Robo de identidad:** Usar tu información personal, como tu nombre, número de Seguro Social o número de tarjeta de crédito, sin tu permiso.
- Reparta la hoja de trabajo “Proteger tu identidad en línea” y asegúrese de que los estudiantes tengan papel en blanco para los letreros de “verdadero” y “falso”.
- Explique que responderán preguntas sobre cómo proteger su identidad en línea.

CONSEJO

Visite el sitio financiero de CFPB glosario de educación en consumerfinance.gov/glosario-de-educacion-financiera/.

Trabajo individual

- Los estudiantes trabajarán individualmente para completar sus hojas de trabajo.
- Pídeles que creen dos carteles en el papel en blanco después de completar su hoja de trabajo, uno que diga “Verdadero” y otro que diga “Falso”.
- Una vez que todos los estudiantes hayan terminado, lea cada afirmación en voz alta.
- Pída a los estudiantes que indiquen si creen que la afirmación es verdadera o falsa mostrando el cartel correspondiente.
- A medida que los estudiantes compartan sus respuestas, lleve la cuenta en la pizarra o en un cartel.

Conclusión

- Una vez que se hayan contado todas las respuestas, revise cada pregunta nuevamente y use la guía de respuestas para compartir la respuesta correcta.
 - Puede usar la sección “Expandir la comprensión” de la guía de respuestas para agregar al debate.
- Anime a los estudiantes a compartir sus pensamientos sobre por qué respondieron cada pregunta de la manera en que lo hicieron.
- Pída a los estudiantes que compartan sus respuestas a las preguntas de reflexión.

Siguientes pasos recomendados

Considere buscar otras actividades del CFPB que aborden el tema de la protección, incluido el manejo de riesgos y la prevención del fraude y el robo de identidad. Las actividades sugeridas incluyen “Componer canciones y versos sobre el fraude” y “Protegerse del robo de identidad”.

Cómo medir el aprendizaje de los estudiantes

Las respuestas de los estudiantes en sus hojas de trabajo y durante el debate pueden darle una idea de su comprensión. Esta guía de respuestas proporciona posibles respuestas para la hoja de trabajo “Proteger tu identidad en línea”. **Tenga en cuenta que las respuestas de los estudiantes a las preguntas de reflexión pueden variar, ya que es posible que haya más de una sola respuesta correcta.** Lo importante es que los estudiantes tengan una explicación aceptable para sus respuestas.

Saber cómo estar seguro en línea - Afirmaciones y guía de respuestas

Afirmación	Respuesta	Ampliar la comprensión
1. Está bien dar información personal si alguien te envía un correo electrónico diciendo que tienes una cuenta con ellos y parece saber algunas cosas sobre ti.	Falso	Asegúrate de saber quién obtiene tu información personal y no la proporcionas por correo electrónico o Internet a menos que sepas con quién estás tratando. Si una compañía te envía un correo electrónico diciendo que tienes una cuenta con ellos, no hagas clic en ningún enlace en el correo electrónico. En su lugar, comunícate con el servicio al cliente a través de tu sitio web y pregunta si enviaron una solicitud.
2. Es seguro abrir archivos adjuntos o descargar archivos siempre que lo hagas desde la seguridad de tu cuenta de correo electrónico.	Falso	Siempre debes tener cuidado al abrir archivos adjuntos o descargar archivos de los correos electrónicos que recibes, independientemente de quién los haya enviado. Los archivos inesperados pueden contener software que puede dañar tu computadora.
3. Hacer clic en los enlaces de los mensajes solo es peligroso si proporcionas tu información personal.	Falso	No abras archivos, no hagas clic en enlaces ni descargues programas de extraños. Esto podría exponer tu computadora a un virus o spyware que roba tus contraseñas u otra información que ingreses.
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 recopilar, usar o divulgar la información personal de un niño.	Verdadero	El Congreso promulgó la Ley de protección de la privacidad en línea de los niños (COPPA, por sus siglas en inglés) en 1998. COPPA requirió que la Comisión Federal de Comercio emitiera e hiciera cumplir las regulaciones relacionadas con la privacidad en línea de los niños. El objetivo de COPPA es dar a los padres el control sobre qué información se recopila de sus hijos pequeños en línea.

Afirmación	Respuesta	Ampliar la comprensión
5. Es más seguro permanecer conectado permanentemente a las cuentas.	Falso	Si permaneces conectado a cuentas que tienen tu información personal o utilizas la función de inicio de sesión automático (que guarda tu nombre de usuario y contraseña), tu información personal está en riesgo si pierdes o te roban tu computadora.
6. La "s" en https en una dirección web significa seguro.	Verdadero	Si ves https como parte de la URL de un sitio web, significa que puedes comunicarse de forma segura con el servidor web. Estos sitios usan software que codifica tu información para que otras personas no puedan acceder a ella a través de Internet.
7. Evita conectarte a redes wi-fi que no requieran una contraseña para iniciar sesión.	Verdadero	Las redes inalámbricas públicas (wi-fi) no son seguras. Siempre debes usar las redes públicas con cuidado. Si conectas tu computadora portátil o teléfono inteligente al wi-fi en una cafetería, biblioteca u otro lugar público, asegúrate de estar utilizando un sitio web encriptado.
8. Es importante tener protección contra virus en tu computadora y actualizarla con frecuencia.	Verdadero	Es importante asegurarte de que tus computadoras estén protegidas por un software de seguridad confiable. Mantén tu software actualizado, incluido tu sistema operativo, los navegadores web que usas para conectarte a Internet y tus aplicaciones, para protegerte contra las amenazas más recientes. El software obsoleto es más fácil de penetrar para los delincuentes.

Afirmación	Respuesta	Ampliar la comprensión
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 usar contraseñas seguras para el correo electrónico y otras cuentas en línea. Una contraseña segura tiene una combinación de letras mayúsculas y minúsculas, números y símbolos. También debes proteger tus contraseñas. Cuanto más larga sea la contraseña, más difícil será descifrarla. La información personal, tu nombre de inicio de sesión, las palabras comunes o las teclas adyacentes del teclado no son contraseñas seguras.
10. Compartir tus contraseñas con alguien que no es un miembro de la familia proporciona una capa adicional de protección para tu cuenta.	Falso	Las personas pueden proteger sus contraseñas al no compartirlas con nadie, incluidos sus amigos.