Robo de Identidad

Lección 6: Actividades para alumnos | Novato: Edades 11-14

FINANCIAL FOOTBALL

Cómo evitar daños con la protección contra el robo de identidad

La protección contra el robo de identidad y la prevención de fraudes son aspectos increíblemente importantes de una vida financiera saludable. Este módulo de 45 minutos te empoderará a fin de que puedas manejar los riesgos, monitorear tus finanzas y realizar acciones preventivas para la protección de tu futuro financiero.

Preparación para el juego: Los atletas que hacen entrenamiento observan muchos beneficios. Genera fuerza y agilidad; brinda tiempo para la práctica y el crecimiento y ayuda a minimizar el riesgo de lesiones. Los jugadores trabajan diligentemente para protegerse en el campo de juego y fuera de él.

Si bien la mayoría de nosotros no evita los placajes a alta velocidad tenemos, de hecho, una necesidad similar de protegernos cuando se trata de finanzas. El robo de identidad es cada vez más predominante e, incluso, afecta a los niños antes de que puedan comenzar a construir su propio crédito. Un paso importante para proteger tu identidad es ser consciente de los riesgos comunes y de las estrategias de prevención.

Nivel del módulo: Novato, Edades 11-14

Temas: Economía, Matemáticas, Finanzas, Ciencias del Consumidor, Habilidades de la Vida.

Materiales: Los facilitadores pueden imprimir y hacer fotocopias de las tareas y los exámenes, y derivarte a los recursos por Internet que se indican más abajo.

- **Preguntas del examen anterior y posterior:** Responde estas preguntas antes de completar las actividades de Robo de Identidad para ver cuánto sabes acerca del tema. Una vez finalizadas todas las actividades con tu profesor y compañeros de clase, vuelve a intentar completar el cuestionario para ver cuánto has aprendido.
- **Recursos de Robo de Identidad en Practical Money Skills:** practicalmoneyskills.com/ffsp43
- **Copia de la actividad Plan de juego de Robo de Identidad:** Haciendo uso de las herramientas de investigación, propone ideas y crea un sketch de tráiler para generar conciencia, prevenir problemas y protegerte del robo de identidad.

Cómo evitar daños con la protección contra el robo de identidad, cont.

- **Copia de Dos estafas y un anuncio:** Juega con un compañero o equipo pequeño para ver cuántos riesgos de robo de identidad pueden identificar.
- **Glosario de términos:** Aprende los conceptos financieros básicos con esta lista de términos.

Contenido

Objetivos del aprendizaje

– Identificar qué se entiende por robo de identidad y por fraude, y cómo pueden impactar éstos en tu vida financiera.
– Examinar estrategias para evitar el robo de identidad y las estafas.
– Descubrir maneras de manejar el robo de identidad, el fraude y/o las violaciones a la seguridad.

Términos y conceptos clave

Antes de empezar la lección, revisa los términos y conceptos clave que se indican más abajo. Las respuestas a las preguntas te ayudarán a prepararte para el juego.

¿Qué es el robo de identidad?

El robo de identidad puede adoptar muchas formas. El robo de identidad financiera es, a menudo, un caso de acceso y uso ilegal de cuentas bancarias o tarjetas de crédito. Por ejemplo: el ladrón puede extraer efectivo o agotar el límite de una tarjeta de crédito. Ello puede tener un impacto grave en tu puntaje crediticio. Otra forma del robo de identidad es cuando los delincuentes obtienen acceso a tu número del Seguro Social y hacen un uso ilícito de él, por ejemplo, para sacar préstamos o abrir cuentas de tarjetas de crédito.

¿Cuáles son los tipos comunes de estafas por robo de identidad?

¿Sabías?

El protocolo de capa de conexión segura (Secure Sockets Layer/ SSL) de datos se utiliza para que tus transacciones en línea sean seguras.

- Fraude electrónico (Phishing): Se trata de estafas que intentan engañar a alguien para que revele sus datos personales tales como números de cuentas bancarias o contraseñas.
- Correos electrónicos: Ten cuidado con los correos electrónicos que provienen de fuentes sospechosas; pueden ser intentos para acceder a tus datos financieros personales. No reveles a terceros tus contraseñas de cuentas financieras, números PIN ni otros datos de seguridad; las organizaciones o instituciones genuinas no necesitan tus datos secretos para realizar las transacciones comerciales habituales.
- Smishing: Smishing es una estafa similar al fraude electrónico. Los usuarios de computadoras reciben un correo electrónico auténtico en apariencia que simula ser de su banco, proveedor de servicios de Internet (ISP, por su sigla en inglés), tienda favorita o alguna otra organización. También te envían mensajes de smishing por SMS (mensajes de texto) a tu teléfono móvil. No los respondas. Elimínalos, al igual que los correos electrónicos.
- Clonación de fraude electrónico (Clone phishing): Se refiere al reenvío de un correo electrónico que ahora contiene un adjunto o enlace malicioso. No abras documentos adjuntos de correos electrónicos sospechosos; pueden contener virus para infectar tu computadora.
- Vishing (uso delictivo del teléfono) es cuando un estafador te llama pretendiendo ser alguien que conoces en un intento por obtener tus datos financieros personales. Las potenciales víctimas pueden escuchar una grabación automatizada en la que se les informa que su cuenta bancaria está en riesgo y ofrece un número gratuito para restaurar la configuración de seguridad asociada a la cuenta.

Objetivos del aprendizaje, cont.

- Clonadores de tarjetas (Skimmers): Son dispositivos que los estafadores colocan en un cajero automático, el surtidor de gasolina de una estación de servicio o la caja de una tienda para copiar la información de tu tarjeta de débito o crédito.
- Fraude electrónico focalizado (Whaling): Son estafas dirigidas a empresarios de alto perfil para obtener sus datos financieros personales.
- Doxing (publicación de datos para acoso): Las estafas por doxing tienen lugar cuando alguien publica a través de Internet datos personales de la víctima tales como su domicilio o número del teléfono celular. Apócope de la frase inglesa 'dropping docs', es una táctica empleada por los piratas informáticos para violar los datos personales de alguien y publicarlos en línea como medio de acoso.

¿Qué pasos debo seguir para protegerme del robo de identidad?

Existen seis pasos simples que puedes seguir para reducir el riesgo de ser víctima de robo de identidad o de fraude con tarjeta.

1. Practica el uso seguro de la Internet.
2. Destruye los documentos financieros innecesarios.
3. Protege tu número del Seguro Social.
4. Controla tu informe crediticio.
5. Ten cuidado con las estafas.
6. Protege tu correo.

¿Sabías?

Para reducir el robo de identidad cuando compras en línea, puedes saber si un sitio es seguro mirando la barra de dirección de tu navegador. Verás un ícono de candado al lado de la dirección del sitio web y ésta comienza con https://.

Información de contacto de las agencias de crédito

Equifax

Solicitar informe crediticio:
1-800-685-1111

Línea directa de Fraudes:
1-888-766-0008

equifax.com

Experian

Solicitar informe crediticio:
1-888-397-3742

Línea directa de Fraudes:
1-888-397-3742

experian.com

TransUnion

Solicitar informe crediticio:
1-877-322-8228

Línea directa de Fraudes:
1-800-680-7289

transunion.com

¿Qué hago si creo que he sido víctima del robo de identidad?

Si tu información financiera privada cae en las manos equivocadas, las consecuencias pueden ser devastadoras. Si descubres que eres víctima de robo de identidad, actúa rápidamente y comunícate con la autoridad de aplicación de la ley y con las empresas de informes crediticios.

- Informa del fraude a la autoridad de aplicación de la ley, acompañado de tus padres.
- Ponte en contacto con las empresas de informes crediticios, acompañado de tus padres.
- Crea un plan de recuperación contra fraudes, acompañado de tus padres.

Objetivos del aprendizaje, cont.

¿Dónde puedo obtener asistencia e información acerca del robo de identidad?

Para información acerca de la lucha contra el robo de identidad, visita el sitio web de robo de identidad de la Comisión Federal de Comercio (Federal Trade Commission/FTC) (practicalmoneyskills.com/ffsp44) o llama a la línea directa: 1-877-IDTHEFT (1-877-438-4338).

¿Sabías?

Un indicador de que eres víctima de robo de identidad es que tu informe crediticio muestra una actividad inusual.

Si has sido víctima de robo de identidad, comunícate de inmediato con los departamentos de fraudes de cada una de las agencias de crédito.

Obtén más información acerca del robo de identidad

- Aprende más acerca de los conceptos básicos del robo de identidad y de cómo protegerte en practicalmoneyskills.com/ffsp43.
- Lee la guía de robo de identidad de Practical Money Skills, en practicalmoneyskills.com/ffsp45.

Actividades para alumnos

> **Examen anterior y posterior**

> Protección contra el robo de identidad: Tráilers

> **Protección contra el robo de identidad: Dos estafas y un anuncio**

Examen anterior y posterior de la protección contra el robo de identidad

Nombre del alumno: _____

Instrucciones: Responde las preguntas con la respuesta que corresponda (a, b, c o d) o llenando el espacio en blanco.

1. A los efectos de ayudar a prevenir el robo de identidad:

a. Guarda las tarjetas y números de cuenta en un lugar seguro.

b. Tritura los documentos que contienen datos personales.

c. Nunca compres por Internet.

d. Ambas respuestas a. y b.

2. ¿En qué situaciones estás en mayor riesgo de que te roben la identidad?

a. Cuando usas un cajero automático.

b. Cuando compras en un sitio web inseguro.

c. Cuando viajas.

d. Todo lo anterior.

3. ¿Qué información NO debes compartir con un amigo?

4. Una estrategia inteligente para proteger tu identidad consiste en:

a. Postear información privada en las redes sociales.

b. Darle a tu compañero de cuarto el PIN de tu cajero automático.

c. Tirar a la basura los resúmenes de tarjetas de crédito.

d. Usar sitios web seguros cuando realices compras en línea.

5. En caso de pérdida o robo de tu billetera, deberás ponerte en contacto inmediatamente con el emisor de tu tarjeta de débito.

a. Verdadero

b. Falso

Protección contra el robo de identidad: Tráilers

Instrucciones: Tu profesor dividirá a los alumnos en pequeños grupos. Forma un equipo para desarrollar un tráiler de uno a dos minutos utilizando uno de los cinco géneros de cine (misterio, acción/aventuras, comedia, ciencia ficción o superhéroes) y los siguientes personajes. Tu tráiler debe incluir: título, lema y un argumento claro. Revisa con tu equipo los riesgos y desafíos del personaje respecto del robo de identidad y entiende los hechos respaldatorios antes de desarrollar el tráiler.

Género de cine

Misterio

Personaje

Femenino, estudiante de secundaria

Fortalezas del personaje

- Resolución creativa de los problemas.
- Rapidez y habilidades con la tecnología.

Riesgos y desafíos del personaje respecto del robo de identidad

- Le encanta descubrir y compartir información nueva, incluso si significa entrar en enlaces aleatorios.
- Dedica mucho tiempo a buscar información en redes sociales.

Hechos respaldatorios

- Es importante proteger la información privada en línea.
- Entrar en enlaces de terceros sin antes asegurarse de que la fuente es segura puede dejarte expuesto a ataques por malware o a que se apoderen de tus datos personales.

Título:

Lema:

Argumento:

Protección contra el robo de identidad: Tráilers, cont.

Género de cine

Acción/Aventuras

Personaje

Masculino, universitario recién graduado.

Fortalezas del personaje

- Rápido para tomar decisiones.
- Sólidas habilidades de comunicación.

Riesgos y desafíos del personaje respecto del robo de identidad

- Lo exaltan las oportunidades para hacer dinero y es rápido para compartir información a fin de conseguir un empleo.
- No está seguro dónde buscar empleo — en ocasiones explora anuncios locales y las redes sociales en busca de ideas.

Hechos respaldatorios

- Nunca pagues por adelantado una promesa. Si alguien vende un kit para iniciar un trabajo o te exige pagar una capacitación, podría tratarse de una estafa.
- Verifica bien los detalles — considera la posibilidad de realizar una búsqueda en línea para ver si hubo alguna queja en el pasado.

Título:

Lema:

Argumento:

Protección contra el robo de identidad: Tráilers, cont.

Género de cine

Comedia

Personaje

Dos mejores amigos en la escuela media.

Fortalezas del personaje

- Excelentes fotógrafos.
- Rápidos para imaginar aventuras juntos.

Riesgos y desafíos del personaje respecto del robo de identidad

- Algunas veces las bromas van demasiado lejos y comparten historias tontas y otros datos personales en las redes sociales.
- Son amigos tan cercanos – ¿Por qué no compartir entre ellos todas las contraseñas de sus cuentas?

Hechos respaldatorios

- Se puede pagar un precio alto por la conveniencia de compartir datos en línea: Si revelas demasiados datos podrías dar lugar a grandes violaciones a la privacidad y generar riesgos de robo de identidad.
- Las contraseñas compartidas, junto con la falta de verificación de la configuración de privacidad en sitios web y aplicaciones, pueden generar riesgos de a propiación de tu información y rastreo de tus actividades.

Título:

Lema:

Argumento:

Protección contra el robo de identidad: Tráilers, cont.

Género de cine

Ciencia ficción

Personaje

Dos hermanos, uno grande y otro pequeño.

Fortalezas del personaje

- Innovadores en el uso de la tecnología para hacer cosas sorprendentes.
- Capaces de manejar situaciones difíciles juntos y separados.

Riesgos y desafíos del personaje respecto del robo de identidad

- Apuro por probar nuevas tecnologías sin pensar en los potenciales riesgos.
- No ven a la tecnología como generadora de problemas, sino de soluciones.

Hechos respaldatorios

- El uso de tecnologías nuevas puede presentar maravillosas oportunidades nuevas, aunque también potenciales riesgos de robo de identidad. Es importante considerar cómo guardas tus datos personales y quién tiene acceso a tus dispositivos.
- Muchas fuentes sugieren cubrir la cámara, inhabilitar el GPS, y monitorear y verificar periódicamente la configuración de privacidad en tus dispositivos a fin de asegurarte de prevenir violaciones a la privacidad.

Título:

Lema:

Argumento:

Protección contra el robo de identidad: Tráilers, cont.

Género de cine

Superhéroes

Personaje

Estudiante de escuela media que ayuda como mentor de niños en un programa después del horario escolar.

Fortalezas del personaje

- Extremadamente experto.
- Excelente en la investigación (tema favorito: detección de estafas).

Riesgos y desafíos del personaje respecto del robo de identidad

- Le encanta compartir consejos y, en ocasiones, postea en línea la ubicación y fotos personales de datos financieros a modo de ejemplo.
- Es sumamente curioso y abre todos los correos electrónicos, aunque parezcan no deseados.

Hechos respaldatorios

- La Comisión Federal de Comercio (FTC, por su sigla en inglés) y la Agencia de Protección Financiera del Consumidor (CFPB, por su sigla en inglés) comparten artículos, videos y otros recursos para ayudar a evitar estafas y a obtener asistencia, de ser necesario.
- Una de las mejores maneras de protegerte del robo de identidad consiste en detectar y abordar señales de advertencia, incluidos correos electrónicos no deseados, facturas por servicios que nunca usaste y llamadas telefónicas de mercado no deseadas que te piden tus datos.

Título:

Lema:

Argumento:

Protección contra el robo de identidad: Dos estafas y un anuncio

Instrucciones: ¿Puedes detectar la estafa? Juega con un compañero o equipo pequeño para ver cuántos riesgos de robo de identidad pueden detectar. En la respuesta, identifica cada escenario como “estafa” o “anuncio”, y explica por qué. Incluye consejos o mejores prácticas para la protección de tu identidad.

Acá hay gato encerrado

1. Recibes una llamada y te entusiasma escuchar que ¡te has ganado una beca! Saben tu nombre, escuela y cuando te graduaste; lo cual parece de fiar. Te dicen que, para poder finalizar el trámite del premio, necesitan tu dirección y datos bancarios.

2. Recibes un texto de una tienda a la que sólo fuiste una vez, que ofrece un 50% de descuento. El texto incluye un enlace al sitio web nacional para descargar la oferta.

3. Recibes por correo electrónico una invitación para ver un documento en línea; es el nombre de tu amigo, pero no reconoces el correo electrónico como perteneciente a él.

¿Mercadeo mal intencionado o simplemente molesto?

1. Recibes un texto con una breve encuesta de tu tienda favorita dos días después de haber comprado allí un producto. Le dijiste al vendedor que no querías recibir ofertas.

Protección contra el robo de identidad: Dos estafas y un anuncio, cont.

2. Alguien llama a la puerta vendiendo revistas para juntar fondos destinados a una escuela. Por sólo $5 puedes obtener dos años de tu suscripción favorita. Necesitas que le proporciones tu nombre, domicilio y datos de la tarjeta de crédito. Ofrece una hoja atractiva que lista las revistas, pero ninguna otra documentación formal.

3. Recibes un texto que ofrece ayuda para obtener becas que dice: «Haz clic aquí para registrarte hoy a fin de tener acceso a soporte con descuento".

¿Problema inesperado al compartir o cuestión grave?

1. Compartiste un video en línea que explica la solución a un problema matemático. El video no muestra tu cara; en la pantalla sólo se ve de cerca el problema de matemáticas. Alguien comentó el video, compartió tu nombre, número de teléfono y correo electrónico y les dijo a los demás que deberían obtener guía instructiva.

2. Descargas una aplicación que te pregunta si puede acceder a tus datos personales.

3. Tus amigos compartieron un cuestionario en línea; es fácil de responder y los resultados te indican a cuáles de tus personajes de TV favoritos te pareces más. Cuando haces clic en el enlace a través de las redes sociales, exige acceso a tu perfil y solicita permiso para postear el resultado en tu perfil.

Glosario de términos

Estudia esta lista de términos de finanzas personales para prepararte antes de jugar Fútbol Financiero. Si dominas estos términos, tendrás una mejor oportunidad de responder correctamente preguntas del juego, y anotar.

Clonación de fraude electrónico (Clone phishing): Se refiere al reenvío de un correo electrónico que ahora contiene un adjunto o enlace malicioso. No abras documentos adjuntos de correos electrónicos sospechosos; pueden contener virus para infectar tu computadora.

Agencia de crédito: Empresa que recolecta y guarda diversos tipos de información acerca de ti y de tus cuentas e historial financieros. Utiliza esa información para generar tus informes y puntajes crediticios. Las tres principales agencias de créditos de consumidores son: Equifax®, Experian® y TransUnion®.

Doxing: (publicación de datos para acoso): Estas estafas tienen lugar cuando alguien publica datos personales en línea acerca de su víctima, por ejemplo, domicilio o número de teléfono celular. Apócope de la frase inglesa 'dropping docs', es una táctica empleada por los piratas informáticos para violar los datos personales de alguien y publicarlos en línea como medio de acoso.

Robo de Identidad: Uso fraudulento de datos de otra persona para obtener una ganancia financiera.

Malware: Software cuyo propósito es dañar o inhabilitar computadoras y sistemas informáticos.

Pharming (redireccionamiento del tráfico de la web a un sitio falso): Práctica fraudulenta de redirigir a usuarios de Internet a un sitio web falso que imita el aspecto de uno legítimo para obtener datos financieros personales tales como contraseñas, números de cuentas, etc.

Fraude electrónico (Phishing): Práctica fraudulenta que consiste en enviar correos electrónicos supuestamente de empresas con reputación a fin de inducir a los individuos a revelar datos financieros personales tales como contraseñas y números de tarjetas de crédito.

Esquemas piramidales: Esquemas ilegales en los cuales el dinero de inversores nuevos se utiliza para mostrar una rentabilidad falsa a otros inversores.

Estafa: Actividad fraudulenta o acto engañoso.

Violaciones a la seguridad: Incidente que resulta en el acceso no autorizado a datos, aplicaciones, servicios, redes y/o dispositivos evitando los mecanismos de seguridad subyacentes.

Clonación de tarjetas (Skimming): Método utilizado por ladrones de identidad para captar información de un titular de la tarjeta.

Smishing: Smishing es una estafa similar al fraude electrónico. Los usuarios de computadoras reciben un correo electrónico auténtico en apariencia que simula ser de su banco, proveedor de servicios de Internet (ISP, por su sigla en inglés), tienda favorita o alguna otra organización. También te envían mensajes de smishing por SMS (mensajes de texto) a tu teléfono móvil. No los respondas. Elimínalos, al igual que los correos electrónicos.

Glosario de términos, cont.

Robo de identidad con el número del Seguro Social: Una persona no honesta que tiene tu número de Seguro Social puede usarlo para obtener otra información acerca de ti. Los ladrones de identidad pueden usar tu número y tu buen crédito para solicitar más crédito a tu nombre. Pueden usar las tarjetas y no pagar las facturas, dañando tu crédito. A veces no te das cuenta sino hasta que no te dan crédito, o recibes llamadas de creedores desconocidos exigiendo pagos por artículos que nunca compraste. ssa.gov/pubs/EN-05-10064.pdf

Whaling (fraude electrónico focalizado): Son estafas dirigidas a empresarios de alto perfil para obtener sus datos financieros personales.