Robo de Identidad

Lección 6: Guía para profesores | 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 empodera a los alumnos a fin de que puedan manejar los riesgos, monitorear sus vidas financieras y realizar acciones preventivas para la protección de sus futuros financieros.

Preparación de tus alumnos para el juego:
El entrenamiento de jugadores tiene 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. La toma de conciencia acerca de los riesgos comunes y las estrategias de prevención constituyen un paso importante en la protección de la propia identidad.

Nivel del módulo: Novato, Edades 11-14

Esquema de tiempo: 45 minutos en total.

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, o derivarte a los recursos por Internet que se indican más abajo.

- **Preguntas del examen anterior y posterior:** Utiliza este pequeño grupo de preguntas para una evaluación rápida y formativa con el módulo Robo de Identidad o como un examen antes y después de terminar la serie completa del módulo.
- **Recursos de Robo de Identidad en Practical Money Skills:** practicalmoneyskills.com/ffsp43
- **Tráilers de la protección contra el robo de identidad (5 argumentos):** Mediante el uso de herramientas de investigación, los alumnosaportarán ideas y confeccionarán un

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

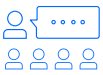
sketch de tráiler para generar conciencia, prevenir problemas y protegerse contra el robo de identidad.

- **Copia de Dos estafas y un anuncio:** Los alumnos pueden jugar con un compañero o equipo pequeño para ver cuántos riesgos de robo de identidad pueden detectar.
- **Glosario de términos:** Los alumnos aprenden los conceptos financieros básicos con esta lista de términos.

Tecla de ícono

Actividad

Asigna a los alumnos la actividad dada y haz que la completen individualmente o en forma grupal, dependiendo de lo indicado en las instrucciones.



Pregunta

Haz preguntas a tus alumnos para que las respondan.

Asigna

Designa individuos o grupos para completar una asignación específica.

Informa

Examina las actividades a toda la clase y compara respuestas y hallazgos.

¿Sabías?

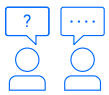
Comparte estas curiosidades con los alumnos durante la lección.

Examen anterior y posterior

Haz que los alumnos realicen el examen anterior previo a la lección y el posterior, una vez completada ésta.

Comparte

Léeles o parafraséales la lección a los alumnos.



Turnos de charlas cara a cara

Haz que los alumnos se dirijan a un compañero y debatan un tema o pregunta en particular.

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 ayudarán a los alumnos a prepararse para el juego. Obtiene información más detallada acerca de estos conceptos en la sección Guión para facilitadores, en las páginas 6 a 9 de esta guía.

¿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 o 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?

- Phishing (fraude electrónico)
- Correos electrónicos
- Smishing
- Clone phishing (clonación de fraude electrónico)
- Vishing (uso delictivo del teléfono)
- Skimmers (clonadores de tarjetas)
- Whaling (fraude electrónico focalizado)
- Doxing (publicación de datos para acoso)

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

Existen seis pasos simples que los alumnos pueden 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. Verifica tu informe crediticio con tus padres cuando tengas 16 años.
5. Ten cuidado con las estafas.
6. Protege tu correo.

¿Sabías?

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

Objetivos del aprendizaje, cont.

¿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.

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

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

Esquema de secciones del módulo con el Guión para facilitadores

Introducción: Calentamiento

Pregunta: ¿Cuántos de ustedes han escuchado acerca del robo de identidad?

Encuesta grupal: Pregunta: ¿A qué porcentaje de niños creen ustedes que se les ha robado la identidad? (1%, 2%, 5%, 10%).

Verdades que no conocías: Al 10% -1 de cada 10 niños- alguien les usa el número del Seguro Social. Exploraremos cuáles son las características del robo de identidad y cómo evitarlo.

Examen anterior opcional: Haz que los alumnos vayan a la página 6 de la guía de actividades para alumnos y respondan las preguntas con la respuesta que corresponda (a, b, c o d).

Conceptos básicos del robo de identidad

Comparte: Existen muchos tipos de robo de identidad asociados con tu información financiera. A continuación, se enumeran algunos tipos habituales de estafas:

- **Phishing** se refiere a estafas que intentan engañar a los consumidores para que revelen datos personales tales como números de cuentas bancarias, contraseñas, números de tarjetas de pago o números de cuentas de seguros.
- **Los correos electrónicos** que provienen de fuentes sospechosas pueden ser intentos de 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** es similar a una estafa por fraude electrónico (phishing). 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), una tienda favorita u 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.
- Por clonación de fraudes electrónicos **(Clone phishing)** se entiende el reenvío de un correo electrónico que ahora tiene un adjunto o enlace malicioso. No abras adjuntos de correos electrónicos sospechosos; pueden contener virus para infectar su computadora.

¿Sabías?

Típicamente, el fraude electrónico en línea solicita datos personales, por ejemplo, el apellido de soltera de tu madre y tu fecha de nacimiento.

Esquema de secciones del módulo con el Guión para facilitadores, cont.

- **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 reingresar la configuración de seguridad asociada a la cuenta.
- **Los clonadores de tarjetas** son dispositivos que los defraudadores colocan en un cajero automático, el surtidor de una estación de servicio o la caja de una tienda para copiar la información de tu tarjeta de débito o crédito.
- Las estafas por fraude electrónico focalizado (**whaling**) están 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.

¿Sabías?

A fin de reducir el riesgo de robo de identidad cuando compras por Internet, sólo adquiere productos en sitios seguros que comiencen con https://

Cómo prevenir fraudes

Comparte: Un paso importante para proteger tu identidad es ser consciente de los riesgos comunes y de las estrategias de prevención. Existen seis pasos simples que puedes seguir para reducir el riesgo de ser víctima del robo de identidad.

¿Sabías?

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

1. Practica el uso seguro de la Internet.

Elimina los correos electrónicos no deseados que soliciten datos personales y mantén actualizados los software de antivirus y espía. Compra a través de Internet sólo en páginas web seguras (verifica en la barra de domicilio que aparezca "https" al lado de la imagen de un candado). Nunca envíes por correo electrónico números de tarjetas de crédito, del Seguro Social ni otros datos personales. Analiza las políticas de privacidad de las aplicaciones de telefonía móvil antes de descargarlas y de autorizar el acceso a tus cuentas de redes sociales.

2. Destruye los registros financieros personales innecesarios.

Tritura los documentos innecesarios que contienen tu información personal. Ellos podrían ser, entre otros, documentos escolares con detalles personales, facturas de teléfonos celulares, recibos de cajeros automáticos o tarjetas de débito, o resúmenes de una cuenta corriente o de ahorro.

3. Protege tu número del Seguro Social.

Los ladrones buscan tu número del Seguro Social porque puede ayudarlos a acceder a tu crédito y abrir cuentas falsas. Nunca lleves tu tarjeta contigo; memoriza el número y guárdala en un lugar seguro.

Esquema de secciones del módulo con el Guión para facilitadores, cont.

4. **Controla tu informe crediticio.**
   Los informes crediticios muestran tu grado de responsabilidad en el uso de dinero en el pasado. La mayoría de los jóvenes de menos de 18 años no tienen un informe crediticio. Sin embargo, debido al crecimiento del robo de identidad, se recomienda verificar tu informe con tus padres cuando estés cerca de cumplir 16 años a fin de asegurarte de que nadie se haya apoderado de tus datos para abrir cuentas fraudulentas. Ocasionalmente, los jóvenes tendrán informes crediticios genuinos antes de los 18 años si fueron agregados como usuario autorizado adicional en una tarjeta de crédito de uno de los padres.

5. **Ten cuidado con las estafas.**
   Nunca proporciones información personal por teléfono o correo electrónico a alguien que manifiesta representar a tu banco, a una compañía de tarjetas de crédito, a una agencia gubernamental, a una entidad de caridad ni a ningún otro organismo. Si consideras que la solicitud es legítima, ponte en contacto con la empresa directamente para confirmarla.

6. **Protege tu correo.**
   Vacía periódicamente tu buzón y considera la posibilidad de invertir en una cerradura para él. Cuando envíes pagos de facturas y cheques por correo, considera la posibilidad de dejarlos en la oficina postal o en un buzón seguro.

Comparte: A fin de ser más ágiles en la protección de información, los alumnos trabajarán en equipos para crear un plan de juego. Divide a los alumnos en pequeños grupos. Cada grupo investigará y documentará qué hay que tener en cuenta (toma de conciencia), qué es necesario evitar (prevención) y qué se debe hacer (protección).

Asigna: Cada grupo de alumnos creará un tráiler de uno a dos minutos utilizando el personaje y género provistos. Los tráilers deben incluir: título, lema y una premisa clara centrada en los riesgos/desafíos del personaje. Los riesgos/desafíos del personaje son, entre otros, los siguientes:

- Protección de la identidad en línea (revisando sitios web, compartiendo información, etc.).
- Protección de la identidad en la vida real cuando estás fuera de tu casa (contraseñas, textos, etc.).
- Protección contra la identidad en el hogar y en tus dispositivos (configuración de privacidad, almacenamiento de datos personales, etc.).

Informa: Comparte los tráilers de los grupos y vuelve a enfatizar la importancia de proteger los. Datos personales mediante la toma de conciencia y acciones preventivas. Agrega las estrategias claves que no se visualicen en los tráilers de los alumnos para ayudar a que sus personajes eviten fraudes y el robo de identidad.

Puesta en práctica

Actividad: os estafas y un anuncio; se juega igual que Dos verdades y una mentira. Instruye a los alumnos a que vayan a la página 12 de su guía de actividades para alumnos.

Esquema de secciones del módulo con el Guión para facilitadores, cont.

Dos opciones para el jugar:
Opción 1: Los alumnos juegan con un compañero o en pequeños grupos para evaluar llamadas, correos electrónicos y materiales de mercadeo, según lo descrito en la copia Dos estafas y un anuncio, a fin de determinar si se trata o no de una estafa.
Opción 2: Instruye a los alumnos a que jueguen haciendo visible su disconformidad. Lee en voz alta una opción y haz que los alumnos que consideran que se trata de una estafa se paren y agrupen a la derecha del salón; los que crean lo contrario se pararán y agruparán a la izquierda del salón.

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.

Cómo obtener ayuda si la necesitas

Comparte: Se deben tener en cuenta varios aspectos si estás preocupado por un potencial robo de identidad, fraude y/o violación a la seguridad. Si tu información financiera privada cae en las manos equivocadas, las consecuencias pueden ser devastadoras. Hazles saber a tus padres si recibes correos no deseados, correos de fraudes electrónicos, llamadas o mensajes de texto no deseados o si detectas en tu cuenta una compra que nunca hiciste. 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.
Informa del robo de identidad al departamento de policía de tu área, con la ayuda de tus padres. La policía generará un "informe de robo de identidad", del que tú y tu familia podrán solicitar una copia.

Ponte en contacto con las empresas de informes crediticios.
Comunícate de inmediato con los departamentos de fraudes de cada una de las agencias de crédito, con la ayuda de tus padres. Alértalos de que has sido víctima de robo de identidad y solicítales que coloquen una alerta de fraude en tu archivo. También puedes solicitar un bloqueo de seguridad a fin de evitar que los emisores de crédito obtengan acceso a tus archivos de crédito sin tu autorización. Ello impedirá que los ladrones abran nuevas tarjetas de crédito en tu nombre.

Crea un plan de recuperación contra fraudes.
La Comisión Federal de Comercio puede ayudarte a crear un plan de recuperación si has sido víctima de robo de identidad. Cuando informes lo que sucedió, recibirás un plan de recuperación personalizado y podrás monitorear tus avances paso a paso en línea. Aprende más visitando el sitio web de la Comisión Federal de Comercio (FTC, por su sigla en inglés) (identitytheft.gov).

Esquema de secciones del módulo con el Guión para facilitadores, cont.

Cierre: Debate grupal

Pregúntales a los alumnos: ¿Qué consejo clave les darían a un amigo sobre la prevención del robo de identidad y de fraudes?

Debate

Examen posterior opcional: Haz que los alumnos vayan a la página 6 de su guía de actividades para alumnos a fin de realizar el examen posterior opcional.

Lección 6 - Robo de Identidad: Hoja de respuestas

> Examen anterior y posterior de Robo de identidad.

> 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

Instrucciones: Haz que los alumnos vayan a la página 6 de su guía de actividades para alumnos y respondan las preguntas con la respuesta que corresponda (a, b, c o d) o llenando el espacio en blanco.

Hoja de respuestas

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?

(Posibles respuestas: tu número PIN, tu cuenta de tarjeta de crédito, tus contraseñas de las redes sociales).

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: Divide a los alumnos en pequeños grupos 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. Los tráilers deben incluir: título, lema y un argumento claro. Instruye a los alumnos a que revisen los riesgos y desafíos de su personaje respecto del robo de identidad y a que entiendan los hechos respaldatorios antes de desarrollar sus tráilers. Haz que los alumnos vayan a las páginas 7 a 11 de su guía de actividades para alumnos a fin de completar la actividad de creación de tráilers.

Género de cine

Misterio

Personaje

Femenino, estudiante de secundaria.

Fortalezas del personaje

- Resolución creativa de los problemas.
- Rápido y con habilidades tecnológicas.

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

- Toma decisiones rápidamente
- Fuertes 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 apropiación 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.
- EEs 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 a dvertencia, 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: ¿Pueden los alumnos detectar la estafa? Haz que jueguen con un compañero o equipo pequeño para ver cuántos riesgos de robo de identidad pueden detectar. Sus respuestas deben identificar cada escenario como "estafa" o "anuncio", y explicar por qué. Deben incluir consejos o mejores prácticas para la protección de su identidad. Instruye a los alumnos a que vayan a las páginas 12 y 13 de su guía de actividades para alumnos a fin de completar el ejercicio.

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. Te dicen que, para poder finalizar el trámite del premio, necesitan tu dirección y datos bancarios.

Respuesta: *Estafa. Una oferta válida de beca no te exige proporcionar información bancaria por teléfono. Pregúntate: ¿Quién llama? ¿Qué solicita y por qué?*

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.

Respuesta: *Es muy probable que se trate de un anuncio si es una tienda y sitio web reconocible.*

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.

Respuesta: *Estafa. Evita abrir enlaces que no reconozcas. Podría instalar malware o ser un fraude electrónico para saber tus datos.*

¿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.

Respuesta: *Es muy probable que sea un anuncio.*

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. Necesita 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.

Respuesta: *Estafa. Evita dar información financiera a contactos que no puedes validar.*

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".

Respuesta: *Estafa. Evita abrir enlaces que no reconozcas. Podría instalar malware o ser un fraude electrónico para saber tus datos.*

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

¿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.

Respuesta: *Estafa/Riesgo de robo de identidad: Esta práctica de compartir datos personales sin el permiso de la persona se denomina doxing y puede causar problemas graves.*

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

Respuesta: *Es muy probable que sea un anuncio; sin embargo, es importante proteger tu privacidad y limitar el acceso de las aplicaciones a tus datos personales. Considera la posibilidad de denegar a todas las aplicaciones el acceso a tu cámara, micrófono y GPS.*

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.

Respuesta: *Riesgo de robo de identidad: Si bien no son siempre estafas, los cuestionarios en línea de aplicaciones y sitios aleatorios que requieren acceso a tu perfil en las redes sociales pueden permitir el acceso a información de tu cuenta en las redes sociales para rastrear comportamientos futuros. Considera leer la letra chica o limitar lo que compartes con terceros.*

Glosario de términos

Haz que los alumnos estudien esta lista de términos de finanzas personales a fin de prepararlos antes de jugar Fútbol Financiero. Si dominan estos términos, tendrán 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.