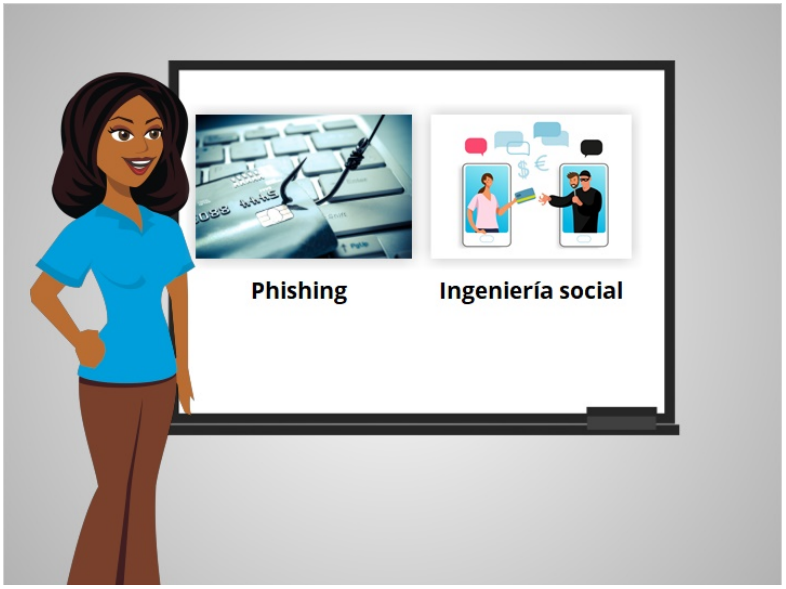
Fraudes y estafas en línea

Tipos de estafas

Hola, soy Belle. Hay muchas cosas que usted puede hacer para protegerse del fraude y mantener sus cuentas y dispositivos a salvo de las estafas en línea. Vamos a seguir a Albert para aprender qué tipos de estafas existen, cómo reconocer las señales de advertencia, cómo responder cuando vea una estafa y cómo reportar una estafa.

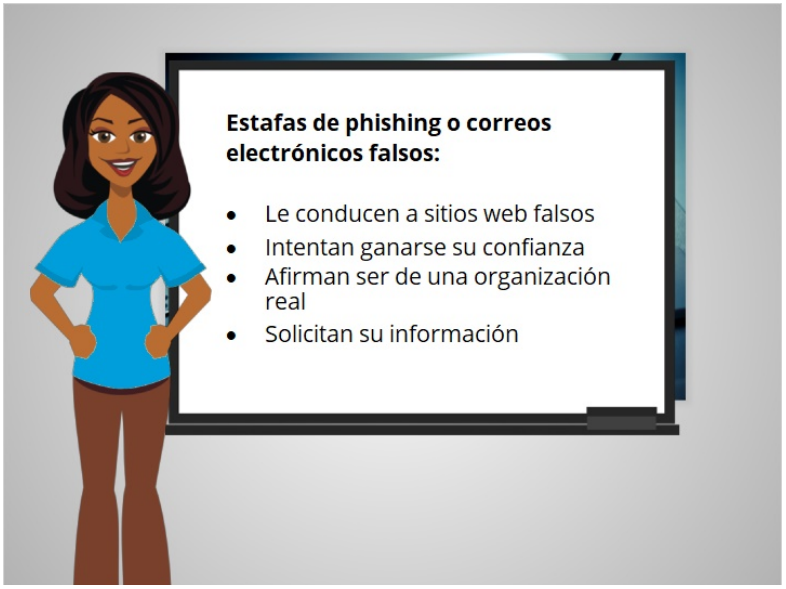
Las estafas en línea pueden venir en muchas maneras y formas. Vamos a ayudar a Albert a aprender cómo reconocer y evitar los tipos más comunes de fraude y estafas cuando está en línea.



Algunos de los tipos más comunes incluyen el phishing (suplantación de identidad) y la ingeniería social.

Estos tipos de estafas se pueden encontrar en un sitio web, en un correo electrónico o mensaje de texto, o incluso en una ventana emergente en su computadora.

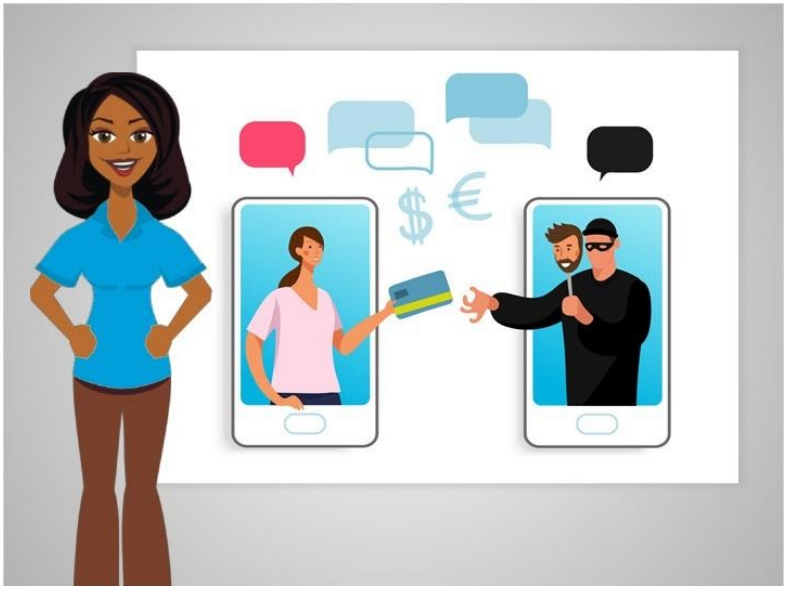
Comencemos hablando del phishing, que es un tipo común de estafa. El phishing es cuando los estafadores usan correos electrónicos o mensajes de texto falsos para "pescar" información.



Estos mensajes falsos pueden parecer reales, pero enlazan a sitios web falsos. El sitio web puede parecer el de una compañía, organización o agencia gubernamental confiable y bien conocida, pero todo es un engaño para obtener información, tal como su número de Seguro Social o de su banco y los números de cuenta de sus tarjetas de crédito.

Un correo electrónico falso también se puede usar para infectar su computadora con software malintencionado, que se conoce como malware, o con un virus tan pronto como abra el correo electrónico. El malware es una herramienta utilizada por los estafadores que puede adoptar muchas formas diferentes. Por ejemplo, el malware puede conducir a virus que infectan su computadora o a “spyware” que rastrea sus actividades en línea.

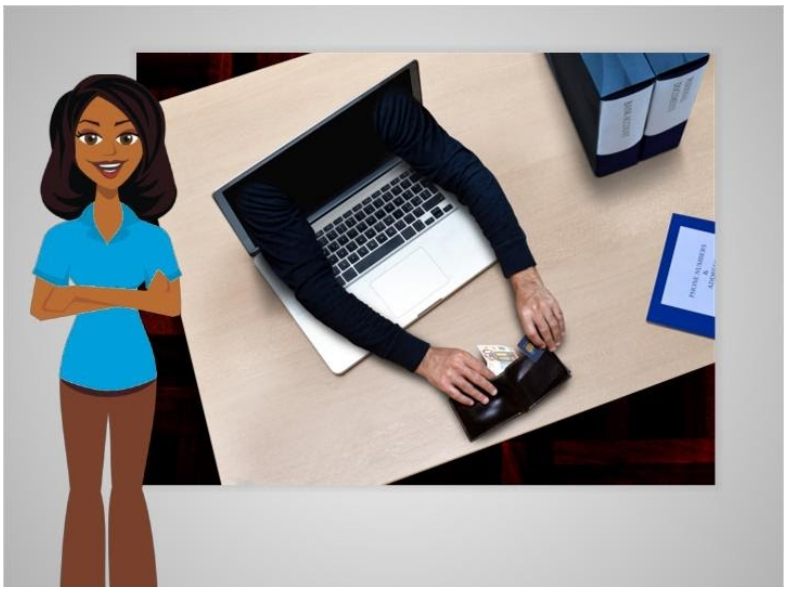
Es posible que usted pueda saber cuándo se ha instalado malware en su computadora o dispositivo si ve estas señales: aparecen anuncios en ventanas emergentes que son difíciles de cerrar; aparecen en la pantalla iconos nuevos o desconocidos en la barra de herramientas; o su computadora o dispositivo móvil no responde tan rápido como solía hacerlo.



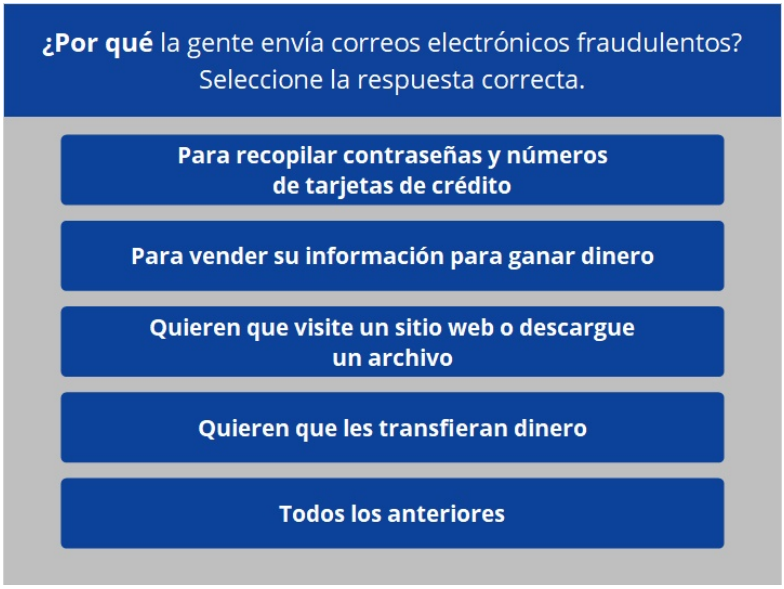
La ingeniería social es otro tipo común de estafa. Este es un nuevo nombre para un viejo truco de los estafadores. En este tipo de estafa, un impostor intenta ganarse su confianza al hacerse pasar por otra persona para obtener su información personal.

Por ejemplo, la persona puede afirmar ser un amigo o familiar en problemas, pretender ser una empresa con un descuento u oferta estupenda, o aseverar que trabaja en nombre de una agencia gubernamental, una organización o agencia de cobranza.

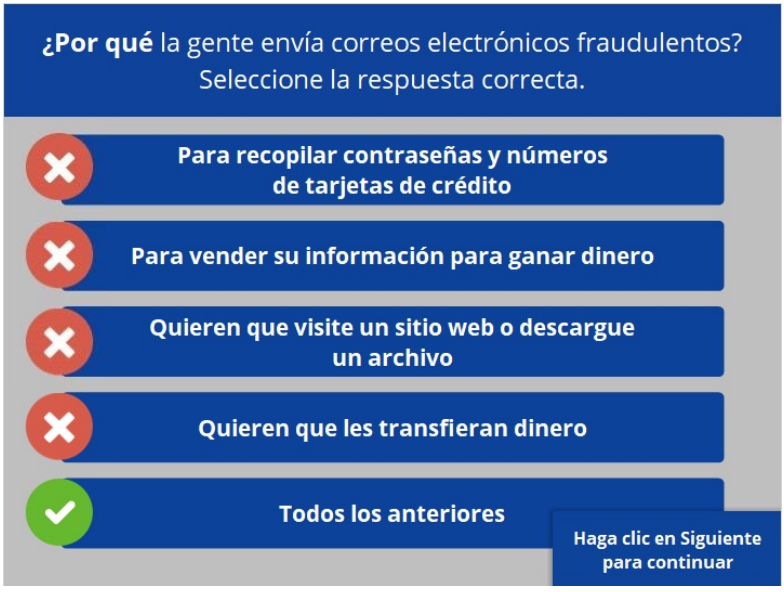
Estos estafadores pueden ponerse en contacto con usted por teléfono, correo electrónico, mensaje de texto o a través de las redes sociales.



Independientemente de la forma que adopte una estafa, los estafadores suelen tener los mismos objetivos: robar su dinero o recopilar información como sus contraseñas o números de tarjetas de crédito. Las estafas también ocasionan problemas en su computadora al infectarla con virus o malware.



Veamos qué recuerda sobre los correos electrónicos fraudulentos. ¿Por qué la gente envía correos electrónicos fraudulentos? Seleccione la respuesta correcta.



La respuesta correcta es todas las anteriores. Los correos electrónicos fraudulentos se envían por diversas razones. Saber qué buscar puede ayudarle a protegerse contra el fraude y mantener sus cuentas y dispositivos a salvo de las estafas en línea. Haga clic en Siguiente para continuar.

En esta lección, Albert aprendió sobre los tipos comunes de fraudes y estafas, incluidos el phishing y la ingeniería social. Aprendió que puede encontrar estos tipos de estafas mientras hace una búsqueda en un sitio web, en un correo electrónico o mensaje de texto, o incluso en una ventana emergente de su computadora. En la próxima lección, Albert aprenderá algunos consejos que le ayudarán a identificar las estafas en línea, en los correos electrónicos y en los mensajes de texto.

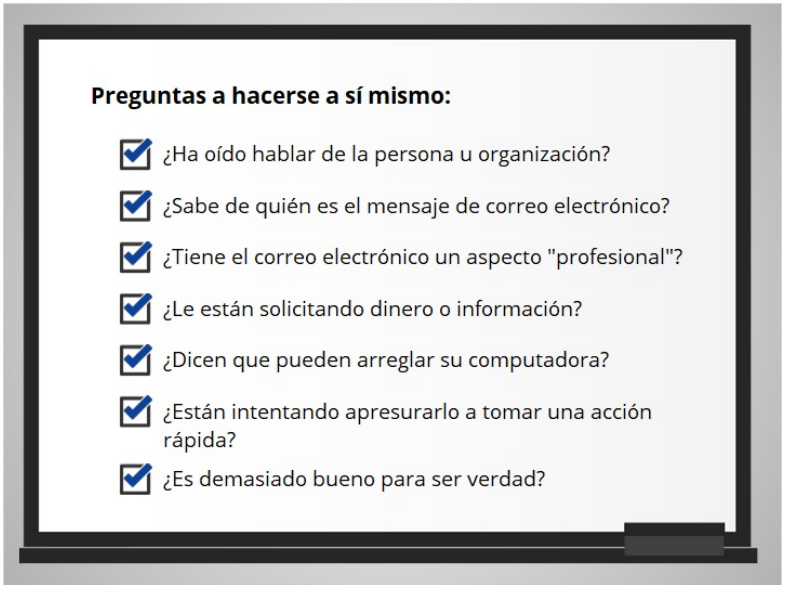
Haga clic en el botón azul para finalizar esta lección.

Fraudes y estafas en línea

Reconocer las estafas

¿Cómo puede saber si algo es una estafa o un fraude?

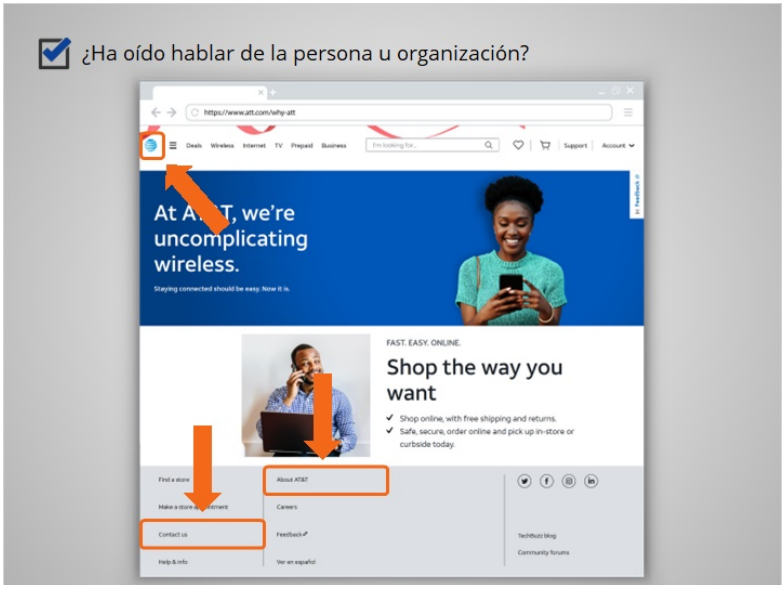
En esta lección, Albert aprenderá varios consejos que le ayudan a identificar las estafas en línea, en su correo electrónico y en sus mensajes de texto.



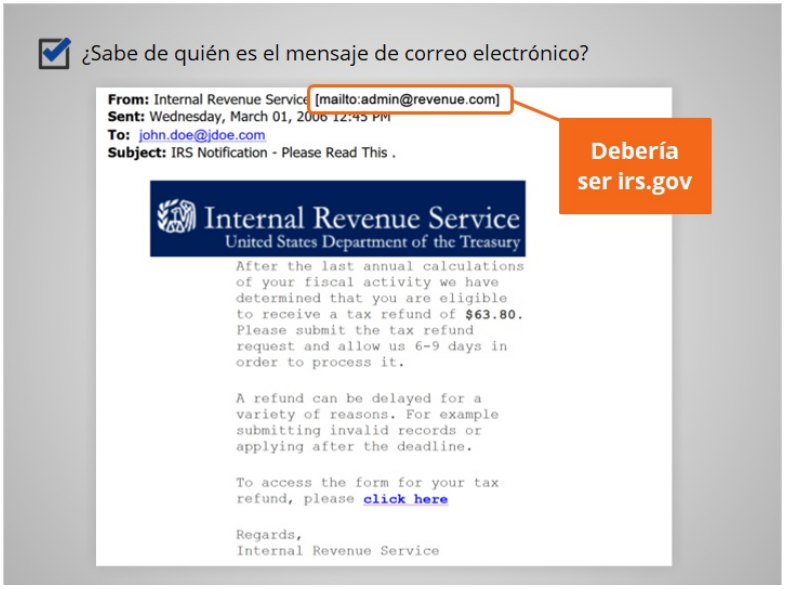
Aquí hay algunas preguntas que debe hacerse a sí mismo si no está seguro.

- ¿Ha oído hablar de la persona u organización?
- ¿Sabe de quién es el mensaje de correo electrónico?
- ¿El correo electrónico tiene un aspecto profesional?
- ¿Le están solicitando dinero o información?
- ¿Dicen que pueden arreglar su computadora?
- ¿Están intentando apresurarlo a tomar una acción rápida?
- ¿Es demasiado bueno para ser verdad?

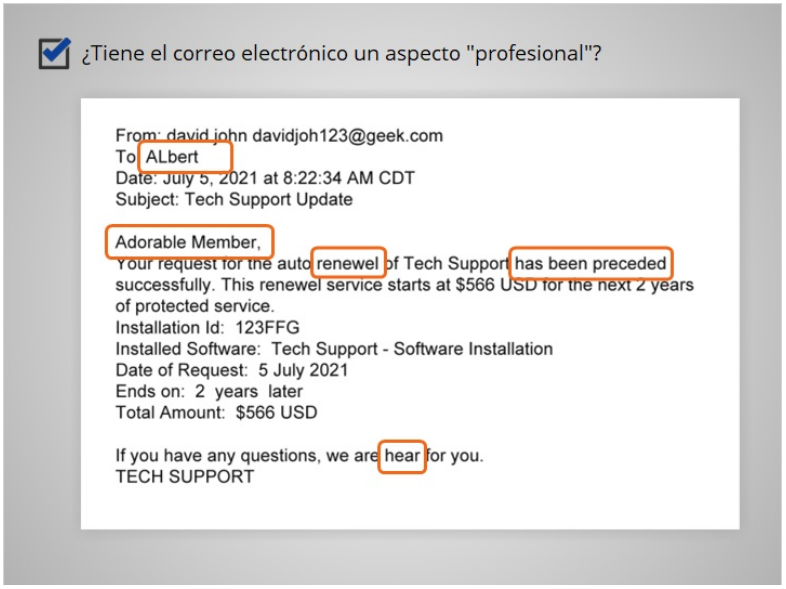
Vamos a verlas una por una.



¿Ha escuchado hablar antes de la persona u organización? Albert está haciendo una búsqueda en la web y encontró este sitio web. Si se trata de un negocio legítimo, como en este ejemplo, su logotipo oficial, dirección e información de contacto deben aparecer en su sitio web.



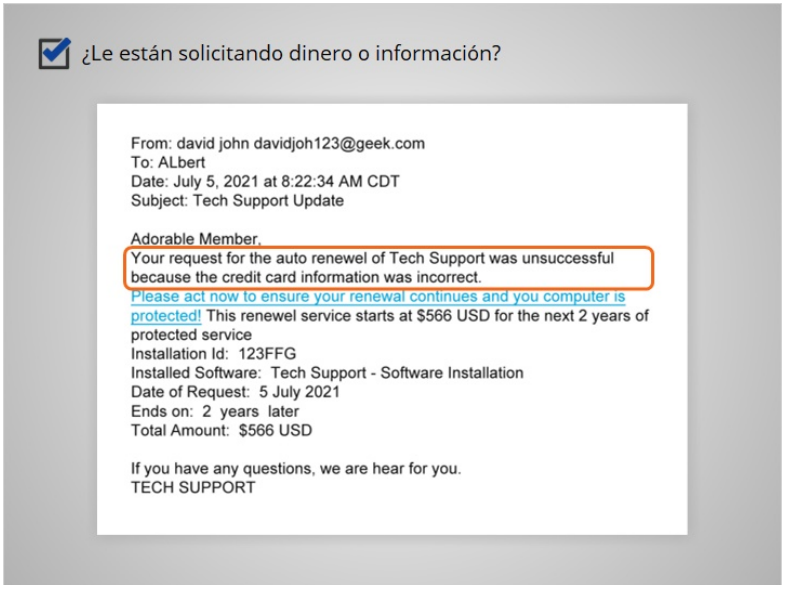
¿Sabe de quién es el mensaje de correo electrónico? Albert recibió un correo electrónico que dice ser del IRS. Pero la dirección de correo electrónico termina con un proveedor de correo electrónico desconocido, no con irs.gov. Esta es una clara señal de que es una estafa de phishing.



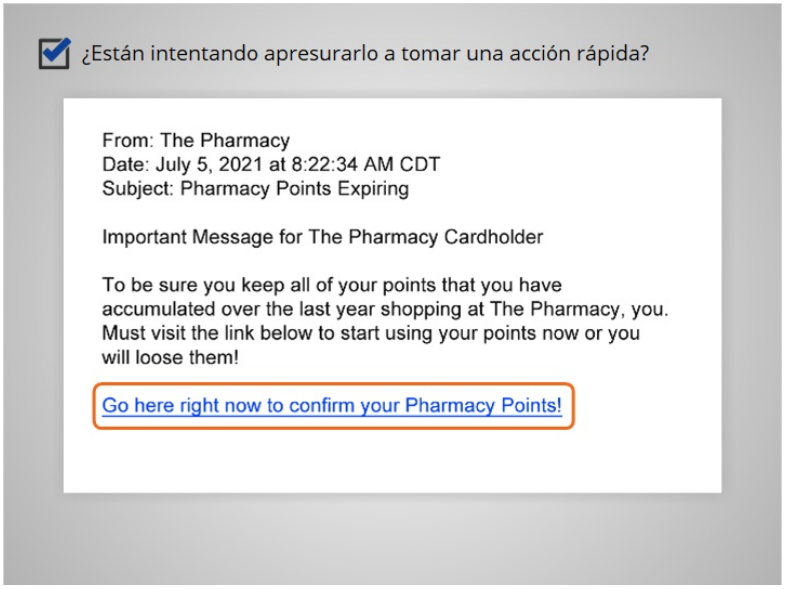
¿El correo electrónico tiene un aspecto profesional? Albert ha recibido un correo electrónico de una compañía en la que tiene una cuenta. Pero cuando recibe otros correos electrónicos de compañías con las que tiene una cuenta, estos normalmente incluyen su nombre. Este solamente dice, "Miembro adorable".

Albert nota que hay errores ortográficos y gramaticales en el correo electrónico. Si el correo electrónico es de una empresa legítima, no tendría esos errores.

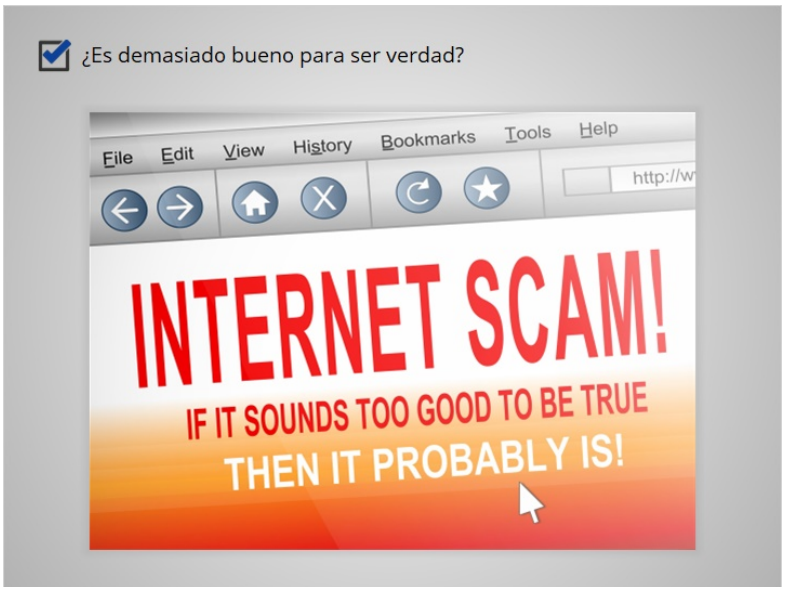
¿Afirman que pueden arreglar su computadora? Albert está haciendo una búsqueda en la web y recibió un mensaje en una ventana emergente. Este le dice que su computadora está infectada y que debe hacer clic en un enlace o llamar a un número para que la pueda arreglar. Las compañías legítimas nunca le solicitarán que arregle su computadora de esta manera.



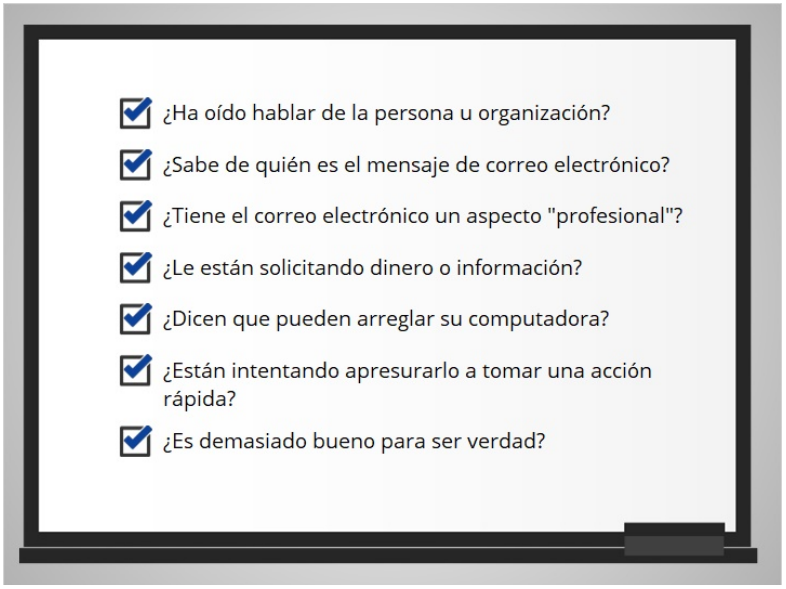
¿Le están solicitando su información? En este correo electrónico que Albert recibió, el estafador solicita la información de su tarjeta de crédito. Los estafadores pueden afirmar que necesitan verificar o actualizar su información. Algunos estafadores también le pedirán que les hagan un giro de dinero o les envíen un depósito, prometiendo pagarle más a cambio.



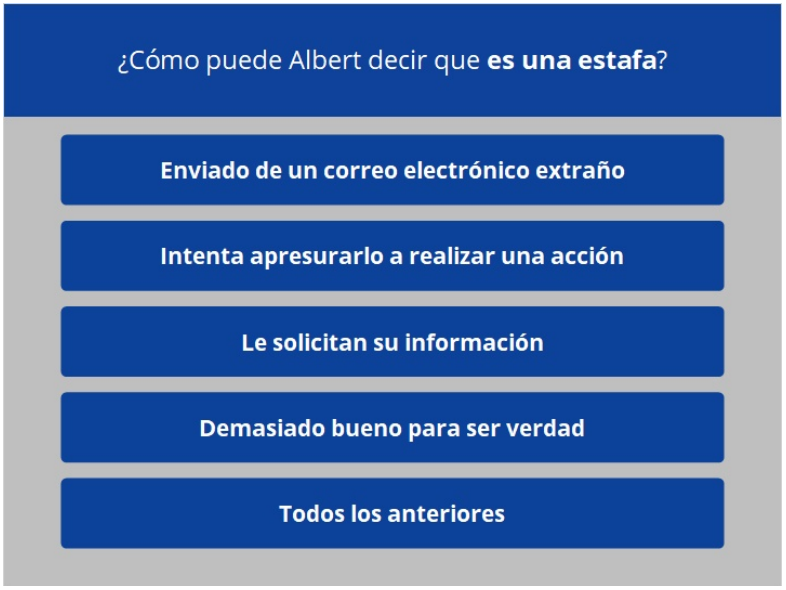
¿Están intentando apresurarlo a realizar una acción rápida antes de tomarse el tiempo para pensarlo? Albert ha recibido este mensaje sobre el vencimiento de los puntos de su farmacia. Algunos estafadores intentan asustarle para que actúe con rapidez, amenazándole con que sucederá algo malo, como que cerrarán una cuenta. Otros estafadores le prometerán algo bueno, pero solo si usted responde de inmediato.



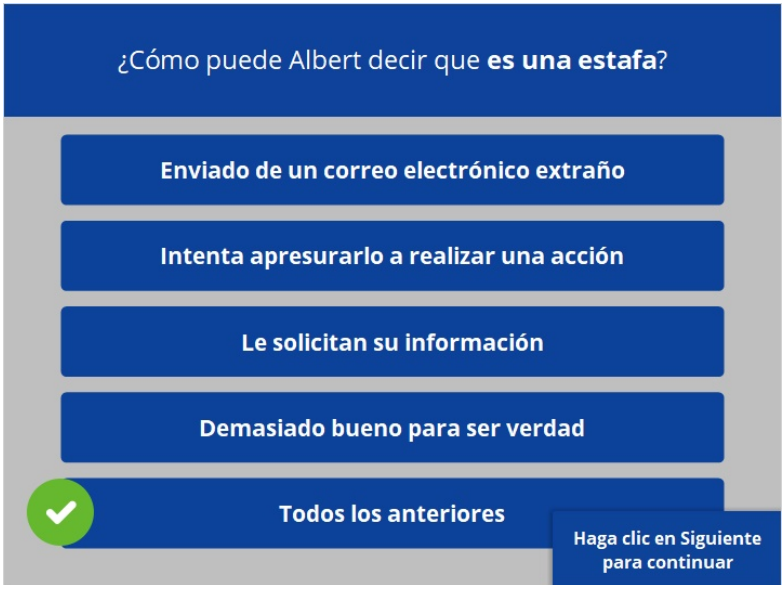
¿Es demasiado bueno para que sea verdad, como que ganó el premio de un concurso en el que no recuerda haber participado? Si suena demasiado bueno para ser verdad, probablemente lo sea.



¡Muy bien, hemos revisado todo en la lista! Veamos qué recuerda sobre cómo reconocer a las estafas.



Albert está mirando un correo electrónico en su bandeja de entrada y no está seguro de que sea una estafa. ¿Cómo puede decir que es una estafa? Seleccione la respuesta correcta.



La respuesta correcta es todas las anteriores. Hay una variedad de formas para determinar si un correo electrónico, un sitio web o un mensaje de texto es una estafa. Saber cómo identificar una estafa puede ayudarle a protegerse contra el fraude y mantener sus cuentas y dispositivos seguros. Haga clic en Siguiente para continuar.

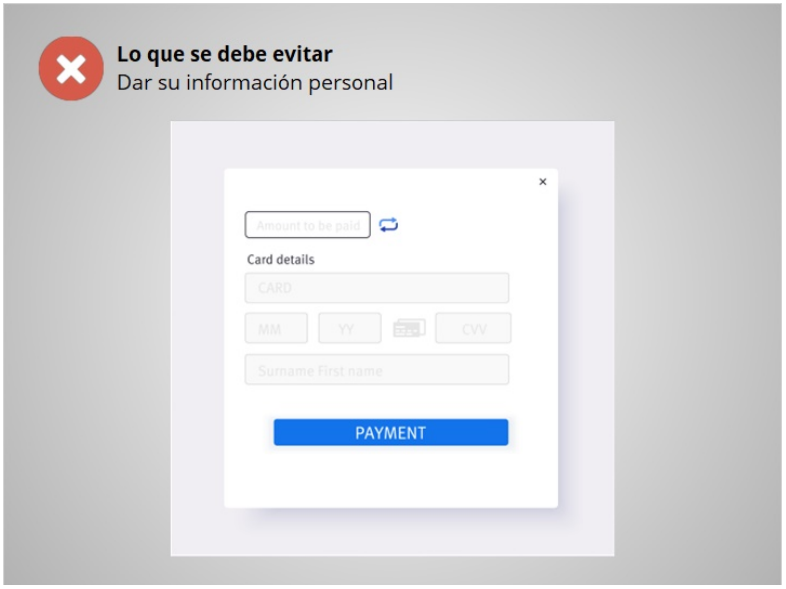
En esta lección, Albert aprendió algunos consejos que le ayudarán a identificar las estafas en línea, en su correo electrónico, en un sitio web y en un mensaje de texto. En la siguiente lección, Albert aprenderá lo que debe hacer con una estafa una vez que la ha identificado.

Fraudes y estafas en línea

Qué hacer con las estafas

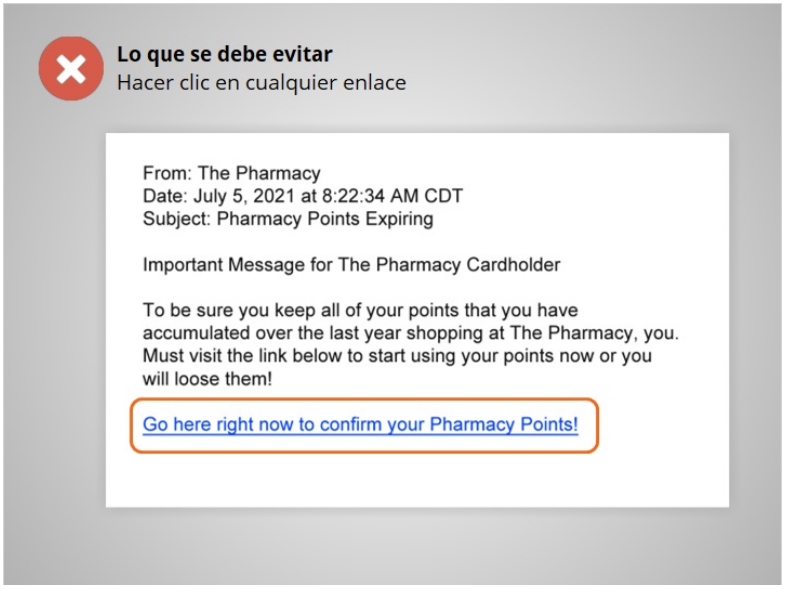
Ahora que Albert ha aprendido a reconocer los fraudes y estafas comunes, quiere saber qué puede hacer cuando encuentra uno.

Estas son algunas de las cosas que debe y no debe hacer. Revisaremos cada una de ellas.



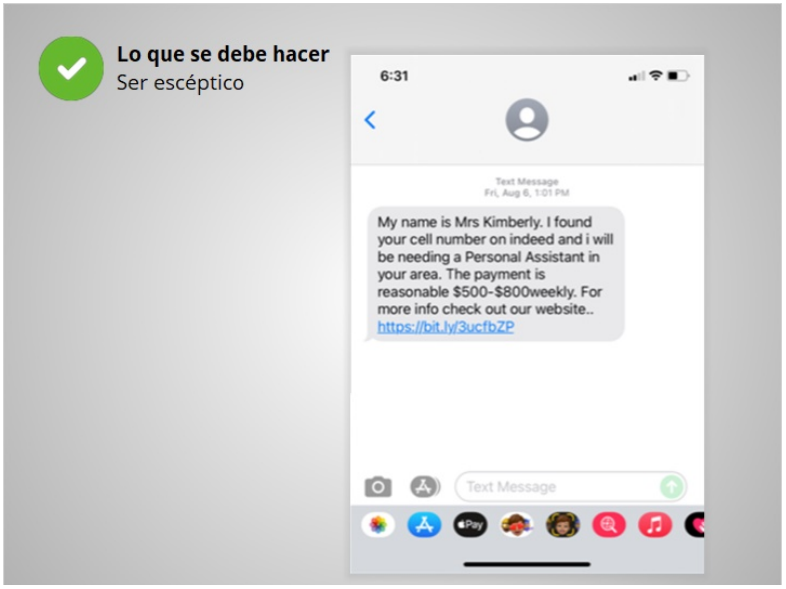
No proporcione información personal a algo que podría ser una estafa. Esto incluye el nombre, la dirección de correo electrónico, el número de tarjeta de crédito o la contraseña.

No responda ni se comunique con ellos. Esto puede notificarle al estafador que se ha comunicado con una persona real, lo que puede resultar en más correos electrónicos fraudulentos.



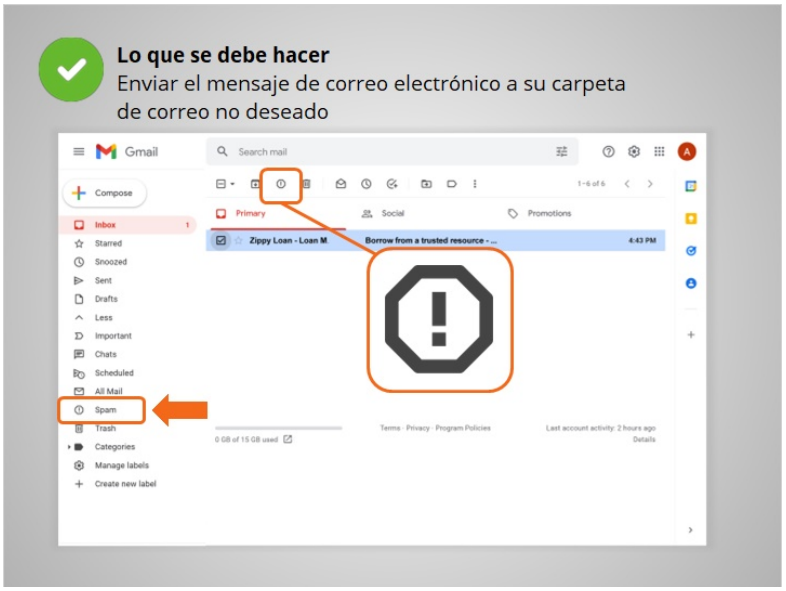
No haga clic en ninguno de los enlaces en un mensaje de correo electrónico de estafa. Esto puede llevarlo a sitios web no confiables.

No descargue ningún archivo no documento adjunto de un sitio web poco confiable. Pueden contener virus o malware que dañan su computadora o que recolectan su información personal.

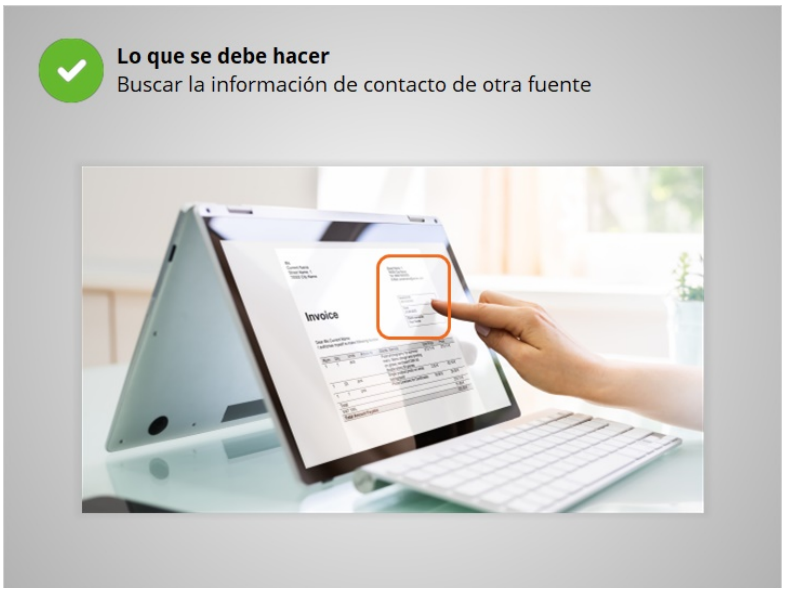


Sea escéptico. Si cree que algo es una estafa, probablemente lo es.

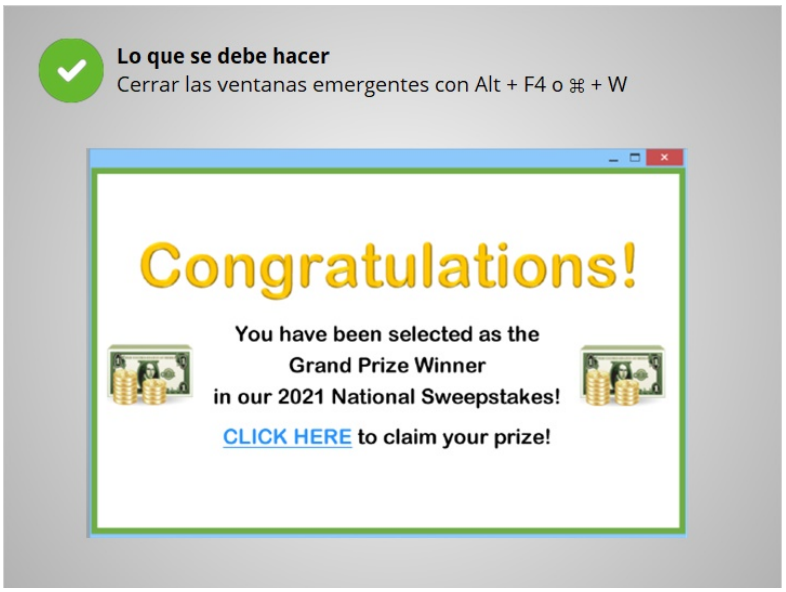
Recuerde leer atentamente los correos electrónicos y los mensajes de texto, asegurándose de que conoce al remitente.



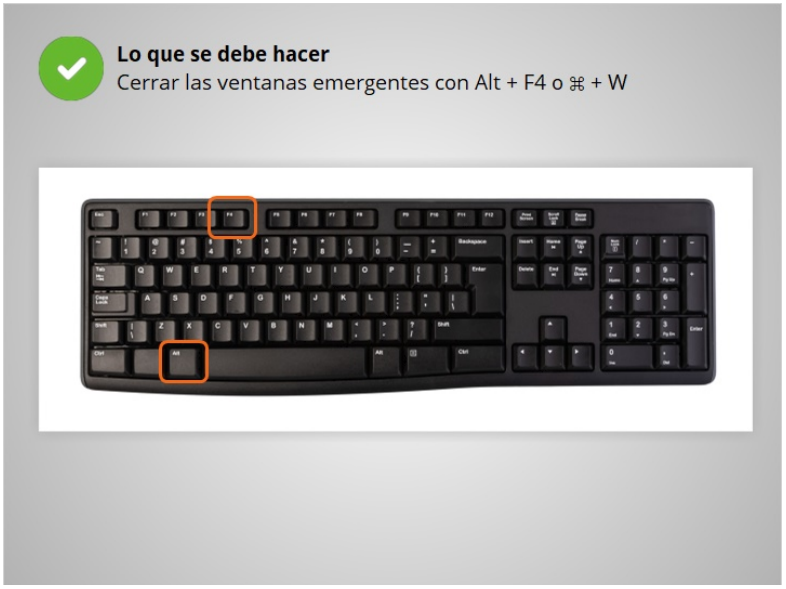
La mayoría de los correos electrónicos marcados como spam (correo no deseado) se mueven automáticamente a la carpeta Spam, por lo que no los ve en la Bandeja de entrada. Este es un ejemplo de la carpeta Spam en Gmail. Si ve un correo electrónico no deseado en su bandeja de entrada, márquelo como correo no deseado en su correo electrónico. Evite abrir el mensaje, hacer clic en los enlaces o ver las imágenes en el mensaje.



Busque su información de contacto por su cuenta, en un estado de cuenta que haya recibido por correo o en su sitio web oficial.

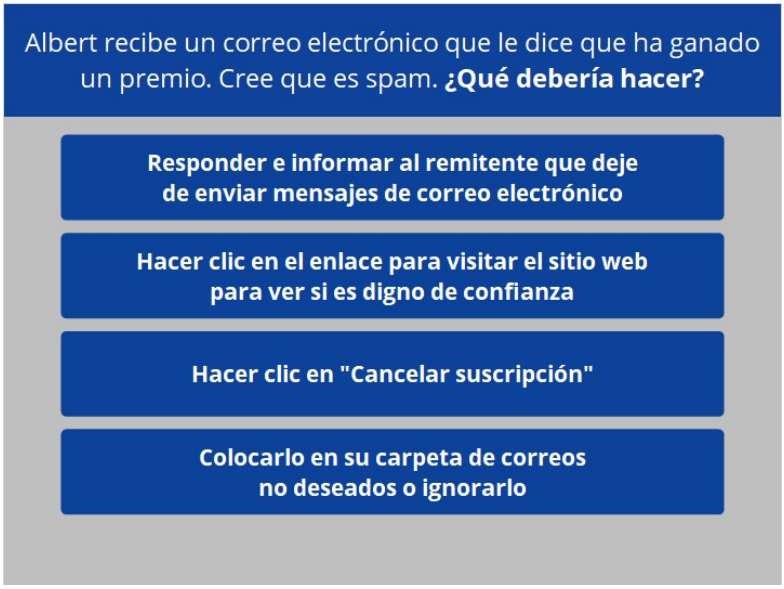


Para las ventanas emergentes en un sitio web, no haga clic en ninguno de los botones. A veces, incluso hacer clic sobre la X no cerrará una ventana emergente de estafa y puede provocar que se abran más ventanas emergentes en su lugar.

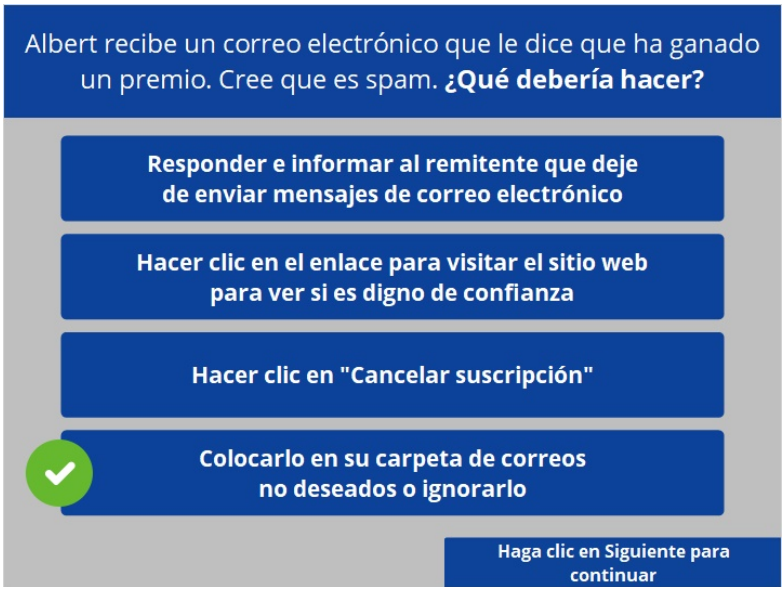


Intente usar otro método para cerrar la ventana emergente. Una forma de cerrarla es mantener presionada la tecla Alt mientras presiona F4 en una PC y Command-W en una Mac. Esto cerrará la ventana. Si todo lo demás falla, reinicie su computadora o apáguela y vuelva a encenderla. Esto es mejor que quedar atrapado en una estafa.

Ahora, vamos a verificar lo que recuerda.



Albert recibe un correo electrónico que le dice que ha ganado un premio. Él piensa que probablemente sea un correo electrónico no deseado. ¿Cómo debería reaccionar Albert a este correo electrónico fraudulento? Haga clic en la respuesta correcta.



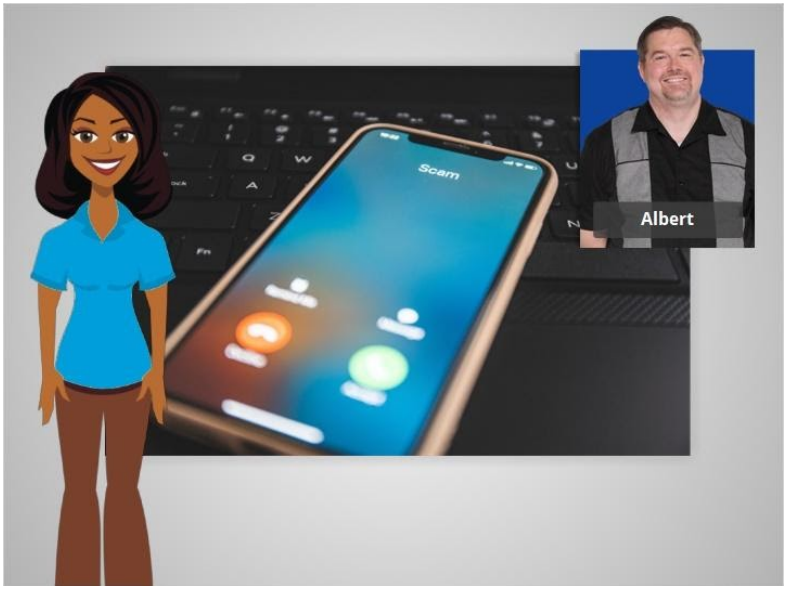
¡Eso es correcto! Comunicarse con el remitente puede ocasionar que reciba más mensajes de correo electrónico no deseados. Hacer clic en cualquier enlace de un correo electrónico fraudulento puede ocasionar que reciba más mensajes no deseados y que lo lleve a sitios web inseguros.

Ahora Albert sabe lo que puede hacer cuando se encuentra con una estafa en un sitio web, en un correo electrónico o en un mensaje de texto. Cuando Albert sigue estos consejos, puede mantenerse a salvo cuando se encuentra con una estafa. En la próxima lección, Albert aprenderá cuándo y cómo denunciar las estafas.

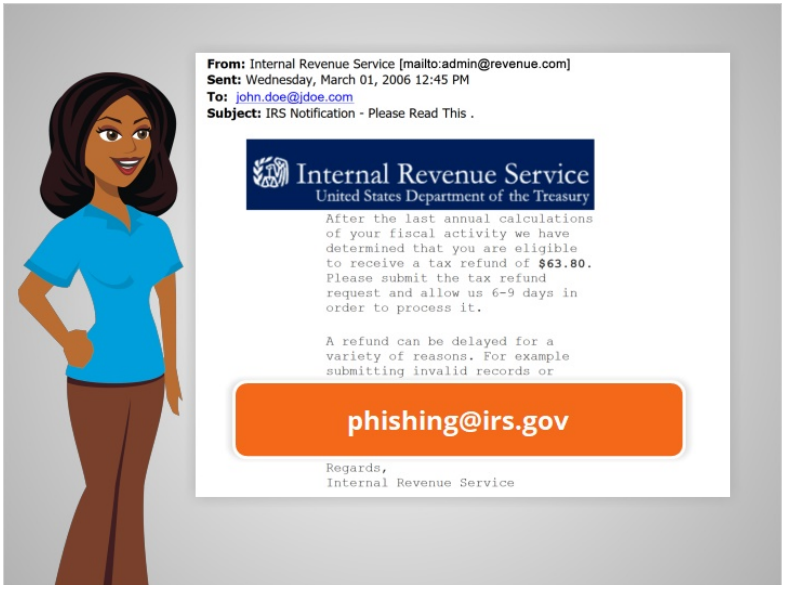
Haga clic en el botón azul para finalizar esta lección.

Fraudes y estafas en línea

Reportar las estafas



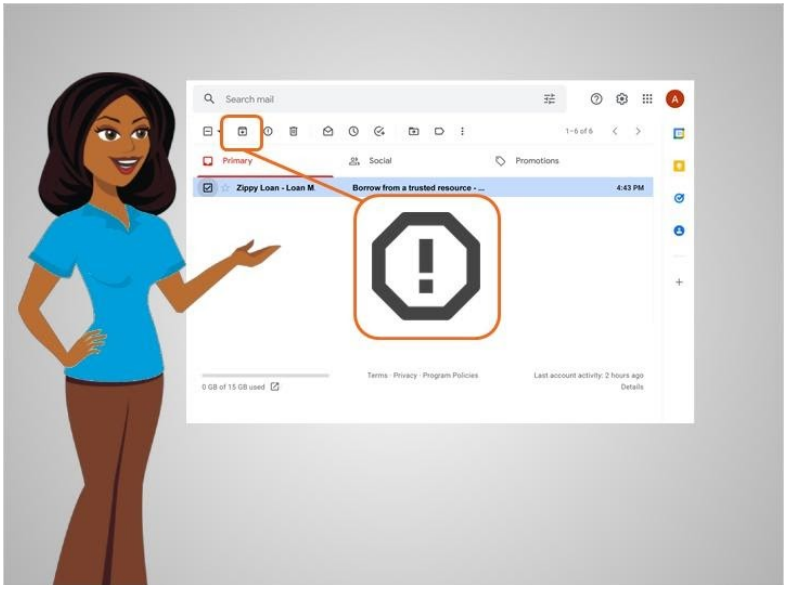
Las estafas en línea pueden originarse en cualquier parte del mundo. Esto hace que sea muy difícil o incluso imposible rastrear a los estafadores que están detrás de ellos. Sin embargo, hay algunas acciones que usted puede tomar para ayudar a proteger a otros de caer en el mismo fraude o estafa. En esta lección, Albert aprenderá cuándo y cómo denunciar estafas.



Si encuentra una estafa de phishing (suplantación de identidad) que imita a una organización que conoce, puede comunicarse con esa organización.

Pero recuerde no utilizar la información de contacto del correo electrónico. Busque la información en una fuente diferente.

Por ejemplo, Albert recibió este correo electrónico sospechoso que decía ser del IRS. Al hacer su investigación, Albert descubre que el IRS tiene un proceso para reportar este tipo de estafas, por lo que Albert lo reenvía a phishing@irs.gov.



Cuando Albert recibe un correo electrónico falso, lo coloca el mensaje en su carpeta de correo no deseado o basura. En este ejemplo, Albert está usando Gmail. Esto ayuda a los proveedores de correo electrónico a identificar y prevenir las estafas.

Usted también puede presentar quejas oficiales ante la Comisión Federal de Comercio visitando su sitio web en reportfraud.ftc.gov.

En esta clase, aprendimos junto con Albert los tipos de estafas que existen, cómo reconocer las señales de advertencia, cómo responder al ver una estafa y cómo denunciarla.

Recuerde las señales de advertencia que ha aprendido en este curso para protegerse y proteger a sus dispositivos de los fraudes y estafas en línea.

Haga clic en el botón azul para finalizar este curso.