ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

¿Sabes identificar cuándo te están estafando?

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*

Índice

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*

1. ¿Sabes identificar cuándo te están estafando?

Los ataques de phishing intentan engañar a usuarios desprevenidos para que revelen información personal o financiera, a menudo mediante la imitación de contenidos provenientes de empresas reconocidas y de confianza. La inteligencia artificial ya está haciendo que estos ataques sean más sofisticados, personalizados y frecuentes.

2. Clasificación

Categoría	**Marcar si aplica:**
Sector	☐ Sanitario
	☑ Público general
	☐ Otro
Temas cubiertos	☑ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ Prevención
	☐ Impacto (ej. Cuando está ocurriendo o ha ocurrido) en el cuidado del paciente
	☐ Impacto en otras actividades que no implican el cuidado del paciente
Idioma del material original	☑ Neerlandés
	☑ Inglés

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*

	☑ Alemán
	☑ Italiano
	☑ Español (versión en vídeo disponible)
Tipo del material	☑ Preguntas de cuestionario
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Descripción

¿Crees que nos puedes decir si es real o falso?

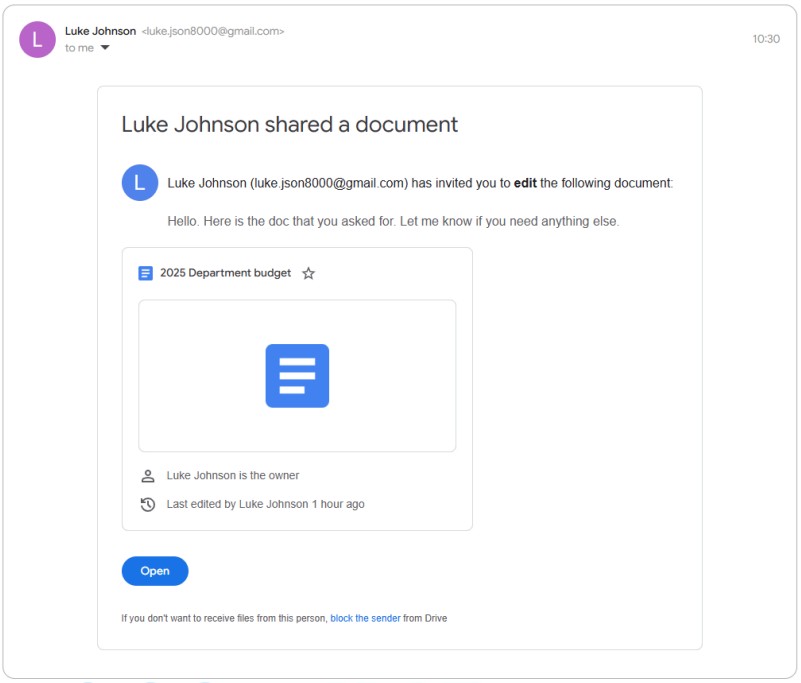
1. Empecemos con este e-mail con un documento de google.

   PREGUNTA: Asegúrate de revisar las direcciones de los enlaces pasando el cursor por encima o manteniendo presionado, y de explorar las direcciones de correo electrónico. No te preocupes. Ninguno de los enlaces funcionará: ¡no queremos enviarte a ningún sitio raro!

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: PHISHING, debiste haber notado la URL que se parece a la real. Ten cuidado con los hipervínculos y los archivos adjuntos que abras en los correos electrónicos: pueden dirigirte a sitios web fraudulentos donde se te pida ingresar información confidencial. Al pasar el cursor sobre el enlace o mantener presionado, verás que lleva al dominio falso e inseguro 'drive–google.com'.'.

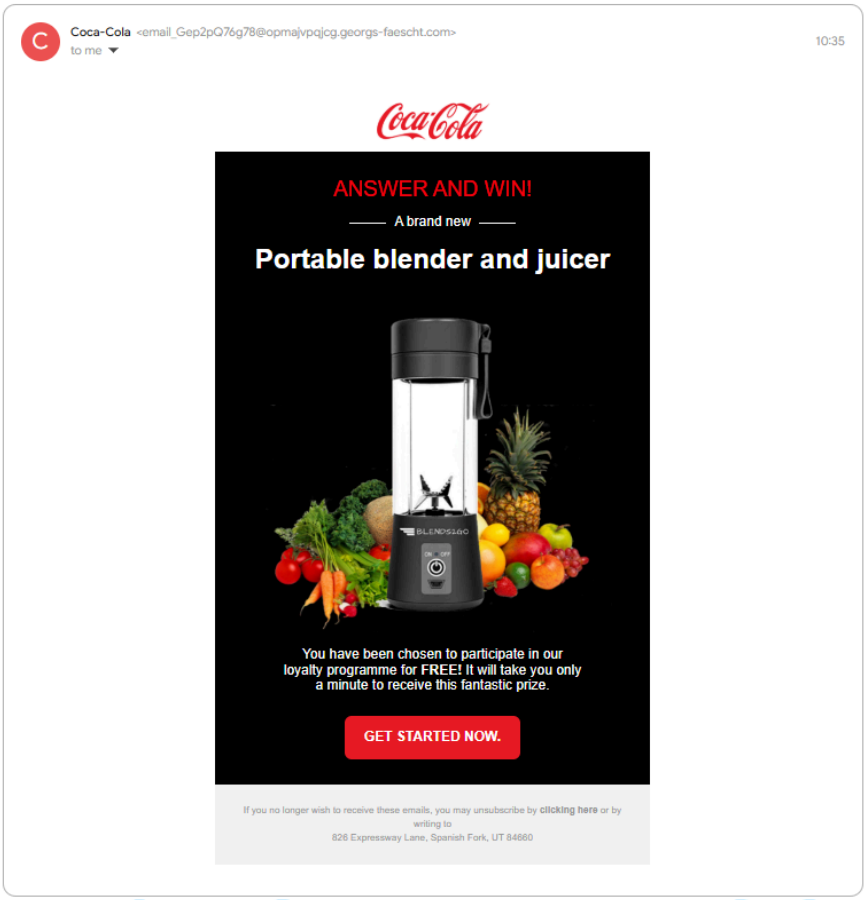
2. Hora de animar las cosas un poco:

   PREGUNTA: Una licuadora gratis es un buen incentivo para una encuesta.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: PHISHING, el correo afirma ser de Coca-Cola, pero la dirección del remitente es muy aleatoria —no imposible en un correo legítimo, pero sí sospechosa. El contenido, incluso el texto, está todo dentro de una imagen. Aunque se usa en algunas comunicaciones legítimas, esta técnica también se emplea para evitar la detección. La URL está diseñada para ocultar varios redireccionamientos y eludir la detección por parte del proveedor de alojamiento activándose únicamente con el texto que sigue al carácter '#'. (Normalmente ese fragmento es un código corto que se usa para enlazar a una ubicación concreta en una página).

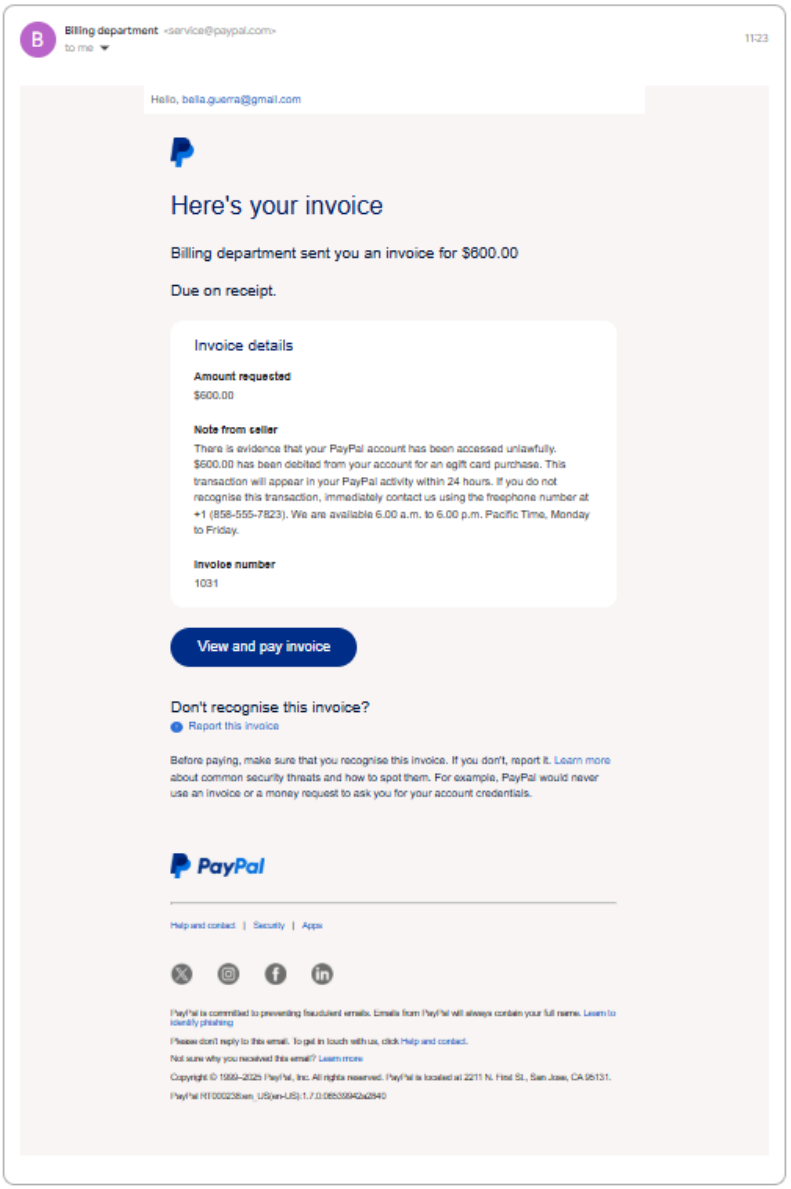
3. ¡Oh, no! ¿Cómo consiguieron tus credenciales de PayPal?

   PREGUNTA: Las estafas de tarjetas regalo son lo peor.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



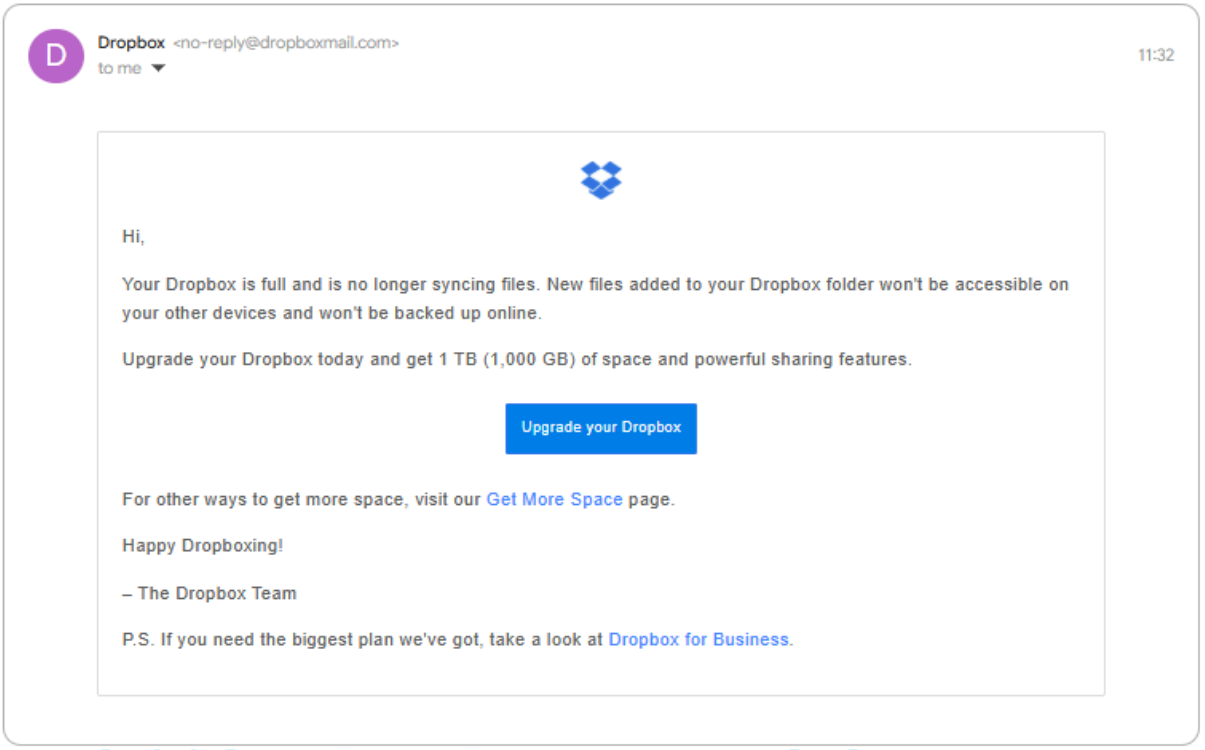
RESPUESTA: PHISHING, este mensaje en realidad es una “nota del vendedor”. Los estafadores crearon una falsa sensación de urgencia, una técnica común para engañar a los usuarios y hacer que actúen rápidamente. Estos estafadores esperan que llames al número que proporcionan, donde continuarán con la estafa. Puedes verificar los números de teléfono de las empresas legítimas a través de sus sitios web (por ejemplo, el sitio web de PayPal).

4. ¡Uh, oh! ¡Parece que tu almacén está lleno!

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

PREGUNTA: ¿Cuánto costaría mejorar el servicio?



RESPUESTA: LEGÍTIMO, esta es una comunicación legítima de Dropbox. El remitente es 'dropboxmail.com', lo cual es poco común pero auténtico, y el enlace es seguro (https) y dirige a 'dropbox.com'.

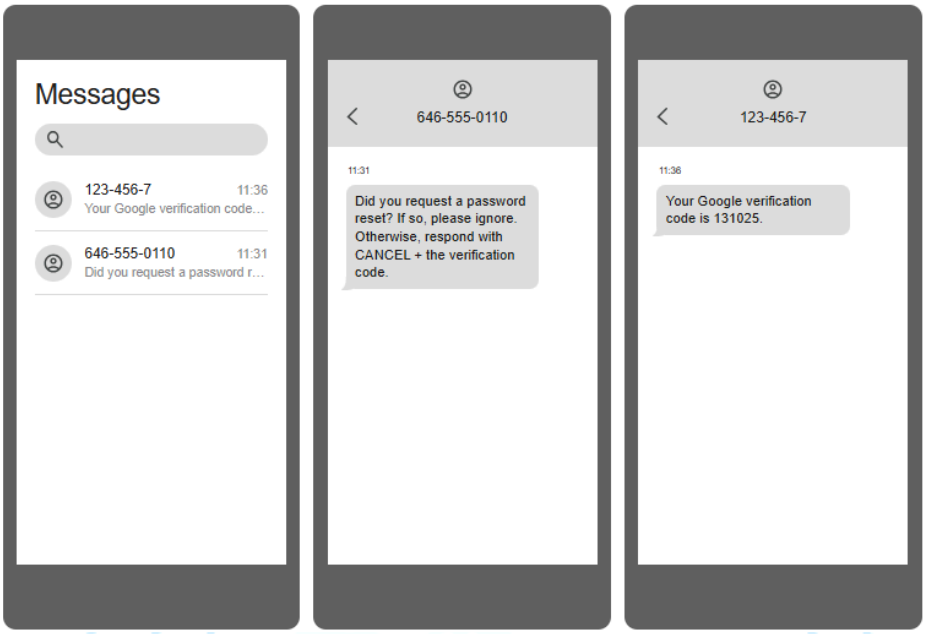
5. ¡Oh, los códigos!

PREGUNTA: Esto es raro, no recuerdas haber recibido un código vía SMS…

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: PHISHING, este estafador utiliza un lenguaje engañoso para crear una falsa sensación de urgencia y miedo, una táctica muy común. Los códigos de verificación en dos pasos por SMS son una medida de seguridad, pero solo deben compartirse durante un proceso de verificación en tiempo real que tú hayas iniciado.

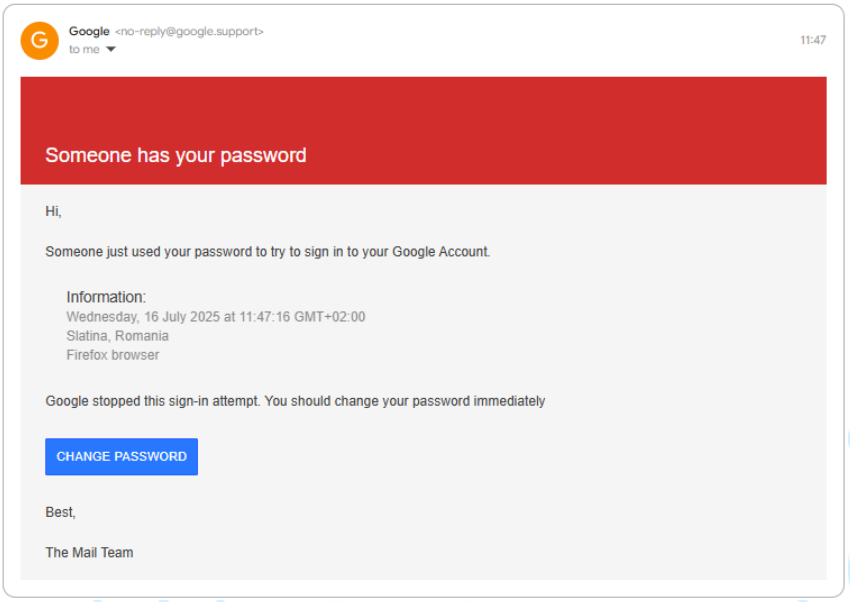
6. Alguien ha intentado acceder a tu cuenta

   PREGUNTA: Mira cuidadosamente antes de cambiar tu contraseña:

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: PHISHING, este correo es casi idéntico a un ataque que se utilizó con éxito para hackear los correos electrónicos de varios políticos. ¡Asegúrate siempre de revisar cuidadosamente las URL!

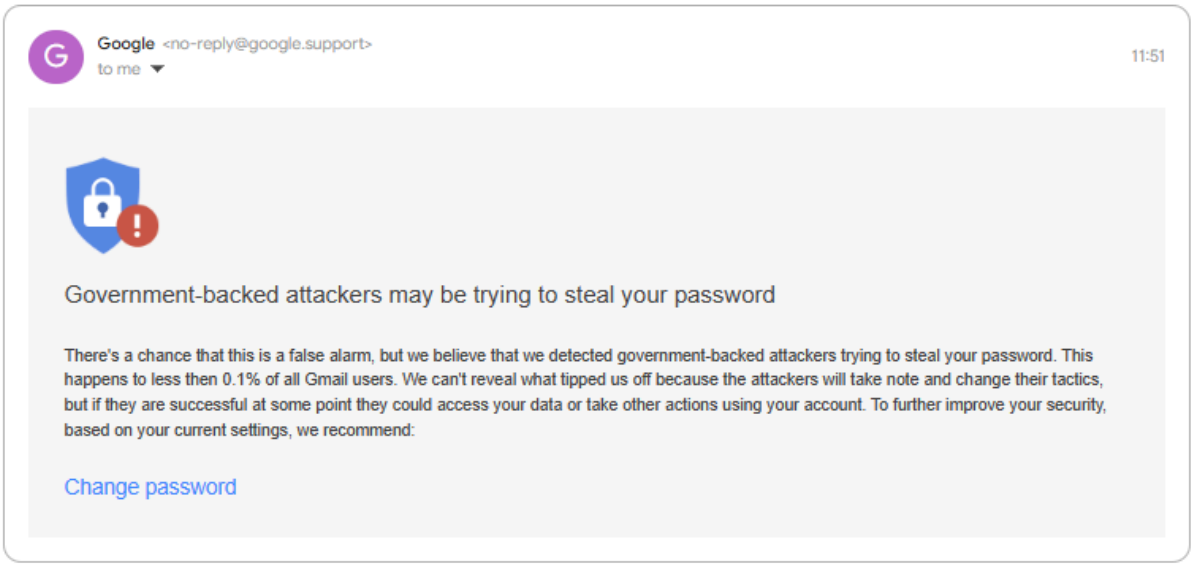
7. Tu cuenta está siendo atacada de nuevo.

   PREGUNTA: ¿O puede que no?

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

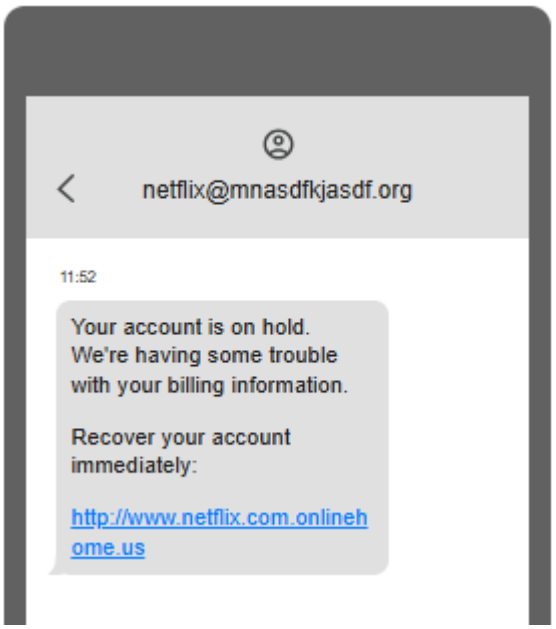
ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: PHISHING, los hackers intentaron usar Google para ocultar el enlace real, que en realidad proviene de tinyurl. Un correo similar a este se utilizó para atacar a centros de pensamiento y políticos.

8. ¡Netflix no!

   PREGUNTA: ¿Cómo vas a ver ahora tu show favorito?



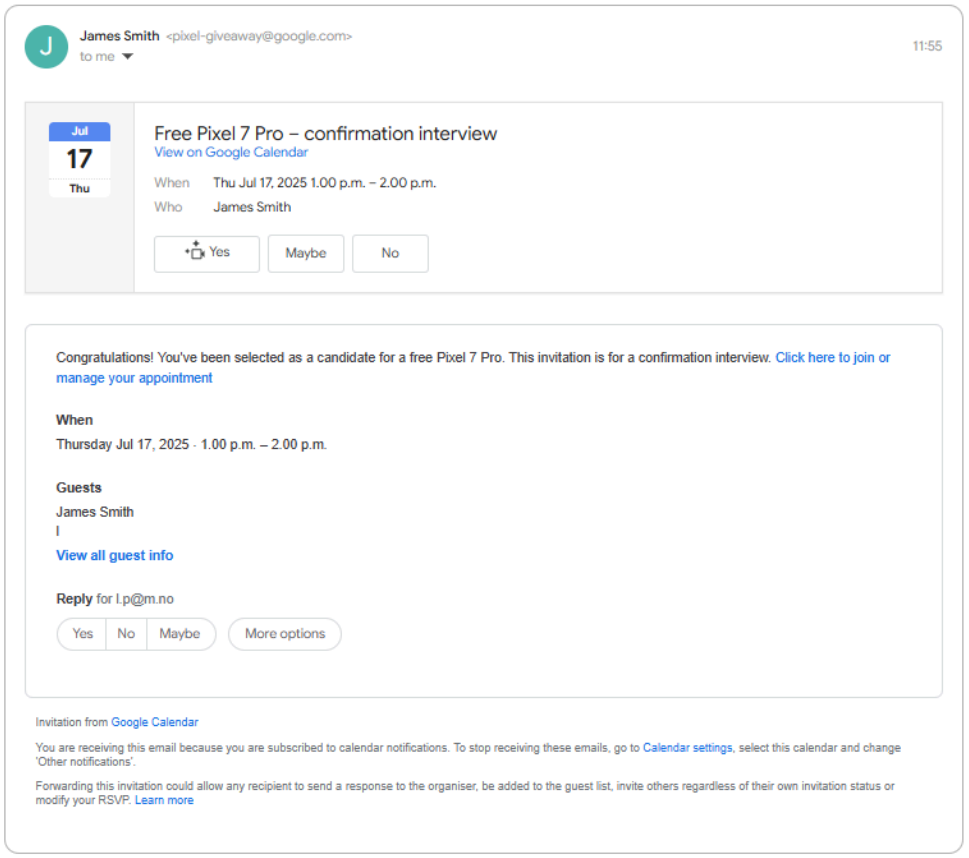
Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

RESPUESTA: PHISHING, debiste haber notado la URL engañosamente similar y que el SMS provenía de una dirección de correo electrónico, no de un número de teléfono. Si alguna vez tienes dudas sobre una notificación, no hagas clic en el enlace; visita el sitio de la manera habitual y contacta con ellos directamente.

9. ¿Un teléfono gratis?

   PREGUNTA: Bueno, hablar no es un problema, ¿verdad?



RESPUESTA: PHISHING, debiste haber notado la oferta sospechosa y el intento astuto de ocultar el correo electrónico real.

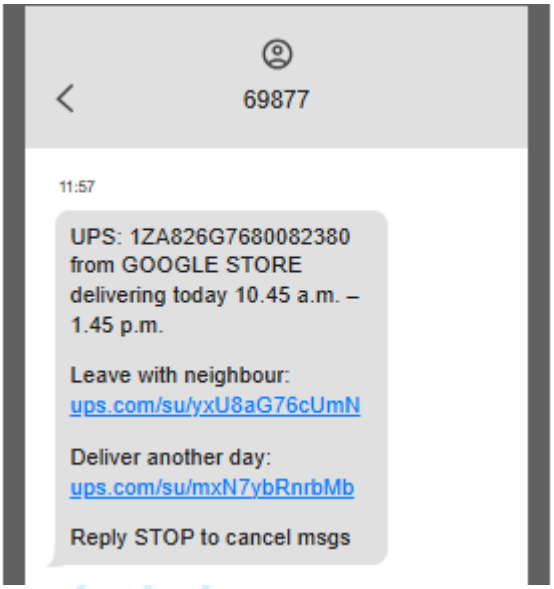
10. Espera, ¡No estoy en casa!

    PREGUNTA: Quizá deberías cambiar ese envío.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Sabes identificar cuándo te están estafando?	
Idioma	*25 idiomas diferentes*



RESPUESTA: LEGÍTIMO, estas URL son enlaces reales a ups.com, sin ninguno de los trucos que se usan para crear imitaciones con otras URL. Se recomienda verificar la existencia de un paquete en el sitio web oficial.

4. Más información

El puzzle está disponible en 25 idiomas. El creador es Jigsaw, una unidad interdisciplinar dentro de Google que construye tecnología para escalar la respuesta a determinador problemas. https://jigsaw.google.com/

Enlace al puzzle: https://phishingquiz.withgoogle.com/?hl=en

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.