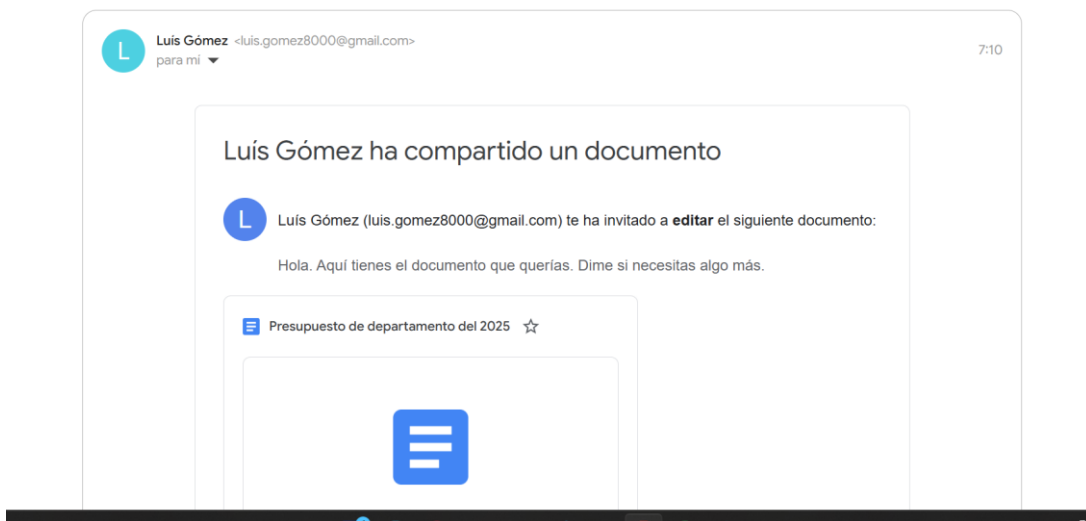


Laboratorio 11: Análisis de Ejemplos de Phishing



¿Puedes detectar cuándo te están

Primera pregunta:



¡Correcto! Este es un correo de phishing.

Parece que has detectado la URL engañosa. Ten cuidado con los hiperenlaces y los archivos adjuntos que abras en los correos electrónicos: es posible que te dirijan a sitios web fraudulentos en los que se te solicite información confidencial.

Explicación

Segunda pregunta:



Coca-Cola <email_Gep2pQ76g78@opmajvpqjcg.georgs-faescht.com>
para mí ▼

7:11

Coca-Cola

¡RESPONDE Y GANA!

— Una nueva —

**batidora y exprimidora
portátil**



¡Correcto! Esta estafa era una combinación de varias técnicas.

Tenías que detectar que los dominios no coinciden y que la oferta es realmente increíble.

Explicación



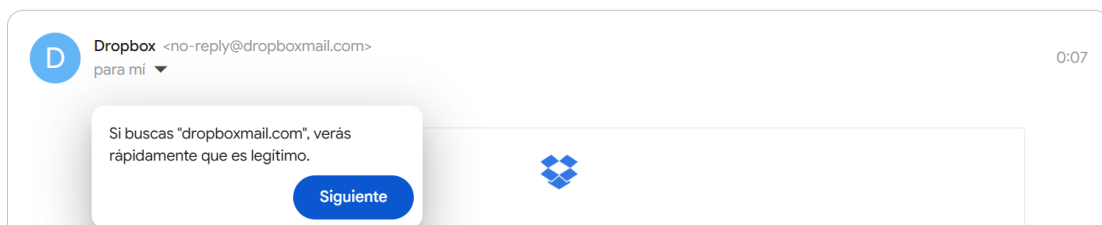
Tercera pregunta:

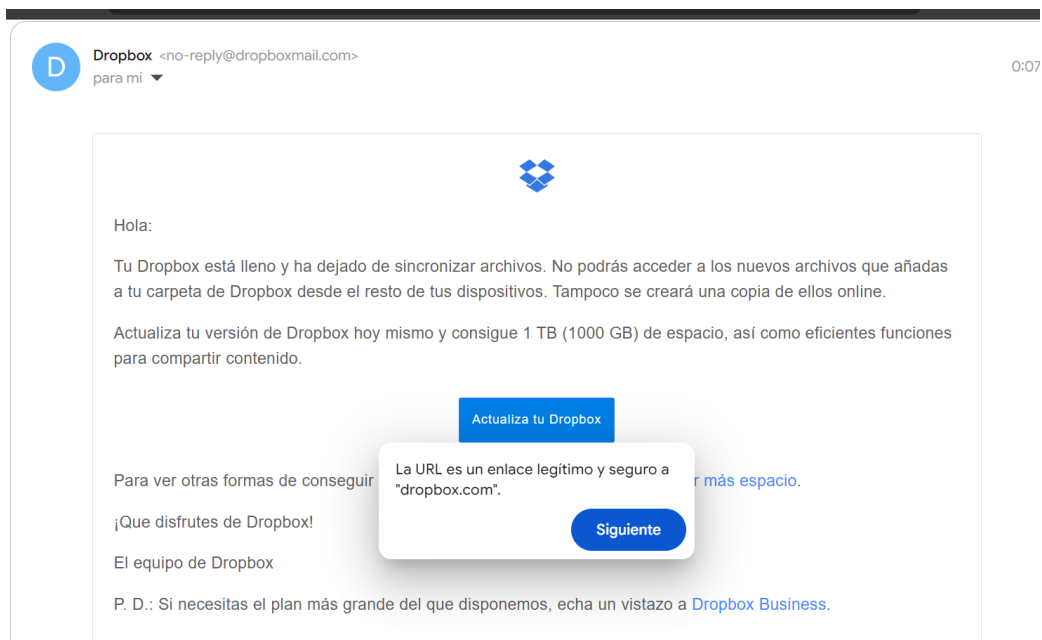
No solamente se nos muestra correos maliciosos sino que también nos enseñan cuando un correo es legítimo

¡Correcto! Es legítimo.

Este es un mensaje legítimo de Dropbox. El remitente es "dropboxmail.com", que es poco frecuente pero legítimo, y la URL es un enlace seguro (https) a "dropbox.com".

Explicación





Otra pregunta:





¡Te hemos elegido para que participes en nuestro programa de fidelización **GRATIS**! Solo tardarás un minuto en recibir este fantástico premio.

¡EMPIEZA HOY MISMO!

Si no quieres recibir este premio, puedes optar por no participar. Si lo deseas, puedes optar por recibirlo en tu correo electrónico o en tu teléfono móvil. Si lo deseas, puedes optar por recibirlo en tu correo electrónico o en tu teléfono móvil.

La URL está diseñada para ocultar una serie de redirecciones y evitar que el proveedor de alojamiento las detecte, ya que solo se activan con el texto después del símbolo "#". Normalmente, este es un código corto que se usa para enlazar a una ubicación específica de una página.

Siguiente

hot.net/public/users/integrators/d112425a2-57e5-445b-896d-425ed79fd2ca41308903/bsdfibigurdeghdohdodod4d4d5d5d1d1d1d1d_2.html