Aprendé a identificar un correo malicioso

VERACIDAD DEL REMITENTE 1

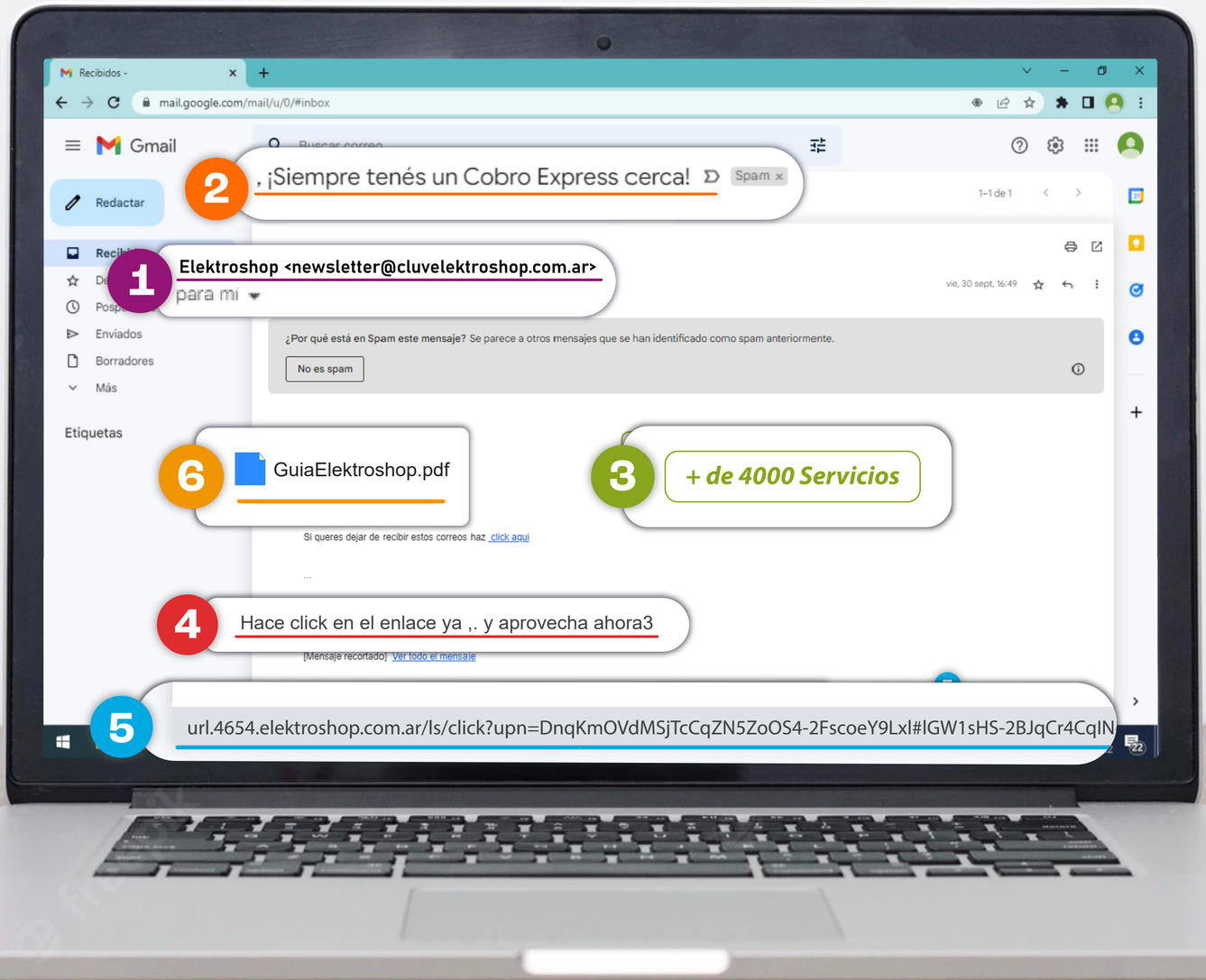
Si no esperabas un e-mail de esa persona o entidad, comprobá que la dirección del correo coincida con quien dice ser.

ASUNTO DEL MENSAJE 2

Si intenta captar tu atención a través de un título llamativo o alarmante, puede tratarse de un correo fraudulento: “Espacio de almacenamiento extra”, “Se ha detectado una compra con su tarjeta”, u otro.

¿QUÉ QUIEREN QUE HAGAS? 3

Si el mensaje intenta que bajes un adjunto, hagas clic en un enlace o entres a una página y dejes tus datos personales, es muy posible que se trate de un fraude.



MALA REDACCIÓN 4

Si parece una traducción automática o el texto contiene errores de ortografía o gramaticales, seguramente es una estafa.

ENLACES ILEGÍTIMOS 5

Si el mensaje cuenta con un link, no le hagas clic. Verificá su autencidad situando el puntero del mouse o tu dedo arriba. Si la URL que se muestra en la barra de estado que aparece abajo de la pantalla, empieza con **Https://**, es un link seguro. Si no, descartá el correo.

DOCUMENTOS ADJUNTOS 6

Si el correo tiene un archivo que, además, no esperabas, no lo abras porque puede tratarse de un malware. Siempre analizalo con un antivirus actualizado.

Ministerio de COORDINACIÓN

CÓRDOBA entre todos