

Cómo evitar fraudes en línea relacionados con el COVID-19



Tipos comunes de fraude



Falsos mensajes de organizaciones sanitarias

Los estafadores se hacen pasar por la Organización Mundial de la Salud, el Ministerio de Sanidad o el Centro Nacional de Epidemiología para ofrecer remedios, pruebas o información relativa al COVID-19.



Sitios web que venden productos fraudulentos

Algunos sitios anuncian desinfectante de manos, mascarillas y otros productos muy solicitados que nunca llegan al comprador.



Falsas fuentes gubernamentales

Ciertos estafadores aseguran proporcionar pagos e información en nombre del Gobierno.



Falsas solicitudes de donaciones benéficas

Revisa cuidadosamente y verifica las presuntas solicitudes de donativos para luchar contra el COVID-19 por parte de organizaciones caritativas, hospitales y el Sistema Nacional de Salud.



Ofertas financieras fraudulentas

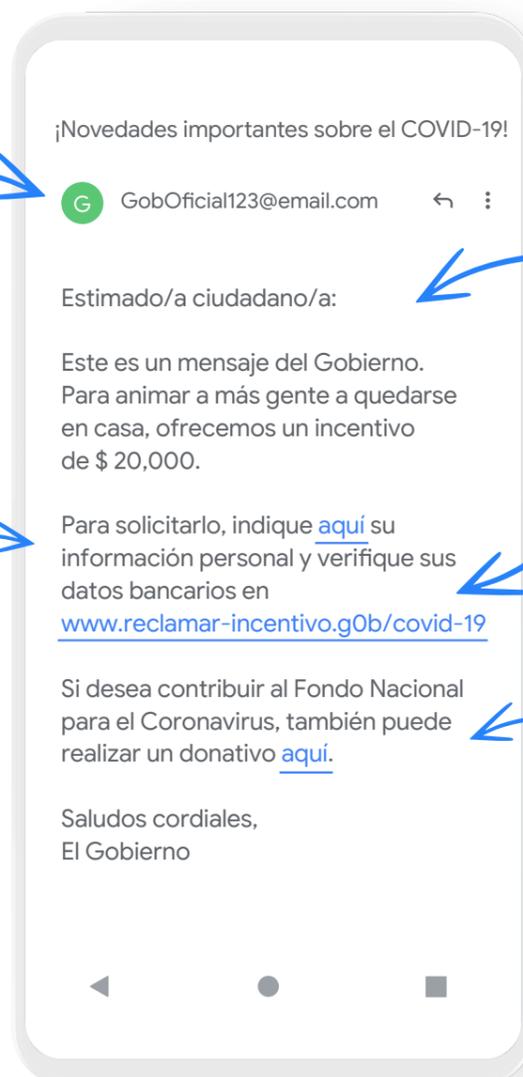
Los estafadores pueden hacerse pasar por bancos, inversionistas o cobradores de deudas con ofertas diseñadas para robar datos financieros.

Consejos para no ser víctima de fraudes comunes

Conocer los canales empleados por los estafadores: correos electrónicos, mensajes de texto, llamadas automatizadas y sitios web maliciosos.

No facilitar nunca información personal ni datos financieros a menos que sepamos perfectamente con quién estamos hablando.

Pegar fragmentos del mensaje sospechoso en un buscador para comprobar si ya se ha denunciado antes.



Consultar sitios web autorizados para conocer las últimas noticias relacionadas con el COVID-19.

Comprobar enlaces y direcciones de correo electrónico antes de hacer clic en ellos.

Donar directamente a través del sitio web de una organización benéfica en vez de hacer clic en un enlace recibido.

Añadir una capa extra de seguridad a las cuentas con la verificación en dos pasos o la autenticación de dos factores.



Repórtalo. Si se detecta algo sospechoso, repórtalo a través de la plataforma.