



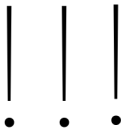
Safe Data
Safe Families

Cómo detectar una suplantación de identidad

La suplantación es un delito cibernético para obtener los datos de acceso o información financiera de posibles víctimas. Una persona puede aparentar ser representante de una organización legítima (banco, IRS, compañía telefónica) y contactar a las víctimas por teléfono, correo electrónico o mensaje de texto para solicitarles información confidencial de manera engañosa.



Cómo evitar ser víctima de una suplantación:



Los mensajes suelen intentar crear un efecto de urgencia (“¡responda en los próximos 10 minutos!”) para forzarle a actuar sin pensar.



Las ofertas generalmente son "demasiado buenas para ser ciertas". Fíese de su instinto.



No descargue documentos anexos de remitentes desconocidos.



No pulse en un enlace que vea en un correo electrónico o mensaje de texto. En su computadora, coloque su ratón sobre el enlace para ver el URL, o entre el nombre del sitio de internet (p.ej., bankofamerica.com).



En caso de duda, llame a la organización directamente y pregunte si el mensaje es legítimo.

Para más información, visite: <https://safedata.umd.edu>