

¿Oferta profesional, contacto real o estafa?

Recomendaciones prácticas para prevenir estafas y fraudes digitales dirigidos a traductores

| Por la traductora pública Lorena Roqué

Las estafas dirigidas a traductores e intérpretes son cada vez más frecuentes y pueden llegar por correo electrónico, WhatsApp, Telegram, redes sociales u otras plataformas. Muchas comienzan con una aparente oferta de trabajo, como una comunicación para pedirte información, solicitudes de descarga de archivos, supuestos pagos, verificaciones de datos o comunicaciones que parecen provenir de empresas e instituciones conocidas.

Ante un contacto inesperado, la primera recomendación es sencilla: no actuar de inmediato. Verificar antes de responder, descargar archivos, proporcionar información o realizar cualquier operación.

Antes de aceptar una oferta de trabajo

Se recomienda identificar al potencial cliente y corroborar su identidad antes de aceptar un nuevo proyecto.

Una oferta legítima debería permitir establecer claramente quién te contrata, cuál es el trabajo que te ofrecen, qué archivos hay que traducir o cuáles son de referencia, la tarifa estipulada, la fecha de entrega y las condiciones de pago. En trabajos profesionales también se involucra una orden de compra (PO) o una confirmación escrita que contenga estos datos.

Si se trata de una empresa, debemos verificar el nombre, domicilio, teléfono, sitio web y la identidad de la persona que te contactó. Debemos prestar especial atención al remitente. Que un correo tenga el nombre y el logotipo de una empresa conocida no significa que realmente provenga de ella. Siempre hay que revisar la dirección completa del remitente. Es importante ver si el dominio del correo electrónico coincide con el sitio oficial de la organización «@nombredelaorganización», que no sea un correo gratuito como «@gmail» o algún otro dominio desconocido. Las empresas suelen tener su propio dominio. Según el programa de correo que utilices, podés verla posicionándote sobre el nombre del remitente o accediendo a los datos del mensaje.

Además, hay que prestar atención a pequeñas diferencias. Por ejemplo, alguien puede utilizar un dominio casi idéntico al verdadero, pero cambiar, eliminar o agregar apenas una letra.

Para verificar la autenticidad de la oferta, no utilices los datos de contacto que aparecen en el propio mensaje. Buscá el sitio oficial de la empresa o institución y comunicate a través del teléfono o correo oficial para comprobar que la persona que envió el mensaje efectivamente trabaje allí.

Si el contacto llega por WhatsApp o Telegram

Un número desconocido o extranjero puede ser una señal de alerta, aunque por sí solo no demuestra que exista una estafa. En el caso de contactos que dicen provenir de la Argentina, verificá especialmente el +54... y que no provengan desde números internacionales inesperados.

Si alguien afirma representar a una empresa, agencia, banco, institución o colega, verificá su identidad por una vía independiente antes de continuar la conversación.

No envíes fotografías de documentos, DNI, pasaporte, credenciales, datos bancarios, contraseñas, códigos de verificación ni otra información personal o profesional sensible.

Nunca pagues para trabajar

Esta es una de las señales más importantes. Un trabajo no debería requerir que le pagues al supuesto cliente para poder trabajar.

Estas estafas se denominan *pay-to-work*. Después de una aparente selección profesional, el





supuesto empleador exige realizar un depósito, comprar determinado *software*, pagar una certificación, una verificación de antecedentes u otro gasto como condición para comenzar a trabajar. Si una supuesta oferta laboral termina con un pedido de dinero, frená y verificá antes de realizar cualquier pago.

Cuidado con los archivos y enlaces

No abras automáticamente archivos adjuntos ni ingreses en enlaces enviados por desconocidos.

Una oferta que llega acompañada inmediatamente por archivos para traducir, incluso antes de acordar condiciones, puede ser una señal de alerta.

También existen ataques de *phishing* que imitan visualmente sitios legítimos y solicitan ingresar datos personales o credenciales. Algunos enlaces pueden conducir, además, a sitios maliciosos.

Ante cualquier duda, no descargues, no hagas clic y no ingreses información hasta comprobar el origen.



Para resumir y agendar

Las siguientes modalidades son las dirigidas específicamente a profesionales independientes: falsas ofertas de traducción destinadas a obtener un trabajo que nunca será pagado, suplantación de agencias o clientes reales, solicitudes de dinero para acceder a un supuesto empleo, pagos por un importe superior al acordado seguidos de un pedido para devolver la diferencia, robo de CV y utilización de las credenciales profesionales de un traductor, y mensajes de *phishing* destinados a obtener información personal o financiera.■

Lecturas recomendadas para profundizar

https://www.argentina.gob.ar/seguridad/ciberdelito/recomendaciones-para-evitar-estafas-en-internet?utm_source=chatgpt.com

https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams

https://proz.papyrs.com/@knowledgebase/Risk-management#Risk-management

https://proz.papyrs.com/@knowledgebase/Scams

Señales de alerta

Desconfiá especialmente cuando se combinen varias de estas situaciones:

- **Te presionan para responder o actuar inmediatamente.**
- **La oferta parece excesivamente conveniente.**
- **Te solicitan realizar un pago o transferencia.**
- **El remitente dice representar a una empresa, pero escribe desde un dominio diferente o gratuito.**
- **La empresa o persona prácticamente no tiene presencia comprobable en internet.**
- **Las respuestas parecen automáticas o no responden concretamente tus preguntas.**
- **No existe orden de compra, contrato ni condiciones claras.**
- **Recibís archivos inesperados antes de haber aceptado el trabajo.**
- **Te solicitan información personal, bancaria, documentación o códigos de seguridad.**
- **Recibís un pago superior al acordado y te solicitan devolver la diferencia.**



Una regla sencilla: RESPIRÁ – VERIFICÁ –ACTUÁ

- **No respondas apresuradamente.**
- **No descargues archivos sospechosos.**
- **No abras enlaces desconocidos.**
- **No proporciones información personal.**
- **No realices pagos para acceder a un trabajo.**
- **Verificá siempre al remitente por una vía independiente.**

Si algo genera dudas, suspendé la comunicación y verificá primero la identidad de la persona, empresa o institución que supuestamente se está contactando con vos.

La prevención empieza por no desesperarse y tomarse unos minutos antes de actuar.