Cuentas confiables (enviar dinero)

Para proteger a los usuarios y evitar que envíen dinero a estafadores, deben indicar que los números de las cuentas bancarias de sus proveedores son confiables antes de poder utilizarlos para realizar un pago.

Abra la cuenta bancaria del proveedor correspondiente y haga clic sobre el interruptor junto al texto **Enviar dinero**.

> **Nota**
>
> De forma predeterminada, al inicio todas las cuentas se establecen como no confiable.

Ataques de phishing

Un **ataque de phishing** es una estafa en línea que se realiza mediante el envío de comunicaciones fraudulentas y está diseñada para engañar a individuos o empresas con la finalidad de que proporcionen información confidencial o envíen dinero. Los estafadores se hacen pasar por empresas legítimas y pueden utilizar alguna información parcial cierta para que sus solicitudes se vuelvan más creíbles.

Hay varios tipos de ataques de phishing, entre los que se encuentra la **estafa de facturas**. En este caso, el estafador finge ser un proveedor verdadero que le da seguimiento a las facturas que no se han pagado o envía una nueva factura, pero con información de pago diferente a la habitual y datos de contacto falsos.

Para protegerse de estos tipos de ataques de phishing, preste mucha atención si es que recibe facturas o solicitudes de pago inesperadas.

> **Importante**
>
> **Le recomendamos contactar por teléfono al proveedor** en caso de que tenga alguna duda. Asegúrese de llamar al número telefónico oficial que usted conozca o haya investigado por su cuenta, ya que las URL, direcciones de correo electrónico y números de teléfono proporcionados en el mensaje que recibió podrían ser falsos.

Elementos a verificar

Hay varios elementos que puede comprobar al recibir una solicitud de pago a una nueva cuenta:

Estilo de la comunicación

Por lo general, los correos electrónicos o facturas que no son reales usan un estilo de comunicación diferente, como una **redacción distinta** y pueden incluir **errores ortográficos y gramaticales**. Examine y **compare** con mensajes anteriores que sabe que son auténticos (por ejemplo, instrucciones de pago, idioma, logotipo de la empresa, etc.).

Urgencia

Es común que en la estafa de facturas se utilice un **lenguaje urgente o amenazante** y que cambien la **fecha límite de pago**. Verifique que en verdad haya recibido un recordatorio sobre un pago atrasado con anterioridad.

Tipo de cuenta

Es poco probable que una empresa sustituya una cuenta bancaria por un **servicio de transferencia de dinero**.

Nombres de dominio en correos electrónicos y enlaces

Verifique cuidadosamente el **dominio de la dirección de correo electrónico** (ejemplo@dominio.com). Sin embargo, tenga cuidado, los estafadores pueden hacer que sus direcciones de correo electrónico parezcan reales. También existe la posibilidad de que hayan accedido de forma ilegal a las direcciones de correo electrónico que pertenecen a los empleados de sus proveedores o incluso de alguien dentro de su propia empresa.

Pase el cursor por encima de los enlaces en su correo electrónico y verifique que las URL a las que redirigen sean auténticas. Por lo general, su navegador de internet muestra la dirección del enlace en la parte inferior izquierda de la ventana.