30 Consejos de seguridad

Evita el phishing y reduce el fraude

aldeamo | Conectamos empresas con sus audiencias

La seguridad en línea es esencial en la era digital actual, especialmente todo lo relacionado con la **protección de nuestra información personal y financiera**. Una de las mayores amenazas en línea es el phishing, una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y robar información confidencial.

Para evitar ser víctima de esta amenaza, es importante tomar medidas preventivas y estar siempre alerta ante posibles ataques. Eres importante para nosotros, por eso diseñamos productos que pueden ayudarte a prevenir el phishing y garantizar la seguridad en línea de tu compañía y así mismo de tus clientes.

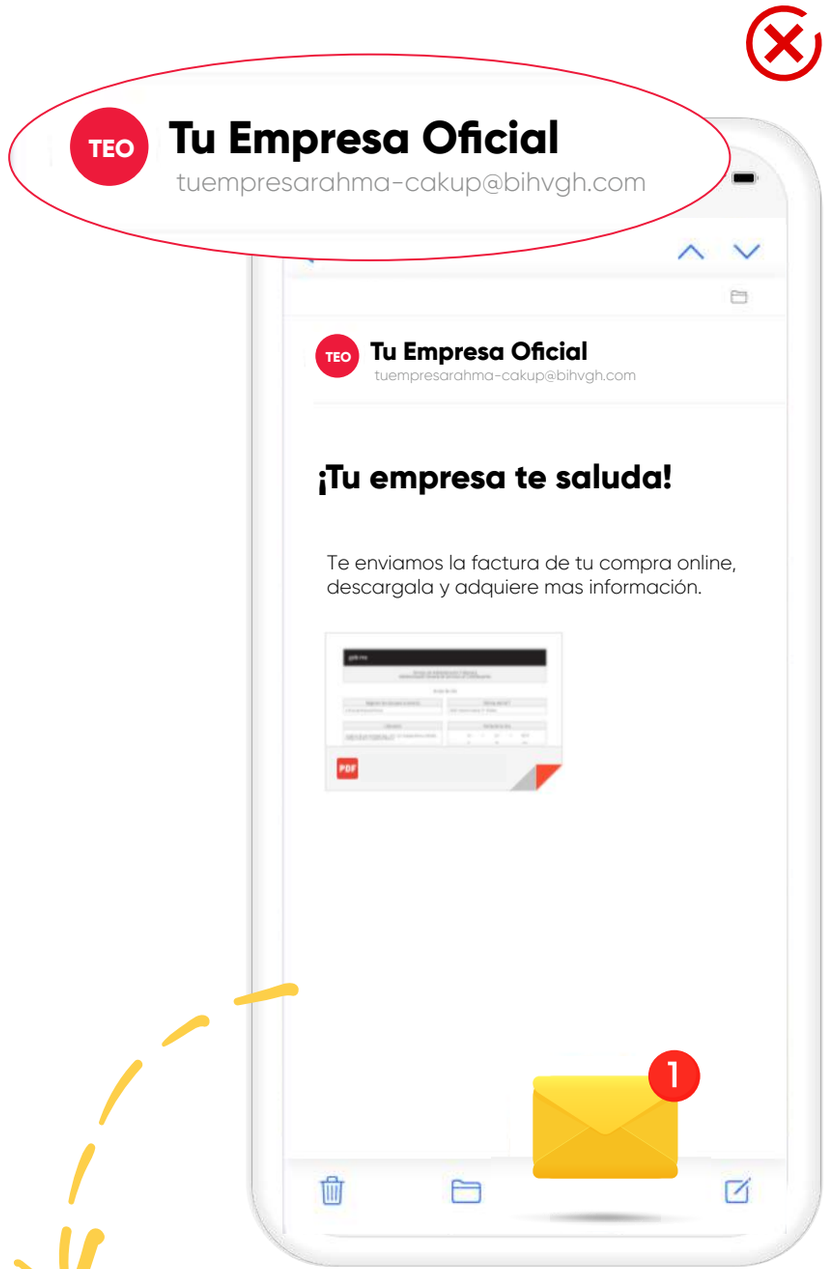
Esta guía proporcionará información detallada sobre el **phishing** y ofrecerá soluciones prácticas para evitarlo, incluyendo las herramientas de seguridad que ofrece Aldeamo para **proteger a los usuarios** de posibles ataques en línea.

Recomendaciones

prácticas

Consejos para:

Correos electrónicos



El **correo electrónico** no existe y no pasó por lo menos 1 de las validaciones realizadas.

Correos electrónicos:

1. No hagas clic en enlaces o descargues archivos adjuntos de correos electrónicos sospechosos o desconocidos.

2. Verifica cuidadosamente el remitente y la dirección de correo electrónico del remitente antes de responder o hacer clic en un enlace.

3. No reveles información personal, financiera o de inicio de sesión a través de correos electrónicos.

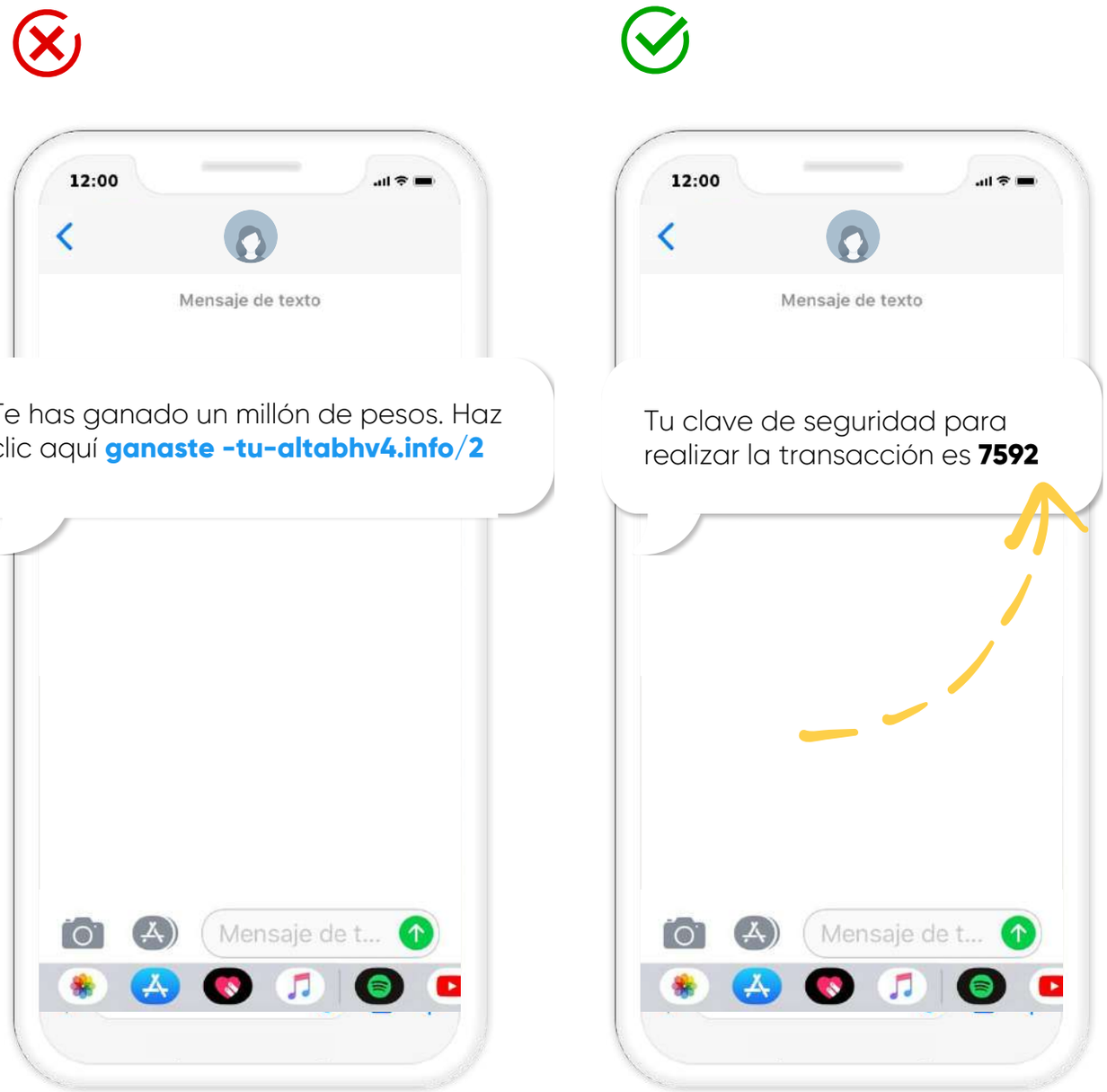
4. Utiliza una herramienta de detección de correo electrónico malintencionado para detectar correos electrónicos sospechosos.

5. Asegúrate de que la conexión sea segura antes de ingresar información confidencial en un sitio web enlazado a través de un correo electrónico.

6. ¿Sabías que hay validadores de correo que te permiten identificar si una dirección no es segura?

Consejos para:

Mensajes de texto



Mensajes de Texto:

7 No respondas a mensajes de texto sospechosos o no solicitados.

8 No utilices una conexión Wi-Fi pública para abrir mensajes de texto confidenciales.

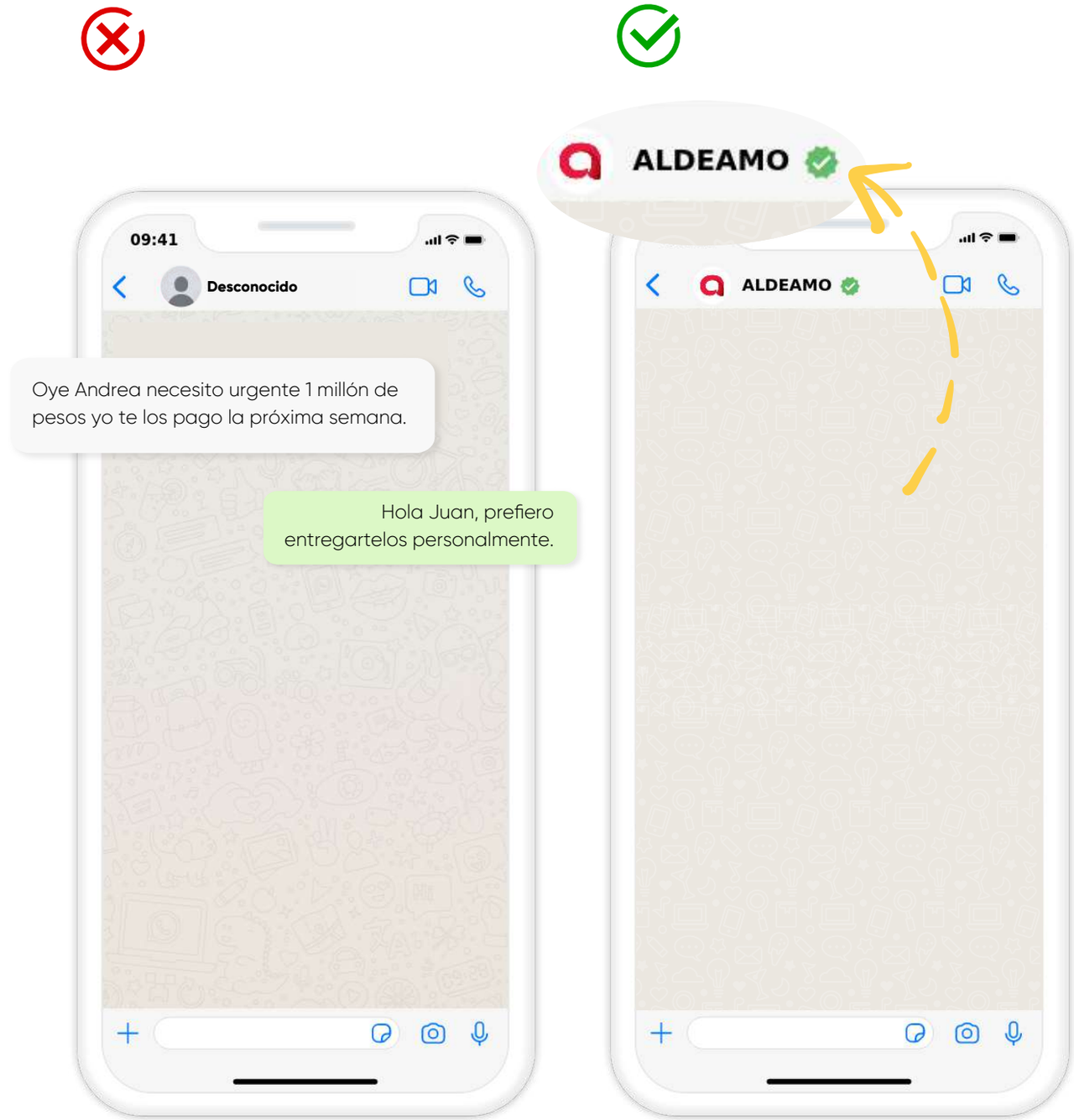
9 Mantente siempre alerta y piensa dos veces antes de compartir información confidencial a través de mensajes de texto SMS.

10 No respondas a solicitudes de dinero o transferencias en SMS sin verificar la autenticidad de la cuenta.

11 ¿Sabías que entidades como los bancos se apoyan en claves de un solo uso para garantizar la seguridad en las transacciones?

Consejos para:

Mensajes de WhatsApp



Mensajes de WhatsApp:

12 Verifica siempre la identidad del remitente antes de compartir cualquier información.

13 No compartas información personal, como contraseñas o números de tarjeta de crédito, a través de WhatsApp.

14 Configura la privacidad de su cuenta para que solo las personas en su lista de contactos puedan ver su foto de perfil y estado.

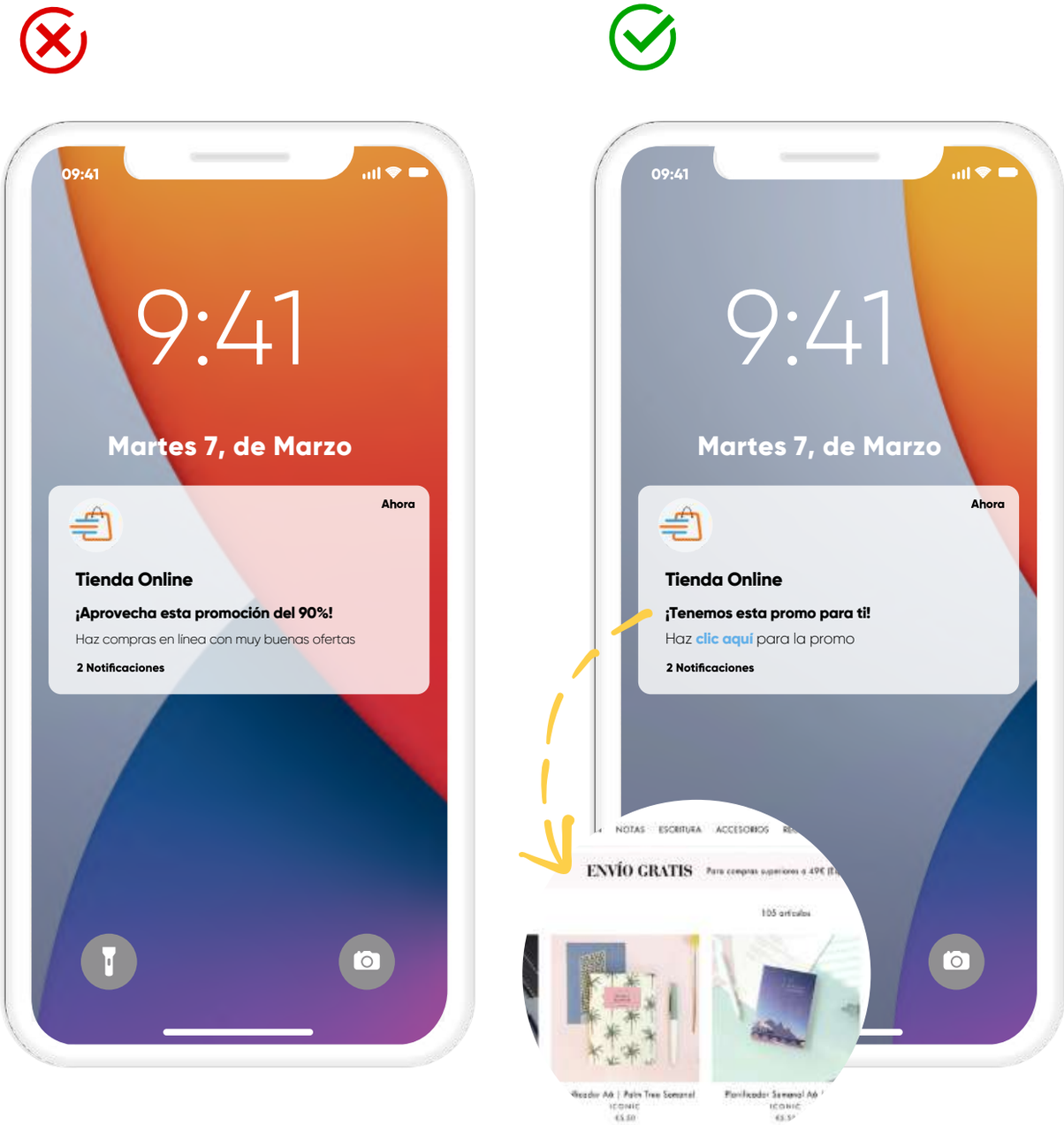
15 Mantén actualizada la versión de WhatsApp y siempre descarga actualizaciones desde fuentes oficiales.

16 Si recibes un mensaje sospechoso de un amigo o familiar en WhatsApp, verifica su autenticidad antes de responder.

17 ¿Sabías que Meta certifica las cuentas empresariales para tu seguridad? Reconócelas por el green label.

Consejos para:

Notificaciones Push



Notificaciones Push:

18 No ingreses información personal en sitios web desconocidos o sospechosos en respuesta a notificaciones push.

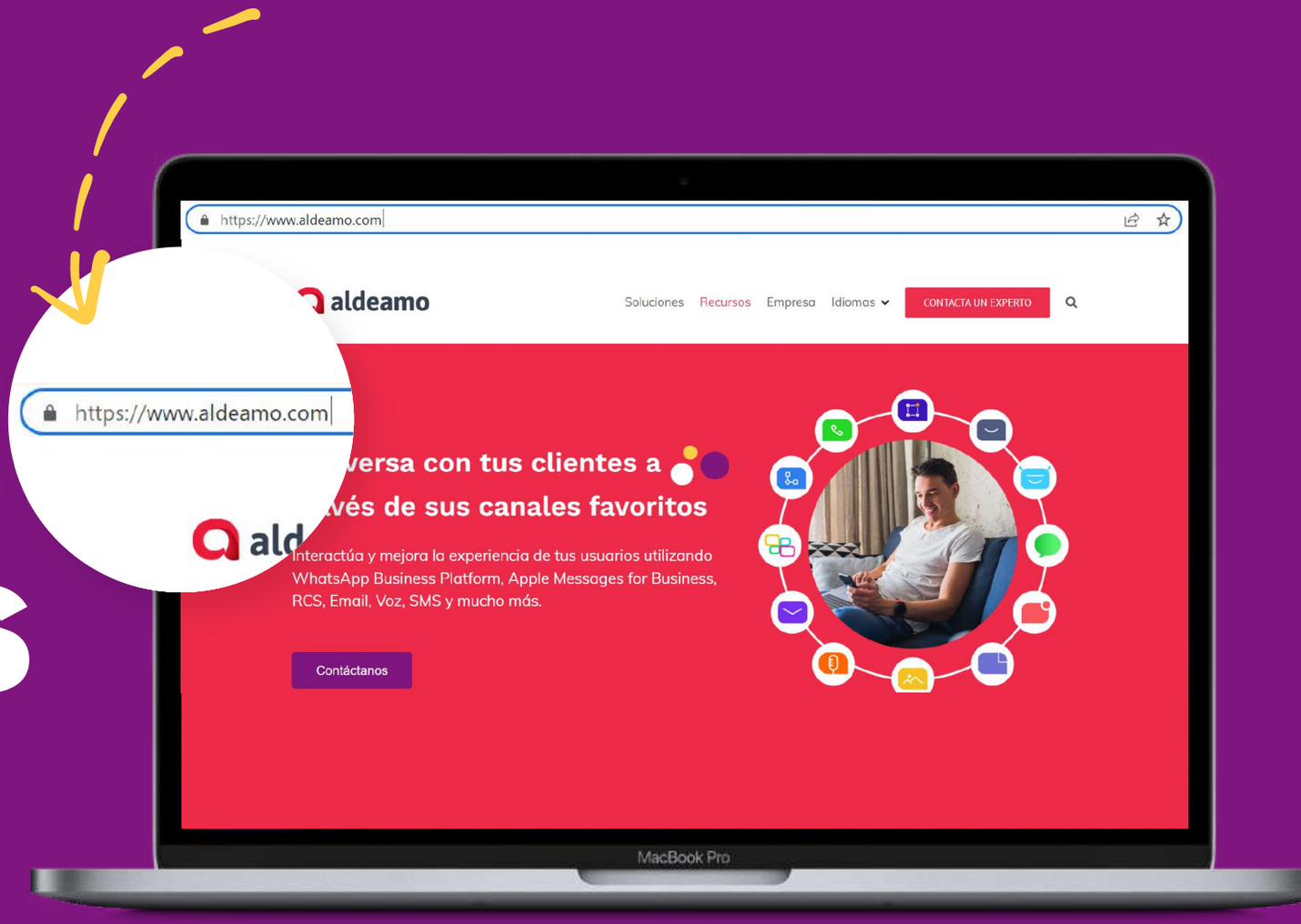
19 No descargues archivos desconocidos o sospechosos en respuesta a notificaciones push.

20 Mantente atento a los indicadores de fraude, como faltas de ortografía y gramática en las notificaciones push.

21 No proporciones información financiera en respuesta a notificaciones push que informa que has ganado un premio.

22 Si recibes una oferta especial, verifica el dominio al que te redirigen.

Consejos generales



Consejos generales

23 Actualiza tu software y aplicaciones de manera regular para reducir las vulnerabilidades de seguridad.

24 Utiliza contraseñas seguras y diferentes para cada cuenta.

25 No compartas contraseñas con otras personas.

26 Verifica la dirección URL antes de ingresar información confidencial en un sitio web.

27 No utilices una conexión Wi-Fi pública cuando hagas consultas financieras o transacciones en línea.

28 Los documentos con claves personalizadas son una herramienta muy importante y han hecho un gran aporte a la seguridad de la información de millones de clientes y empresas.

Los canales digitales son de gran ayuda para la comunicación empresarial, saber usarlos y tener presente este tipo de recomendaciones son claves para que la interacción y la información de tus clientes esté protegida.

Si quieres obtener más información sobre

nuestras soluciones

de seguridad en línea, no dudes en ponerte en contacto con nosotros.

Ideas de valor

Si crees que esta información es valiosa y le puede servir a tus clientes, arma una campaña similar. Puedes hacerlo con un correo masivo o una llamada pregrabada de voz, o deja que tu creatividad se apoye en cualquiera de nuestros canales. ¿Y sabes qué es lo mejor?, ¡te regalamos toda la información de esta guía para que la uses como quieras! Cópiala, reenvíala o inspírate.

Si has tenido una experiencia positiva con esta guía o con nuestros servicios, nos encantaría recibir tu reseña en Google o un comentario en nuestras redes sociales.

¡Gracias por elegir Aldeamo como tu aliado de seguridad en línea!