

What to Know About Phishing Emails Sent From Kareo

To enforce our security measures at Kareo, you will only receive corporate emails from @kareo.com and we would never ask for your password. However, some people may receive fake or suspicious emails that look like they were sent by Kareo. These emails might include malicious attachments or links to spam or phishing websites. Because these phishing emails can create significant problems for Kareo if not stopped, we have prepared the following FAQs:

What is phishing?

Phishing scammers send fraudulent messages to a large group of people online, hoping to trick them into revealing private information, like a password. An email or website may be disguised to appear legitimate.

It can be difficult to recognize a spoofed email as they may look very convincing or appear to come from a Kareo email address. Contact Kareo Security if you are not sure if you are receiving a phishing email.

What should you do if you receive a phishing email?

Immediately delete the email from your inbox and don't download any attachments that are included. For additional information on account security, visit our Help Center for tips to protect your account. (create page)

Why am I getting these phishing emails?

The number of these type of emails has certainly increased in recent years. To learn the various ways spammers may find your email address, visit FTC's Help Page here. <https://www.consumer.ftc.gov/>.

For more information about Kareo's policies on information collection, disclosure and sharing, please visit our privacy page at <https://www.kareo.com/privacy-policy>.

Questions?

If you have questions or suggestions you can contact us at:

Kareo Security Administrator

1111 Bayside Drive Suite 150

Corona Del Mar, CA 92625

security@kareo.com

To report a security violation, please call us at 888-77-KAREO (888-775-2736).

Last Updated: This policy was last updated on July 10, 2020