

12th September 2019

IMPORTANT! Warning about spam mails using the INGUN name

Once again, there is currently an increase in spam mails in circulation, which are intended to invite recipients to click on links or instruct them to transfer invoice amounts to a third-party account by means of a highly personalised layout.

At first glance, these e-mails seem to originate from known contacts such as INGUN employees by using the e-mail addresses of such contacts as the display name in the sender. Many e-mail programs, at least in the default setting, only show the recipient the display name and hide the actual sender address. Upon closer inspection, however, it can be seen that the spam mails in question usually come from external, unknown senders.

The raw view of the e-mail (visible under menu items that are more or less hidden) provides exact information about where the e-mail was actually sent from. Usually these are external, unknown servers, and not from the INGUN domain.

We advise against following the requests these emails contain! Under no circumstances should you divulge personal data. In addition, do not execute payment orders based on an e-mail only; ensure the authenticity of the order in a telephone or personal conversation with the person requesting payment.

Thank you for your attention on this matter.

INGUN Prüfmittelbau GmbH