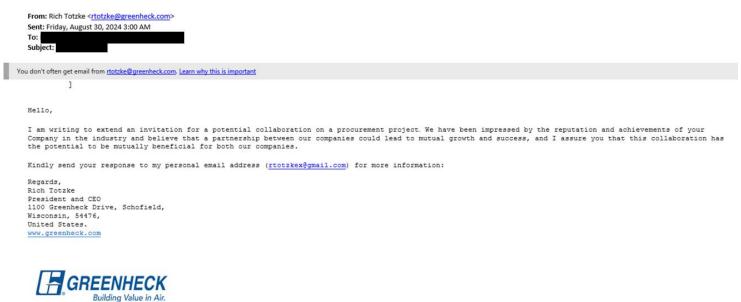




AUGUST 30, 2024

- TO: Greenheck Representatives
- FROM: Matt Spink, Chief Sales Officer
- SUBJECT: Email Scam Alert





You will note that the email address in the above message is from rtotzke@greenheck.com and NOT rich.totzke@greenheck.com which is Rich's correct email address.

The reasons for email spoofing or using a close representation of an email address and signature, typically taken from online searches or social media, are quite straightforward. Usually, the criminal has something malicious in mind, like stealing the private data of a company. Here are the most common reasons behind this malicious activity:

• **Phishing.** Almost universally, email spoofing is a gateway for phishing. Pretending to be someone the recipient knows is a tactic to get the person to click on malicious links or provide sensitive information.



• **Identity theft.** Pretending to be someone else can help a criminal gather more data on the victim (e.g., by asking for confidential information from financial or medical institutions).

• Avoiding spam filters. Frequent switching between email addresses can help spammers avoid being blacklisted.

• Anonymity. Sometimes, a fake email address is used to simply hide the sender's true identity.

Please be cautious of the emails you open and reply to. If you have questions regarding this subject, contact the Greenheck IT Helpdesk at <u>helpdesk@greenheck.com</u>