BULLETIN

AUGUST 30, 2024

TO: Greenheck Representatives

FROM: Matt Spink, Chief Sales Officer

SUBJECT: Email Scam Alert

We have received word of a scam by someone purporting to be Rich Totzke. The request shown below was not sent by anyone at Greenheck. Please do not reply to an email from rtotzke@greenheck.com soliciting a procurement proposal. The email also notes a personal email of rtotzkex@gmail.com for reply in the email.

From: Rich Totzke <rtotzke@greenheck.com>
Sent: Friday, August 30, 2024 3:00 AM
To: [redacted]
Subject: [redacted]

You don't often get email from rtotzke@greenheck.com. Learn why this is important

]

Hello,

I am writing to extend an invitation for a potential collaboration on a procurement project. We have been impressed by the reputation and achievements of your Company in the industry and believe that a partnership between our companies could lead to mutual growth and success, and I assure you that this collaboration has the potential to be mutually beneficial for both our companies.

Kindly send your response to my personal email address (rtotzkex@gmail.com) for more information:

Regards,
Rich Totzke
President and CEO
1100 Greenheck Drive, Schofield,
Wisconsin, 54476,
United States.
www.greenheck.com

GREENHECK
Building Value in Air.

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.

GREENHECK

BULLETIN

- **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 helpdesk@greenheck.com