GROWERTALKS

GT in Brief

5/1/2022

Watch for Bank Scams Via Email!

Chris Beytes

It has come to our attention that several companies in our industry have fallen victim to so-called email spoofing. Whether or not this has to do with certain geopolitical events taking place abroad is anyone's guess. Certainly, spring is our busiest time, and scam artists may know you and your staff will be harried and frantic and won't take the time to cautiously review the emails you receive. But what could be a worse time for a malicious computer attack than the height of spring?

Here's how this particular scam works:

You receive a legit-looking email from a recognized industry supplier, informing you that their bank account information has recently changed, and that any future ACH payments or wires should be made with this new bank information.

Except … the supplier's bank information HASN'T changed. Instead, the bank information is that of the spoofer, who was posing as the supplier. Unfortunately, by the time the payer (and the unknowing supplier) find out, the money transfer has happened too long ago to get the money back or the criminal has already closed the bank account.

What should you do when you or someone in your company receives such an email? First of all, be suspicious of any email asking for financial or personal information like this! Few if any companies would tell you about bank account changes via email; they would use old-fashioned snail mail instead, with official letterhead, company envelopes and a postmark from their city.

If you do receive an email like this, and it looks legit but you aren't sure, pick up the phone and call your supplier to ask if the banking change is real. And whatever you do, DO NOT use the phone number in the email because that may be fake as well. Instead, go to the supplier's website or your own address book and call the number you find there.

While watching out for this specific scam, beware that regular ransomware attacks have been on the rise, too. In these cases, the bad guys lock your computer system and threaten to destroy all your files unless you pay a ransom—again, never a good thing, but especially bad in the middle of spring.

Computer threats like these are why you need to train your team to recognize spoofing and phishing schemes and remind them to be extra diligent. Plus, you need hack-proof backups! If you don't know where to get such training and systems, start with your IT/computer supplier. In the meantime, you can find some basic info from the Cybersecurity Awareness Program at Texas Tech University at ttu.edu/cybersecurity/lubbock. **GT**