

Subject: re: Email Spoofing REVISITED

From: info@nonprofitdynamics.com

Attention: Website Administrators!

"**Email spoofing**" continues to be an issue for all your members.

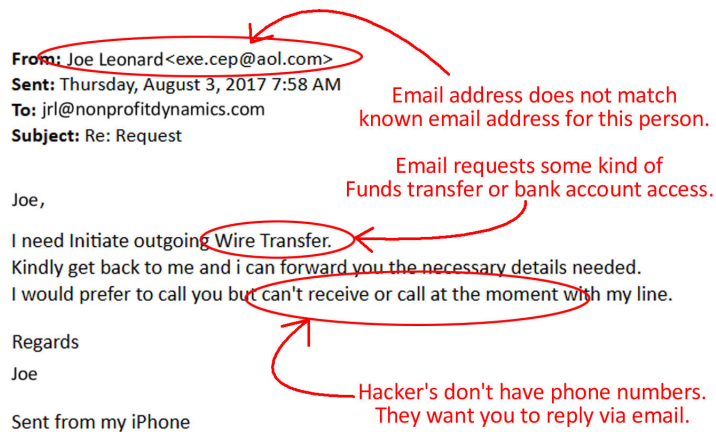
But there is something you can do about it.

You should have your Newsletter Editor include this information in your NEXT NEWSLETTER so that all your members are aware of this issue.

"Email Spoofing" is a form of hacking where the email "header code" is manipulated to make it look like the email originated from a known sender.

This manipulation makes it more likely that you, the recipient, will reply to a request for bank account information, a wire transfer, or other funds transfer.

Here is an example of what a "spoofing" email might look like:



The image shows an email header and body with several red annotations and circles highlighting suspicious elements:

- From:** Joe Leonard <exe.cep@aol.com> (Circled in red, with an arrow pointing to the text "Email address does not match known email address for this person.")
- Sent:** Thursday, August 3, 2017 7:58 AM
- To:** jrl@nonprofitdynamics.com
- Subject:** Re: Request
- Joe,
- I need Initiate outgoing Wire Transfer. (Circled in red, with an arrow pointing to the text "Email requests some kind of Funds transfer or bank account access.")
- Kindly get back to me and i can forward you the necessary details needed.
- I would prefer to call you but can't receive or call at the moment with my line. (Circled in red, with an arrow pointing to the text "Hacker's don't have phone numbers. They want you to reply via email.")
- Regards
- Joe
- Sent from my iPhone

Unfortunately, there is no way to prevent these emails from occurring. Instead, **you must exercise discipline when reading ALL your incoming emails:**

Here are some suggestions on ways to identify these email spoofs:

- Check the "from" email and name. Very often, they don't match. But beware, sometimes they do match!
- Be suspicious! Any email requesting funds or having anything to do with financial matters should be deleted immediately.
- View the source code to determine the true origination of the email.

If you suspect that an email is not authentic, you should:

- NEVER click a link or open an attachment from an unknown source.
- NEVER reply to these emails.
- Add a spam filter to your email program that filters words like "bank", "wire" "transfer" and "funds"
- Regularly scan your computer for Malware. I use Malwarebytes.com

I am initiating global filters for all my client email servers that can reduce the incidence of these email spoofs. However, there is no assurance that I can delete them entirely.

Please see [this page](#) on my website for more information about email spoofing.

Whenever you receive what you suspect is a spoofing email, please forward to me.

Regards,

Joe

Joe Leonard
Non Profit Dynamics
Visit our Website
[Forward to a Friend](#)
[Remove from Mailing List](#)
[Update your Registration with Us](#)

Powered by:

Non Profit  Dynamics

This email has images! Please set your [email program](#) to show images.