From: Steve Chacon
To: Steve Chacon
Subject: Important FEA Security and Fraud Alert - A Message From the FEA President.
Date: Thursday, February 2, 2017 1:46:30 PM
Importance: High

Dear FEA Members,

First off, let me insert SAVE 1031 into this email. Now, on to the message.

Many of you have recently received and some have been directly impacted by virus infected emails. Here's what we know and what each of us can do.

SUMMARY:

- On Wednesday, February 1, a group of the FEA membership received an email with the **subject line "CES FEB Review"** and an attachment which contained a virus.
- Today, some FEA Members received additional emails that looked like they came from Lynn Harkin at FEA Headquarters and from another FEA member.
- Lynn and the other two FEA member email addresses were victims of "spoofing". As the name suggests, cybercriminals spoof emails in a way that it **appears** to be originating from someone you trust.
- After investigation by FEA IT staff, our vendor partners and the affected member company, it was determined that the FEA and CES® websites were not hacked and no FEA email servers were compromised.

STEPS FOR MEMBERS:

1. The best defense is always to be highly skeptical of incoming email (even if it looks like it's coming from someone you trust) and NEVER open attachments or click on links you weren't expecting and/or that are vague about what is contained within. If you suspect something, call the sender to see if the email is legitimate.

2. If you opened any of the offending emails and *especially, if you opened the attachments or clicked on the links*, please perform a virus scan on your local computer immediately. If you don't have virus protection already on your computer, you can download Malwarebytes from Download.com. (It's a 14-day trial that will allow you to install it and run a scan today on your local computer that will detect this specific virus.)

3. Contact your IT departments and make them aware of this situation. They may be able to put additional security in place on your email server and make additional recommendations to you for added security on your local computer.

ADDITIONAL INFO:

- ✓ For the time being, any Emails with links/attachments coming from FEA Headquarters will have a phrase (SAVE 1031) in the first line of the body of the Email so that you know it is legitimate. **Do not open any emails, attachments or links from 1031.org that do NOT contain this line!**

- ✓ The GOOD news is most of these cyber criminals move on to a new group of addresses within a day or two as soon as the recipients understand what is happening and take steps to avoid spreading the infection.

- ✓ Please contact FEA Headquarters if you have any questions or receive any additional suspicious emails - Lynn Harkin can be reached at (515) 334-1067, or at director@1031.org.

Thank you for your attention to this matter. As with everything, the FEA is made better by the collective efforts and expertise of our members.

Steve

Steve Chacon, CPA CES®
Vice President, Service Operations
www.accruit.com
303-865-7316
LinkedIn | Twitter | YouTube