Topic: Spam/Phishing E-mails

Question by: Tom Riley

Jurisdiction: Tennessee

Date: February 10, 2020

Jurisdiction	Question(s)
	I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account. I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this. If there is, in fact, a problem with me receiving listserv emails, please let me know.
Manitoba	
Corporations Canada	
Alabama	
Alaska	
Arizona	
Arkansas	
California	
Colorado	
Connecticut	Just from our experience, this is usually because your email account has been compromised and someone is using it to send out phishing emails, so whoever has access to the IACA email, should change the passwords. Ct.gov accounts are getting hacked frequently, and that is always the first step.
Delaware	
District of Columbia	
Florida	
Georgia	
Hawaii	

Jurisdiction	Question(s)
	I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account. I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this. If there is, in fact, a problem with me receiving listserv emails, please let me know.
Idaho	
Illinois	

Jurisdiction	Question(s)
	I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account. I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this. If there is, in fact, a problem with me receiving listserv emails, please let me know.
Indiana	I would advise everyone to take precautions and follow your agency's protocols for suspicious emails. I do not know of anything related to the Listserv that requires a log-in. Please do not respond to any Listserv requests asking you to log-in. I will have Wade Knotts, IT Chair and Trevor Timmons, IT Vice Chair look into the matter and update you when we understand the issue. I wanted to follow up with you regarding the concern that Tom Riley had related to messages he was receiving from the IACA Listserv and the possibility that the Listserv was compromised. Wade and Trevor looked through the administrative side of each of the Listservs (BOS, STS & IT). Based on the administrative settings, Trevor and Wade agree that the Listserv software itself was sending Tom the bounce messages. We suspect this is likely due to anti-spam security settings his office has in place regarding incoming emails. Because the Listserv received bounce messages, it sent messages to Tom asking the him to log-in and confirm that his email was valid and it should not be removed from the distribution list. Because Tom did not respond to the request, the system removed him from the list. Trevor and Wade also reviewed the emails Tom received and confirmed that they were sent from the hosting provider which supports the IACA website and listserv. The bounce message from the Listserv included a password, which is clearly not an acceptable practice in today's environment. This caused Tom to be suspicious (as he should have been) and to believe it was a phishing attempt. We have changed the settings on BOS, STS and IT Listservs to prevent them from sending emails with passwords. We also changed the passwords on each of the Listservs as a precaution. Trevor spoke with Tom, and based on the conversation and research, we have concluded that it does not appear to be a compromise. We have received feedback from other Listserv recipients that they are having difficulties receiving email as well. Trevor and Wade are planning on looking into upgrades that will prevent or reduce these issues.
Iowa	

Jurisdiction	Question(s)
	I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account. I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this. If there is, in fact, a problem with me receiving listserv emails, please let me know.
Kansas	
Kentucky	
Louisiana	
Maine	
Maryland	
Massachusetts	
Michigan	
Minnesota	
Mississippi	
Missouri	
Montana	Montana seems to have the same issue with the DMARC, and my emails that are incoming are being moved to that.
Nebraska	
Nevada	
New Hampshire	
New Jersey	
New Mexico	
New York	
North Carolina	
North Dakota	
Ohio	

Jurisdiction	Question(s)
	I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account. I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this. If there is, in fact, a problem with me receiving listserv emails, please let me know.
Oklahoma	
Oregon	
Pennsylvania	
Rhode Island	
South Carolina	
South Dakota	
Tennessee	
Texas	
Utah	
Vermont	
Virginia	
Washington	
West Virginia	
Wisconsin	
Wyoming	

Additional comments:

If you want to forward that email to suspiciousemail@mailware.cisecurity.org<mailto:suspiciousemail@mailware.cisecurity.org> to check it out in their sandbox, they will. TN is a member of Elections-Infrastructure ISAC, as are all the state offices who run elections and they will be happy to check that out for you.

Others might want to do the same if they are seeing the same email. Tell them that your office has elections within the jurisdiction of your office (if they do) and that you want to be sure that this is not a potential phishing attempt.

Thanks!
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001

202-624-3525

I would like to add some information to this dialogue. I have also seen an increase in emails from IACA members that are not accepted by our email system and have received emails advising that due to the number of bounces re-registering was required. The reason many emails are being bounced is related to a system referred to as DMARC. I am not a techie, but the link below will offer basic information about this system deployed a while back that requires some technical changes to outbound emails in order to avoid being bounced on the recipient side.

I respectfully suggest someone with more technical expertise that I have add some information to this thread as I do not believe this is related to a compromised email account but rather issues with the systems of some senders.

https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.validity.com%2Fblog%2Fhow-to-explain-dmarc-in-plain-english%2F&data=02%7C01%7Cpviverto%40azsos.gov%7Cd8613cafb08f44cf75b208d7afdddb43%7Cb4494a03f26d475dba4139871e763531%7C1%7C0%7C637171239732561082&sdata=1aD60bTE6Xjo33B8YEZtFAVEtxnYU4A1%2FTTorXV%2FjZc%3D&reserved=0

Bruce Jacobi
CEO
Corp 800. 221.0102 Ext 1128

Direct 212.379.1928

Full text of email:

Good afternoon.

I have been receiving emails that appear to come from IACA. These emails claim that list serve emails to me have been bouncing back. They request that I log in to fix it. Of course, I would not be receiving that email if there was some legitimate problem with my account.

I am assuming that these are phishing emails that have somehow obtained your email list. I suspect you may be hearing from other IACA members about this.

If there is, in fact, a problem with me receiving listserv emails, please let me know.

Thomas H. Riley, III
Director of Business Services
Office of Tennessee Secretary of State Tre Hargett
312 Rosa L. Parks Ave. - 6th floor
Nashville TN 37243
Phone (615) 253-7742
Email: tom.riley@tn.gov