BE AWARE – FAKE FONASBA.COM EMAILS USED FOR PHISHING

It has recently come to our notice that some "@fonasba.com" email addresses used by members of the Executive Committee have been hijacked for phishing purposes. This is where what appears to be a genuine email address is used as an alias for someone trying to steal data or infect your computer with malware, viruses etc. We are all aware that these emails exist, Andrew Jamieson highlights them every year at the C&D Plenary! Anyone receiving such an email should therefore treat it carefully until it has been proven to be genuine. Confirmation that the email is bona fide can in most cases be established relatively easily by carefully applying the following tests:

1. Is the email addressed to you by name? In a close organisation such as ours, it would be expected that the email will be addressed personally. The level of personalisation will depend on how close you know the sender but use of given names is common within FONASBA. At the very least "Dear Mr./Mrs. (Family name)" would be expected. The lack of any greeting, or something generic like "Hi Friend" or "Hi Mate", especially if the sender hasn't used that expression before, is a major clue to the fact the email is suspicious.
2. Is the spelling and grammar correct? This applies to emails in English and in other FONASBA languages. Ideally, this rule should be applied in conjunction with…
3. Does the email refer to a topic that you would reasonably expect the sender to contact you about, or does it refer to something completely out of character? FONASBA only circulates emails on bona fide issues of interest to the ship agency and ship broking communities or internal administrative issues so anything out of the ordinary, and especially those offering great deals (for example: "Hi, I saw this great offer and thought of you") or promising prizes is immediately suspect.
4. Does the message appear to be in response to an issue you that you initiated, or a matter you are likely to be involved in? If you did not start the conversation it appears to be responding to, or the action it is referring to is not something you or your association would engage in, it is probably fake. As an example, FONASBA receives regular emails appointing us as agents for a vessel or asking us to provide lists of the products we supply – neither of which we do so they go straight to Spam.
5. Does the return address field show a completely different address? If the email is legitimate, it will show exactly the same return address but if it has been hijacked for phishing purposes, that address will be different. In Outlook you can check the actual address by hovering the cursor over the hyperlink and it will reveal the fake one hiding behind it. Similarly on an iPhone you can place your finger over the address and it will do the same thing. Presumably most other email clients do this. A different address may also appear in the "Reply to" field, for example:

   From: "FONASBA" <generalmanager@fonasba.com>
   Subject: FONASBA has shared a OneDrive for Business file with you
   Date: 22 February 2018 22:33:52 GMT-3
   Reply-To: "FONASBA" <**david.bradley@maliciousemails.com**>

6. Check the email address carefully. It doesn't take too much imagination to add another character to the domain name ("@fonas1ba.com") or change ".com" to ".co.uk" and then register a shadow email account in that name. It is, however, easy to miss these subtle but important changes.
7. Finally, does the email look right? As in most cases, if it doesn't look right, it probably isn't!

Unfortunately, email servers only look at the headline address so flagging a "@fonasba.com" email address as spam will result in all bona fide messages from that address being blocked. Some anti-virus applications can flag a suspect message with the word "SPAM" or "VIRUS" added to the title bar but unless there is a virus or piece of malware embedded in the message itself, this does not work. In many cases the malware is picked up when you click on the link.

So, if in doubt, do not open any attachments, click on any embedded links or do anything the email asks/instructs you to do. Instead contact the sender using the email address or telephone number in your contacts list. The only holders of "@fonasba.com" email addresses are current members of the Executive Committee and the Secretariat staff. Full contact details for all Execom members are shown on the list that can be found on the website at: www.fonasba.com/fonasba-member/committee-members. DO NOT use any contact details shown on the suspect email.

There is no easy way to defeat these phishing emails (although a huge reward awaits someone who develops something 100% effective!) but a bit of time, care and common sense should keep you safe from these malicious emails.

IF IN DOUBT, DON'T CLICK, CHECK!!!