

MD19 Website Report

To: MD19 Council of Governors

Date: June 12, 2023

From: J.D. Nellor, Past Council Chair

The website has undergone numerous changes since it was first launched, all in an effort to make it easier to use and to provide the access to information most useful to MD19 Lions and Leos.

Upcoming Changes. Here are changes and updates currently on the agenda:

- First, The website is currently undergoing edits and modifications to reflect the change from a 9 subdistrict to a 5 sub-district Multiple District. Those changes are going on in the background — you will not see the changes until after the close of the fiscal year (the adjournment of the International convention on July 11, 2023). There will be some “refreshing” of the format but buy and large the website seems to be working so formatting will be familiar.
- Next, the MD19 website is moving its current shared host to its own dedicated host. This move has been planned for some time, but it seemed logical to coordinate the move with the rewrite of the website following redistricting. This move will open space for adding databases (which will streamline annual updating every fiscal year) and will add space for MD19 to offer related entities (MD19 Lions Foundation, for example) districts and committees entities to park their websites without having to pay for their own dedicated hosts. The annual cost to MD19 of this move currently is... \$60⁰⁰ (for a 3-year contract, \$84⁰⁰ for a 1-year contract). The move should be seamless to users.

Email Spam: On to another topic that has been discussed before.

Earlier this year a few users in District 19-I reported receiving phishing emails that they believed were caused by their email addresses being listed on the MD19 website. These turned out to be, what should be, a very familiar phishing scam where people receive an email that says it is from someone familiar to them, but it is not. After an investigation by the MD19 web host, a likely source was located and was referred to the appropriate authorities. No connection to the MD19 website was found.

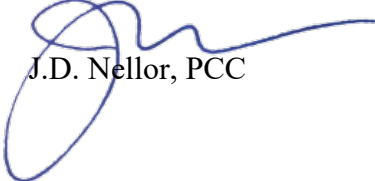
If you receive a suspicious email that you think is somehow connected to the MD19 website, forward it to handyman@lionsmd19.org, and we will refer it to our web host for tracing and referral to appropriate authorities, and will take whatever steps are required if meddling with the MD19 website is found.

So we are all on the same page, here is a brief summary of what I have previously reported on this subject, beginning with when we first launched the new website (*see*, for example the October 22 Council of Governors report):

- We list email addresses and telephone numbers of club presidents and secretaries, zone chairs, vice district governors, district governors, the MD19 office, committee chairs and members and affiliated entities in various places on the website. We *do not* publish personal addresses on the website.
- The MD19 website employs up-to-date, recommended technologies to hide email listed addresses from electronic cultivation. Yes, it is possible for someone write down phone numbers and emails off the MD19 website, one at a time, while sitting at their computer. But that is not what spammers spend time doing because they need to hit thousands of addresses at time to have any chance at convincing one or two people to go buy cash-cards, or whatever, for them.
- Unfortunately, the biggest source of spam/phishing comes from using your email. The only way to totally eliminate the potential of spam/phishing is to never send an email to anyone. Email is not secure (although, there have been some significant advances in securing email being implemented by email providers that started back in November/December 2022). There are businesses that intercept email transmissions, collect the email addresses, and then sell their lists.
- Personal vigilance is your best protection. Do not click on links in emails from people you do not know. Do not respond to emails from “friends” that ask for you to buy something or send them money or give them access to your bank account — if in doubt, call them. Do not provide personal information to anyone in response to an email. Do not respond to emails purportedly from a bank, eBay, Amazon, etc, or click on any links in an email to “update your personal information” or “reinstate” your account — check your account by the way you would normally do so (such as by logging in to your account directly from your browser).
- If you don’t want your phone published on the website, tell MD19 and it will not be published. I will let you assess the wisdom of remaining incognito to your constituents.

Thanks to all of the suggestions on things to add to the website and ways to make it better, many of which have been adopted. Keep the suggestions coming, please.

Respectfully submitted,



J.D. Nellor, PCC