

Recently there have been a large number of scam and phishing emails sent to our members. These sometimes offer mailing lists or purchase orders, they may send links for you to pay accounts or subscriptions, or they may be purporting to be Board members or Committee Chairs requesting help making or processing payments. THESE ARE SCAMS! Bots and scammers have programs to scrape public websites for email addresses to try to steal your money and/or infect your files and systems.

Here is an example:

From: Michael Morgenthal <president001877@gmail.com>
Date: Fri, May 15, 2026 at 6:38 PM
Subject: Program Expenses (Guides Association Of New York City)
To: [REDACTED]

Lili,

I am currently out of Town with limited phone accessibility. Will you be able to handle Program Expenses on our behalf?

Sara Lyons needs to pay a vendor but is currently down with a severe flu, Would you be able to assist with these platforms(Paypal, Zelle or Chime) to process the payment to the Vendor? I will have your reimbursement processed as soon as possible.

I await your response.

Regards,
Michael Morgenthal

Notice the email address is not president@ganyc.org, the capitalization does not make sense, and the request is extremely vague. No one from the GANYC Board or GANYC Committees will ever ask you for money to make GANYC payments via email or text. Payment requests are only processed for FAM tours, fees, and membership dues. If you receive this kind of email, please delete it immediately and ignore; you do not need to notify IT.

Keep in mind GANYC communicates primarily via email announcements like this one processed via Wild Apricot. **You will only receive official emails from ganyc.org and/or from ganyc.wildapricot.org.**

If your phone number is published on your profile, you may also receive suspicious requests via text message. These are also scams and should be ignored. Right now, GANYC does not use text messaging for contacting members with official business or announcements.

[Here](#) are some useful tips about how to recognize and avoid online scams. Personally, I always hover over the email address and if it looks unfamiliar or strange, I delete it right away.

[Here](#) is useful information about protecting your personal information. One of the most important security steps that you can take is to update your passwords regularly, avoid using the same password for multiple accounts or websites, and use two-factor authentication whenever possible. If you use multiple accounts and websites that you may want to consider a password manager; I use RoboForm for all my passwords.

Please feel free to contact GANYC IT: it@ganyc.org if you have any questions.

Emma Guest-Consales, Ph.D.
Chair, IT Committee

Marc Landman
Emeritus Chair, IT Committee