Scam Attempts in Meeting

March 2025

In late February, 2025 at least three of our members received emails signed (apparently) by one of our clerks. The message began:

“Greetings,
Hello, are you less busy at the moment? I got a request for you to manage discreetly. I will be going into a meeting shortly, please no calls so kindly respond back via email.”

The person signed with the name of one of our clerks and identified themselves accurately as clerk. Their profile image was the AFSC logo. A little odd, but Quakerly nevertheless.

One member responded:
“Sure. Let me know what’s needed.”

The “clerk” then said:
“Thanks! Here’s what I want you to do for me because I’m a little busy right now. I have been working on incentives and I aimed at surprising some of our diligen”

Another message soon followed:
“I will be glad if you can do this now. I need 10 qty of Sephora gift cards worth $200 value on each (total $2000). You should get them at any local stores around you now. After you get them, I need you to remove each card from the pack and scratch the back then take a clear picture of the front and back of each card and receipt then send them to me on here in my email so I can easily get them sent to each member myself. Please keep physical cards for reference. Let me know when you are on your way to the store. Thank you.”

Our members realized this was a fraud attempt and ended the conversation. Here are some of the warning signs:

1. The “from” address at the top of the email was our clerk’s name followed by an email address: <friendsmeeting888@gmail.com> This is not our clerk’s email address, nor is it a familiar address for anyone in our Meeting.
2. “Greetings” is not a typical salutation among people who know each other well. Especially not immediately followed by “hello.” Unusual usage like this is a red flag.
3. Requests to handle something “discretely” and with “no calls” are also red flags. What is the reason for secrecy and no personal contact? Especially among friends!
4. The clumsy and ungrammatical language are also red flags.

Let’s review the early warning signs in that first message:

The requests to “manage discretely” and “no calls” back, were enough to raise an initial concern. Yes, that is our clerk’s name in the from field, but <friendsmeeting888> is not an address we have ever known for her.

It would have been appropriate to forward that initial message to an address known to be hers (from our directory or from a personal address book) and ask if she has a new email address. Or better yet, telephone her later when she is out of the meeting she mentions.

The first lesson is to train yourself to always look at the address in the from field, for any message. In this case, it clearly was not our clerk's customary address.

Scammer "friendsmeeting888" was clever in using Quaker identifiers including the clerk reference and the AFSC logo as a profile picture. But some scammers are more clever. A couple of years ago, another of our member's email account was hacked, and many of us received messages sent to her contacts. The "from" field contained her name and (apparently) her email address. The request was unusual, so a closer look at the "from field" was called for. The "ie" of the name used in her email address had been transposed to "ei." Not easy to spot at first glance! All it takes is one character different or out of place to create a separate account. For example, using the digit "1" in place of the letter "l" is also a neat trick.

So, to summarize:

1. *Always* pay attention to the "from" field.
2. Be skeptical of unfamiliar and unusual requests, even from people you know!
3. Make personal contact with anyone making an unusual request, especially if money, gift cards or sensitive information is involved.
4. Always use trusted contact information (telephone number or email address) instead of whatever is provided in a suspicious message or unusual request.
5. Do not click on links, download or open attachments, reply to, or use contact information provided in unfamiliar messages.

Now, if you discover that your identity is being used to send scam messages to your contacts, *immediately* change the password on your email account.

Then examine your account and your contact address book to make sure everything is intact. If a hacker has damaged or emptied your address book, contact your email service provider. They may be able to restore your address book. Or not.

The best practice is to reset your account passwords periodically, or use a password manager. Unfortunately, most of us fail to do so and remain vulnerable.

It is possible that this scam attempt was initiated by someone with a copy of our directory. That possibility is being addressed separately. Keep your directory secure at all times.

For more information about how to protect yourself from cybercrime, visit
https://milwaukeequakers.org/cybersecurity/