Clerk's Corner
October 4, 2023

Last week several people received emails claiming to be from our Council Moderator, Mary Ann Bromley, asking for a moment of their time. If you looked closer, you would have noticed that it didn't come from her usual email address and just didn't sound like her. A few years ago, something similar happened to me. Members of my previous presbytery received emails from "me" asking for immediate response on a matter that needed to be kept discrete. Even though the email claimed to be from "Rev. Barry Chance," used a professional photo of me as a profile picture, and was sent to several people in the presbytery's leadership it was not, in fact, from me. Unfortunately, this is a common scam used particularly with pastors and churches to take advantage of our generous nature, busy schedules, and the sometimes confidential nature of our work. Churches also have notoriously bad cyber security (click here for a shocking report on that!). In fact, we have often made the job of scammers easier because most pastors, church employees, and sometimes session members have a lot of information about them publicly available on church websites. Scammers use our desire to be transparent and available to take advantage of us. In that case, the scammers were able to identify that I am presbytery staff, pull my picture from the website, and send emails pretending to be me to other people in presbytery leadership. The scammers set up a fake email address using my name and photo and then sent emails to my friends and colleagues hoping that they wouldn't see through the ruse!

And here is the thing: almost all of that information was likely publically available on the internet between the presbytery website and the websites our of member congregations. No hacking was needed! Unfortunately, that also means that the solution to the problem is not as easy as simply changing my password. This is not the first time that this has happened to me and it will not be the last. A few years ago my congregation's Treasurer received a similar email like this wherein "I" asked him to transfer several thousand dollars from one account to another. Fortunately, he saw through it but the fact that scammers are putting the time and effort in means that this scam works often enough to make it worth it. Situations like these are a good reminder of why the Book of Order requires congregations to establish standard financial practices (G-3.0205). Those practices ought to include issues like "Who counts the offering on Sunday?" but they also ought to include some procedures like requiring two signatures for checks or money transfers that will prevent fraud attempts like the one described above. If your congregation needs help establishing standard financial practices, the presbytery will be glad to assist. In light of the fact that these scams are fairly common for churches, here are a few tips on detecting, responding, and preventing them in the future:

Detecting

1. Always be suspicious of requests for immediate response. Scammers are trying to take advantage of your desire to help and hoping that you will be in too much of a hurry to notice any red flags.

2. Always be suspicious of requests for confidentiality. Scammers are trying to take advantage of the (sometimes) confidential nature of pastoral ministry and hoping that your ego will ignore any red flags because you are "in the loop."
3. Always be suspicious of requests that seek to limit the medium through which you can respond. Scammers rarely have access to the person's actual email or cell phone so they might say they are "in a meeting" or "out of the country" so you cannot call or text. What they are really doing is trying to make sure that you only contact them so they can complete the scam.
4. Always check the email address. Most often these scams are not the result of hacking the pastor's email password. Instead, they have taken the pastor's name, position, and even picture and set up a new email address pretending to be that person. This is called spoofing and since the scammer never had access that means the pastor changing the password won't stop it. In checking the email address, pay careful attention, sometimes the difference can be very subtle with .co instead of .com or a slightly misspelled name. At other times it is quite obvious. The scam that prompted me to write this article the first time was from an email that did not resemble any one of my three email addresses.

Responding

1. Do not respond to the email as this will verify for the scammer that your email is valid.
2. Do not follow any links or open any attachments in suspicious emails.
3. Contact the person you suspect is being impersonated through another form of communication.
4. Report the suspicious email to the domain where it originated (gmail.com, yahoo.com, etc.) so they can shut it down.

Preventing

The best way to limit these kinds of scams is to limit the amount of information that is publically available on your church website and for your pastor to place some privacy limits on his or her social media pages. Doing so will reduce the amount of information that is available to scammers; unfortunately, it will also limit the amount of information available to members and visitors who may be using your pages to contact the church. Fortunately, there are some simple steps that you can take while also retaining the usefulness of your online presence.

1. Use an email form on your website instead of publically posting email addresses. Most website hosts already have the tools available to establish this extra layer of security.
2. Establish a password-protected portion of your website that will allow members to access directories and other important information without making them publically available.
3. Pay attention to what information you post online. Bulletins, newsletters, and Session minutes often contain the same kind of information as a church directory so posting those on your website may be the same thing as posting your church directory online!
4. Use secure passwords. This will help prevent actual hacks and further deny scammers the information that they need to make their scams successful.

5. Educate yourself and your staff, leaders, and members about these threats so that they are better equipped to avoid and prevent them.

Do you have questions for the General Presbyter & Stated Clerk? Email him! Your question may help other churches as a topic for a future article.

May the Peace of Christ be with you,
Barry