First Unitarian
SOCIETY OF MILWAUKEE
nurture. engage. inspire.

Cyber-Attack, Phishing Emails: What should I do?

by Shari Wright, Office Manager & Information Tech Team Lead

Several church members have reported to us suspicious email in their Inbox. The first step to stop scammers on the web is to identify the suspicious email in your Inbox. So great job if you found one!

A phishing email imitates someone's familiar email with similar words, but not the real email address. At First Church, our ministers will NEVER send you an email to request cash or gift cards by replying to the email.

If you receive a phishing email, please take these steps to handle it:

1. Identify the phishing email by carefully looking at the email address. Don't reply to this email or click on any links.

2. Report the phishing email to your email provider.

3. Mark the email as spam, then delete the email.

4. Notify the person who was imitated in the phishing email.

5. It is not necessary, but always a good idea, to run a virus and malware scan of your PC.

Don't fret if you received a phishing email. These types of emails are sent frequently to try to get through to your email Inbox. The junk and spam filters try to catch these emails and do a good job of removing many which you will never see. If you practice these simple steps, you have learned a lot about computers and how to communicate in the digital world.

Phishing is described by Wikipedia, "Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication."