STAY ALERT THIS HOLIDAY SEASON

The Cybersecurity & Infrastructure Security Agency (CISA), and the Federal Bureau of Investigations (FBI) recommend maintaining vigilance against the multiple techniques that cybercriminals use to gain access to networks, including:

- Phishing scams, such as unsolicited emails posing as charitable organizations.

Staying vigilant against phishing is critical, here are some common traits of phishing emails to help you stay protected:

- **E-mails Insisting on Urgent Action:** E-mails insisting on urgent action to fluster or distract you from taking time to validate its authenticity.
- **E-mails Containing Spelling Mistakes:** E-mails purporting to come from a professional source that contain spelling mistakes, or grammatical errors should be treated with suspicion.
- **E-mails with Unfamiliar Greetings:** E-mails where greetings are not normally used, and those containing language not often used by friends, parishioners, or other colleagues.
- **Inconsistencies in E-mail Address:** Check the senders' e-mail address, especially when an e-mail address belonging to a regular contact is unfamiliar.
- **Inconsistencies in Links and Domain Names:** Hover your mouse pointer over a link in an e-mail to see what pops-up as the e-mail address. If an e-mail claims to be from (say) a church leader, but the pop-up indicates an unfamiliar website, the e-mail is likely a phishing e-mail.
- **Be Wary of Suspicious Attachments:** E-mails with file attachments should be treated with caution – particularly if the attached file has an unfamiliar extension (.zip, .exe, .scr, etc.).
- **E-mails That Seem Too Good to Be True:** E-mails that seem too good to be true, incentivize targets to click a link or open an attachment with the promise that they will benefit by doing so.
- **E-mails Requesting Log-in Credentials, Payment Information or Other Sensitive Information:** E-mails requesting log-in credentials, payment information or other sensitive information should always be treated with caution.
  Do not access gift cards and coupons or other links in e-mails or texts without first checking the official website of the business to validate that any links you receive direct you to the official business site.

- Fraudulent sites spoofing reputable businesses—it is possible that malicious actors will target sites often visited by users doing their holiday shopping online

WHERE TO REPORT SUSPICIOUS ACTIVITIES:

- Federal Bureau of Investigation's Internet Crime Complaint Center: https://www.ic3.gov/
- Better Business Bureau website: https://www.bbb.org/
- Better Business Bureau Scam site: https://www.bbb.org/all/scamstudies
- Charity verification: GuideStar, CharityNavigator, CharityWatch, National Association of State Charity Officials

PLEASE REMEMBER THAT ALL OF OUR OUTREACH EVENTS WILL BE PUBLISHED IN OUR BULLETIN AND/OR ANNOUNCED IN CHURCH. THE CHURCH DOES NOT SOLICIT GIFT CARD DONATIONS BY TEXT OR EMAIL! PLEASE CHECK WITH MOTHER LISA, OUR TREASURER DENISE CRATES, OUR OFFICE MANAGER JON EWBANK, OR ANY LAY LEADER IF YOU RECEIVE ANY REQUESTS FOR DONATIONS.