IMPORTANT NOTICE – PHISHING and SPOOFING EMAILS

St. Mary's office has noted an unusual increase in the number of internal phishing & spoofing emails lately. Phishing & spoofing is an attempt by fraudsters to (1) have you transfer money (2) make a purchase, e.g., iTunes cards (3) reveal personal information by sending you an email from a person or organization that they are pretending to be. This current spate of phishing emails is most likely related to a hacked email account where the email contacts are now being used. Because of this we would like to warn you to be wary of emails you may receive from our Pastor or staff that request information, favors, money, or gift cards.

Note the following excerpts from a recent example:

1st Email to parish staff or parishioner

Hello.

How are you?

I need a favor from you. Email me back when you get this message.

Many Blessings,

2nd Email to parish staff or parishioner

Good to hear from you, I need you to get an iTunes gift card for some patients going through cancer in the hospital and i promised each patient but i can't do this right now. I'm currently busy in a pastoral meeting. Can you get it from any store around you? I will pay back as soon as i get back. Let me know if you can get it now

Note, that some recipients of these emails have gone through the process of purchasing iTunes cards and have provided the codes on the cards to the fraudsters who have then used them to make purchases

---

Do not get scammed. Here are some tips on dealing with phishing:

- Confirm as legitimate any email that is requesting a sensitive business task to be completed.
- If the tone of the email is urgent this should be a signal for additional caution.
- Never respond to a wire transfer request - always **STOP-CALL-CONFIRM** with the Pastor or manager.
- Do not share bank account numbers or other banking information over email.

- Do not publish staff email addresses on a website – use a ‘Contact Us’ form instead.
- Be cautious about opening attachments or clicking on links in emails. Even your friend or family members’ accounts could be hacked. Files and links can contain malware.
- Search for the terms ‘email spoofing’ and ‘phishing’ to become familiar with these tactics.
- Learn more about how to protect your personal information
- Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.
- Routinely backup all your business files and test you can recover these on a periodic basis (in case malware wipes your data access.)

Tips to make online accounts secure:

- Do not use the same password for your various internet accounts (email, Facebook, Twitter, Bank Accounts, etc.) Each account must have a unique password.
- Do not use simple passwords but rather use complex passwords comprising a mix of uppercase and lowercase letters, numbers, and special characters.
- Use multifactor authentication (MFA) if you have that option.
- Change your email account password if it is older than 6 months.
