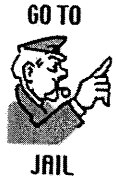

SCAM ALERT

We want to make Parishioners aware of a "phishing" scam that has been discovered within the Diocese and specifically here at St. Thomas More Parish. Hackers have penetrated our email system and have been sending bogus emails asking for sensitive information or unusual things to be done. Examples include asking for the purchase of gift cards, wire transfers of money, or bank account information to be sent back to the sender by email. At first glance, these emails look legitimate and often even have the greeting you might expect from Fr. Andy or other members of our Parish staff, so it is hard to distinguish them from legitimate emails that members of the Parish may send out. These scammers are using "Social Engineering" to try to make you believe the messages are legitimate and convince you to provide your credentials and other secure/sensitive data. A "Social Engineering" Scam is "the art of manipulating (e.g., impersonating) people in order to persuade you to provide confidential or sensitive information via email, phone, and text messaging." There is some indication that a few Parishioner's Facebook accounts may have recently been similarly manipulated.

Here are some general guidelines you should follow:

- Exercise caution when receiving or replying to emails and report all suspicious emails. **RED FLAGS** that should make you suspicious: your account is closing, announcing a change of payment process requiring your information, last minute changes to a schedule, information is needed immediately to meet an artificial deadline.

- If you receive an email that you were not expecting or the request in the email is looking for confidential or personal financial information, contact the sender directly (NOT through the email you received – call them directly) and ensure the request is legitimate. Never reply to these emails. **DO NOT** provide any information (private or otherwise) to the source.

- **DO NOT** click on any hyperlinks or attachments in a suspect email. This can compromise your account and/or computer. If in doubt, you can move your cursor over the hyperlink without clicking, and the Internet web address will appear. Look closely at the web address, and if it looks suspicious, don't click on the link.

- **DO NOT** download or open any attachment in an email unless you trust the sender **and** you were expecting the information or request. Again, the safest policy is to call the sender and verify the request.

- **NEVER** provide your password or login information and **DO NOT** allow anyone access to your computer. Some scams indicate you have a problem with your computer and they will help you if you contact an 800 number. If you have provided your password, change your password immediately.

- **NEVER** send money, gift cards or the like if the request is via email. Always contact the sender directly to verify the request.

- When reporting a suspicious email, **DO NOT FORWARD IT**. Contact the parish by phone or send a separate email to stmfinance@comcast.net or stmdurham@comcast.net . After reporting the fraudulent email, block the sender from your computer.

- The best motto is "When in doubt, check it out". Call the sender.