SCAM ALERT

This week our parish has seen heightened spam activity. A particular attack has been experienced by several parishioners and the parish office these days. Malicious individuals gained access to a parishioner Contact List including names, mailing addresses, phone numbers, and email addresses. **NO financial or other proprietary personal information was released**.

All parishioners are reminded that *only official parish and school* email addresses, telephone numbers, and mailing addresses are used, as listed in the parish bulletin and on the parish website, www.ourladyofthecross.com.

At no time will Fr. Pierz, the Parish Office, or others affiliated with the Parish ask for gift card codes, banking transfers, or other solicitation of funds by text, email, or any means other than those directly affiliated with the parish, its school, and our diocese. The current platform for online giving is through OSV (Our Sunday Visitor).

Do NOT open or click on suspicious emails without first verifying their source is **@ourladyofthecross.com** or **@materdolorosaschool.org** or **@diospringfield.org**

St. Michael the Archangel, protect & defend us!

Here below are tips provided by a risk management organization of our Diocese of Springfield:

- **Always look at the sender's email for clues of its legitimacy**. Examine the sender's email address closely, comparing it to previous emails or correspondence known to be legitimate. Scammers will use email addresses that look similar to a legitimate email, but you will usually find tell-tale signs that it's a fraud.
- **A transfer of funds should never be performed solely on the basis of an email exchange. Obtain verbal confirmation** by calling your known contact directly.
- **Do not call the number listed in the email or on the letter you received.** If it's a fraudulent email or letter, the number will be fraudulent as well. Always call the legitimate number of your known contact.

- **Do not share bank account numbers or other banking information over email.** Banks will never ask for your account number, social security number, name, address or password in an email or text message. They will only ask you to provide this information to verify your identity when you call them directly.
- **Frequently check your bank account for possible unauthorized payments**. Check over all charges at least once a week and flag any suspicious or unrecognized charges. Be on the alert for very small amounts that may “test” whether they can follow up with a larger amount, as this is a big red flag.
- **Check with your bank** about controls over unauthorized debits.
- **Watch for potentially misspelled Words.** It’s less common these days to find typos in a fraudulent email or text, but you may still encounter it. If you find one in the message, it is most likely a scam.
- **If the tone of the email is urgent, this should be a signal for additional caution.** Never transfer money to anyone who pressures you to pay immediately, or who says this is the only way to pay.
- **When in doubt, call the Parish Office**

REMEMBER: STOP – CALL the Parish Office – CONFIRM