# SCAMMERS POSE AS PRIESTS IN TEXTS/EMAIL, ASK PARISHIONERS FOR GIFT CARDS, CASH

# All,

We have been alerted once again that many parishioners of the Diocese have been targeted by fraudsters and it's not just happening in New Jersey. The Diocese of Scranton, Pennsylvania, and the Archdiocese of Miami, Florida and others also have reported the scam and the Texas attorney general issued a <u>consumer</u> <u>alert about it</u>. The alert indicates that the scammers are probably using information found on church websites or in online parish bulletins to trick parish members into parting with their cash. Fraudsters using Facebook messenger have even gone so far as to include a priest's profile picture, captured from Facebook or another online source, to make their correspondence appear more authentic.

## Don't fall for it! Here's what to know and do:

- First, your pastor or associate pastor will never contact a parishioner directly with an emergency request for cash or gift cards. Messages asking parishioners to help fulfill a need would come through the parish's or the diocese's official communication channels or be accomplished through a collection approved by the diocese. If you're not sure about a text or email you've received, do not engage or respond and call your parish office right away to notify a staff member. In addition, please note that neither your parish nor the diocese will ever sell or give away parishioners' personal information.
- Often times with text messages, a scam can be identified by looking at the phone number.
- If you are contacted by a scammer, report it to your parish. If you can, capture screen shots of the correspondence on your phone or laptop and email those to the parish. File a report through the Federal Trade Commission's <u>Complaint Assistant</u> which helps the FTC detect patterns of fraud and abuse.
- If you suspect that your Facebook account has been hacked, CBS News offers these tips on how to tell if your account's been hacked and what to do about it, and Facebook offers these action steps for hacked and fake accounts.
- ٠

### Other resources for reporting fraud and scams

How to report things on Facebook

Scams and Safety (FBI)

5 Signs of a Scam (from the Texas Attorney General's Office)

### If you spot any of these tactics, stop and walk away. You're probably being scammed.

### They contacted you

When you contact a business, you know who's on the other end of the line. But when someone contacts you first, you can't be certain they're telling the truth. You don't know if they are whom they say they are. And remember, email addresses and caller ID information can be faked.

### They dangle bait—usually money

Let's face it: People simply don't give away large sums of money easily. If someone dangles bait in front of you—a big prize, a shopping spree, an easy loan — for nothing, they're probably lying.

### They want your personal information

Anytime anyone asks for your personal information — bank accounts, social security number, etc. — you should be on alert. Don't give it away quickly or easily, especially to someone you don't know. You may become a victim of identity theft.

#### You have to pay them first

If someone offers you a prize, debt relief, or employment — but first you have to pay an upfront fee to get it —you're probably being scammed.

### You have to wire money or send gift cards

If you're about to wire money or send gift cards to someone in order to receive a prize, or pay off a debt collector that contacts you ... STOP! This may be a scammer trying to take your money.

#### Additional resources

Scammers pose as pastors in email, ask faithful to buy gift cards (National Catholic Reporter, May 2019)

Do not hesitate to reach out to us if you have any questions.

Be assured of our prayers and support.

Leonardo Cortelezzi IT Director Diocese of Metuchen 146 Metlars Lane Piscataway, NJ 08854 732.562.2400 Icortelezzi@diometuchen.org