DIOCESE OF METUCHEN

To: All priests

From: Father Timothy A. Christy,
Vicar General and Moderator of the Curia

Re: Technology scams

Date: May 5, 2020

The COVID-19 situation continues to result in the suspension of Masses, services and gatherings at our parishes. Gratefully we are beginning to review possible protocols for re-opening; whenever those civil executive orders are provided. In the meantime, one major innovative approach to remain engaged with our people has been an increase in virtual and digital communication to our parish communities.

Pope John Paul II prophetically described the advances in technology to present the Church a "new Areopagus" for the mission of evangelization. Yet, with these efforts, there unfortunately continues to be issues where scammers are increasingly attempting to take advantage, especially with the rapid technology learning curve created by this pandemic situation to steal personal information and money. The issue of scamming should neither deter nor prevent digital or virtual communication to our parishioners. Rather, I write to share with you information about scammers so that you remain aware and implement the necessary protocols to either prevent an incident and/or a parishioner falling victim to a scam.

Gratefully, our Office of Communications and Office of Information Systems have issued correspondence in recent weeks about how to prevent scammers taking advantage, tactics they are using and examples of where it has taken place. However, it is important to continue sharing this information with you in the hopes that you also find means to communicate it to you parish communities. Below you can find further information in this regard.

We must remain prudent in our efforts and continue to be a source of confidence and care during these times. Please call or email the Office of Information Systems for assistance in any of these

matters or for further detail on prevention tactics. Bishop is grateful for all of your efforts to guide and protect your communities and to be a source of inspiration and evangelical zeal.

Here are a few tips that can help prevent the scammers from taking advantage of you:

- Be careful handling sensitive Information. Many people are working from home, and it's crucial to maintain a high level of security with any sensitive information such as social security numbers, address information, legal documents, etc.
- Never share your personal and/or financial information on the phone or through email and/or text messages
- The government will never call you to ask for money

In addition, here are some examples of scare tactics scammers are using:

- Scammers may attempt to contact you regarding: "free test kits to be delivered to your home" and warn you about "protecting your loved ones from the coronavirus"
- Scammers may offer help to pay student loans
- Scammers may attempt to make you believe they are from your local health department and scare you into believing you have come into contact with someone who has the coronavirus
- Scammers may use phishing emails that appear to be from the Center for Disease Control (CDC) or the World Health Organization (WHO)
- Websites on the internet offering vaccine kits for a small shipping fee
- Scammers may attempt to go door to door requiring you to take a fake coronavirus test

The NJCCIC encourages recipients who discover signs of malicious cyber activity to contact the NJCCIC via the cyber incident report form at http://www.cyber.nj.gov/report

Helpful Reminders

- Beware of fake websites; it has been reported that a similar version of Johns Hopkins University's Coronavirus Dashboard was created to spread malware and steal sensitive information.
- Beware of fake emails from fake medical experts claiming they have a cure you can purchase or spreading false information. **You may also receive emails from someone spoofing your workplace email (such as your HR department) that targets employees at our organization**.

As you are probably aware, anyone can spoof a link to be redirected somewhere else. Example: https://www.irs.gov/coronavirus/non-filers-enter-payment-info-here

Scammers are very good at spoofing sender email addresses and create similar false websites to direct the unsuspected donors to donate.

Please see the below incidents in the diocese of Venice, Florida, and others:

https://dioceseofvenice.org/warning-text-email-scam-alert-in-the-diocese/

https://www.episcopalswfl.org/dfc/newsdetail_2/3196873

https://stmarycharlevoix.com/email-scam-hitting-all-churches/

https://thecatholicspirit.com/featured/online-scam-targets-priests-parishioners/

Please consider informing your parishioners via your website/social media/email and/or other

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 Complaint Assistant, 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.

Other resources for reporting fraud and scams
How to report things on Facebook
Scams and Safety (FBI)