

Tips for Spotting a Scam. Don't fall for it! Here's what to know and do:

- First, Fr. Dennis or Fr. Charles 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 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. Call the 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 the area code is not local, it's likely a scam. If you are contacted by a scammer, report it to the Parish Office. If you can, capture screen shots of the correspondence on your phone or laptop and email those to the Parish Office.
- 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 at: <https://www.cbsnews.com/news/how-to-tell-if-your-facebook-has-been-hacked-and-what-you-can-do/>. You can also check the "help center" on Facebook for information on hacked and fake (cloned) accounts.

Be on the lookout when someone:

Pretends to be someone you know.

Scammers often pretend to be contacting you from the IRS or Social Security Administration, or from a company you're familiar with like your bank. They might make up a name that sounds official, or say they're calling on behalf of a loved one.

Presents you with a conditional prize or problem.

Scammers may say you've won a prize that's too good to be true, and you have to pay a fee in order to receive it. They might say you're in trouble with the government, or a family member is in trouble and needs money.

Pressures you to act immediately.

Scammers want you to act before you have time to think. They may say a family member has an emergency or your computer has a virus. Sometimes they threaten legal action, arrest or to freeze your bank account.

Asks you to pay in a specific manner.

Scammers will often insist you pay by sending money through a payment app, wire transfer or by putting money on a gift card and then reading them the number on the back. Some will send you a fake check, ask you to deposit it and then ask you to send them the money.

Actions to help protect yourself from scams:

| | |
|-----------------|--|
| Block | Filter unwanted emails to your spam folder and block unwanted calls and texts. |
| Resist | Don't let anyone pressure or threaten you into giving them personal information or money. Hang up or don't respond. |
| Refuse | Even if it's a business you recognize, don't give your personal or financial information to any one who contacts you. |
| Pause | If anyone says you must act right now, stop and ask yourself, "Is this how a legitimate company would act?" If something seems "off," it probably is. |
| Validate | Instead of clicking links in e-mails and text messages or calling the numbers provided to you, use a company's contact info from their official website. |
| Talk | If someone tells you to keep a secret or says something suspicious that makes you uncomfortable, stop and check with someone you trust. |