Prince William County Police

Crime Alert

5/8/18

Phishing Scam: Fraudulent Gmail Accounts

Suspected scammers have reportedly created fraudulent Gmail accounts in the names of pastors of Catholic churches in the Arlington Diocese and the Archdiocese of Washington D.C., and are using these accounts to solicit parishioners for monetary donations.

The Catholic Church does not use Gmail and does not solicit donations via email. Any email solicitation for money or other donations from a Gmail address in the name of a Catholic priest should be immediately suspected as fraudulent. The Diocese has been advised to report these emails to the Internet Crime Complaint Center via the provided link (https://www.ic3.gov/default.aspx) and is suggesting victims contact their local law enforcement agencies.

There has been one reported incident involving a Prince William County resident who lost an undisclosed amount of money as a result of this scheme. In that case the perpetrators spelled the pastor's last name wrong in the Gmail account. Any email received should be inspected for any indications of a potential scam including misspellings.

When you donate to a charity or any other organization, you are giving because you care and want to help — and you want to be sure your money actually gets to those you're trying to help.

Consider these tips before you give:

- Rule out anyone who asks you to send cash, pay with a gift card, or wire money.
- Phishing emails typically contain misspellings and poor grammar, and demand that you "act immediately."
- Do not click on links in suspected emails or use numbers contained in them.
- Never reply to a suspicious email or provide personal information to an unsolicited phone call.
- Report the email to the purported institution or appropriate law enforcement agency.
- Confirm the exact name of the charity and do some research, especially when donating for the first time. Search for the name of the charity online — plus the word "complaint" or "scam." That's one way to learn about a charity's reputation.
- Give to charities you know and trust, with a proven track record. Before you give to any charity, check them out with the Better Business Bureau's (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.
- Be wary of charities that seem to pop up overnight in connection with a natural disaster or other tragedy.
- Before you text to donate, confirm the number on the charity's website.
- Never click on links or open attachments in e-mails, even if they appear to be from a trusted source. You could unknowingly install malware on your computer or be taken to a look-alike website run by scammers.
- For more information, visit ftc.gov/charity. If you think you've spotted a charity scam, contact the FTC at ftc.gov/complaint.

REPORT ALL SUSPICIOUS ACTIVITY TO THE POLICE

Emergency: 911 - Non-Emergency: 703-792-6500