Roman Catholic Diocese of Portland

510 Ocean Avenue
Portland, ME 04103-4936

Telephone: (207) 773-6471
Facsimile: (207) 773-0182

Office of Information Technology

Please Read:
Email Safety in the Diocese of Portland

Good afternoon,

This is just a reminder to all that phishing email scams are happening on a regular basis in the Diocese of Portland. On occasion, emails claiming to come from the bishop, priests, or other staff members are received but are not actually from them. Their email has not been hacked, however, scammers have created email accounts with fraudulent information, so that it ***appears*** to be coming from a known recipient. Typically, these are coming from @gmail.com addresses.

These phishing emails are attempts by scammers to trick you into giving out personal information such as your bank account numbers, passwords, credit card numbers, or to purchase gift cards.

Never follow links, open attachments, or reply to suspicious or unsolicited messages.

<u>These signs can help you identify phishing scams:</u>

- the sender's email address or phone number doesn't match the name of the company that it claims to be from;
- the message starts with a generic greeting, like "Dear customer." Most legitimate companies will include your name in their messages to you.
- a link appears to be legitimate but takes you to a website whose URL doesn't match the address of the company's website.
- the message looks significantly different from other messages that you've received from the company/person.
- the message requests personal information like a credit card number or account password.
- the message is unsolicited and contains an attachment.

<u>What to do:</u>

- **DO NOT** send any personal information over email such as your bank or credit card accounts/passwords/login information, etc.
- You may verify the sender's address by hovering over the name or clicking the email details in the "From:" column to see the email address. As you may see, the email says it's from Father John, but the email address listed is from frjohn.portlanddiocese@gmail.com. That is NOT a valid email from Father John, who will always send emails from an @portlanddiocese.org address.
- If an email seems suspicious or questionable, always call the person or parish that sent the email to verify that they sent it.

- Hover your mouse over any links embedded in the body of the email. If the link address looks strange, don't click on it. In general, never click links from unsolicited emails.
- Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, it does not mean that it's legitimate. **Be skeptical when it comes to your email messages. If it looks even remotely suspicious, don't open it**.

This is a good practice to keep in mind for not only diocesan emails but also from your family, friends, or any other contacts you have.

Phishing Text Recommendations from the Federal Trade Commission (FTC):

- Don't email or text back. Legitimate companies won't ask you to verify your identity through unsecure channels like text or email.

- Don't click on any links within the message. Links can install malware on your device and take you to spoof sites to try to get your information.

- Report the message to your phone carrier's spam text reporting number. If you are an AT&T, T-Mobile, Verizon, Sprint, or Bell customer, you can forward the text to 7726 (SPAM) free of charge.

- File a complaint with the Federal Trade Commission. Your complaint can help the FTC detect patterns of wrongdoing.

Read the full page at https://www.consumer.ftc.gov/blog/2013/08/dont-text-back

Additional resources:

What is Phishing? www.phishing.org/what-is-phishing

Two government web pages that talk about phishing and scam emails and how to report them can be found at www.usa.gov/stop-scams-frauds and www.consumer.ftc.gov/articles/0038-spam.