ST. JOHN THE BAPTIST
Catholic Church & School

Beware of Email Scams

If you receive an email that appears to be from Father Phil or a staff member asking you to take some kind of unusual action – click a link or download an attachment you didn't request, wire money to a specified account, purchase gift cards and reply with the serial numbers, or simply to reply quickly, watch out – it could be a form of email "phishing" known as "whaling."

Whereas "phishing" involves sending a fraudulent email to a large group of people in the hope that a few will respond, "whaling" involves forging communications that look like they're from the "big fish" in an organization, i.e. the "whale." For us, this usually means the Father Phil, although it could be someone else in authority.

The message will give some explanation of why Father needs your help *immediately*. They may include some story about another person in dire circumstances whom Father Phil is trying to help. But instead of helping a needy person, if you respond you will actually be turning over money and possibly your identity information to a scammer.

Because these emails are usually crafted more carefully than your standard "phishing" email, they can be more difficult to detect. Unfortunately, it's difficult to stop these "whaling" attacks. The email accounts in question have not been hacked. Instead, they are being "spoofed" – that is, a fraudulent email account is cleverly configured to look at first glance like a legitimate one. Even if you block the fraudulent email, they'll just use another.

You can't stop the senders of "whaling" emails, but what you can do – which is entirely free – is educate yourself and other potential recipients. Here are two simple guidelines to help potential recipients avoid being tricked:

Verify the "from" email

The malicious actors behind "whaling" attacks are counting on people springing into action as soon as they see an important name on an email. You can outsmart them by looking beyond the name and checking the "from" email address to see if it matches what you know the alleged sender's email to be.

If you only see a name, you can cause the "from" email address to be displayed by hovering the cursor over the name.

Father Phil is always reifenbergp@sjbplymouth.org. No other variation of his email address is official.

Confirm requests with a conversation

Even if the email seems legitimate, if a request seems even remotely "off," don't act on it until you confirm it with a phone call or face-to-face conversation.

In the case of an alleged message from Father Phil, you may want to reach out to a member of the parish staff. DO NOT reply to the suspicious email. Likewise, if a member of your parish staff is asking you to do something unusual, confirm with a phone call.

Observing these two steps will go a long way in identifying and avoiding "whaling" attacks before they get their hooks in you.

Thanks to the communications staff in the Diocese of Newark for composing a version of this email and allowing others use it.