

## Phishing Scams

One of the facts of life in our modern digital world is there will be people trying to get money or goods fraudulently through phishing scams. This happens when an individual receives an email supposedly sent by someone they know and trust (their priest, senior warden or even the bishop). The email is sent to a number of people asking for assistance or a favor. *This is now all-too common and seems to occur on a weekly basis at any one of the congregations in our diocese.*

**"Spear phishing" is especially difficult because the perpetrator has the name of the sender or the recipient of the email and uses this to gain trust.**

**There is no way to stop these scams from occurring. But by being vigilant, the risks can be minimized or averted. Here are some steps to take.**

1. Check the return email address. If the address doesn't match the name of the sender, be wary.
2. Never open attachments from unknown sources, especially those with .exe extensions.
3. Be wary of generically addressed emails like Dear Friend or Dear Customer.
4. If there are links in the email, hover over them without clicking on them. This will show where the link will actually take you.
5. Look for grammatical or spelling errors in the text of the email.
6. Check the address at the bottom of the email. If it says "Pastor Jim" and Jim never goes by "Pastor", it's fake.

Finally, if after all these steps it looks safe and the sender is asking for money or access to secure data, **call the person directly to get verification.**

If you are so inclined, you are welcome to alert the international Anti-Phishing Working Group by forwarding the message to [reportphishing@apwg.org](mailto:reportphishing@apwg.org). However, **your best**

**defense for this is to simply delete the email, do not click on any links or reply to the sender.**