Identifying phishing scams sent to your Saint Mary's account

1. Information Technology will never send an e-mail to you regarding your account without providing detailed contact information in a signature that you can confirm via the Saint Mary's Online Phonebook (http://eureka.saintmarys.edu/phonebook).

2. A legitimate message regarding your account will come from an e-mail address ending in saintmarys.edu.

3. A legitimate message regarding your account will have a reply-to address ending in saintmarys.edu (if you reply to the message, it will send a message to a saintmarys.edu address).

4. If there is a link in the message regarding your account, it will direct you to a website that includes saintmarys.edu in the beginning portion of the address (http://www.saintmarys.edu, http://apps.saintmarys.edu, http://www.saintmarys.edu/prism).

5. Saint Mary's e-mail accounts have unlimited quota. Any message saying that you have exceeded your e-mail quota will be fraudulent.

Please keep these details in mind the next time you see a request for your password or other personal account information via e-mail. You should delete any messages that do not pass these five ways to identify a phishing scam.

If you still have doubts about the validity of a message:

- Students should contact resnet@saintmarys.edu.
- Faculty and staff should contact helpdesk@saintmarys.edu.