THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

Memo

Date: September 17, 2018

To: Priests, Deacons, Brothers, Sisters, Principals and Chancery Staff

From: Tom Hardy, Director, Office of Information Technology

Re: Potential Hurricane Florence Phishing Scams

The National Cybersecurity and Communications Integration Center (NCCIC) warns users to remain vigilant for malicious cyber activity seeking to exploit interest in Hurricane Florence. Fraudulent emails commonly appear after major natural disasters and often contain links or attachments that direct users to malicious websites.

Users should exercise caution in handling any email with a subject line, attachments, or hyperlinks related to the hurricane, even if it appears to originate from a trusted source.

NCCIC advises users to verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number. Contact information for many charities is available on the BBB National Charity Report Index. User should also be wary of fraudulent social media pleas, calls, texts, donation websites and door-to-door solicitations relating to the hurricane.

The NCCIC encourages users and administrators to review the following resources for more information on phishing scams and malware campaigns:

- The Federal Trade Commission articles on Wise Giving after a Hurricane and How to Donate Wisely and Avoid Charity Scams
- Using Caution with Email Attachments
- Avoiding Social Engineering and Phishing Attacks

We hope you find these tips helpful. If you have any questions or are in doubt, please contact the Help Desk at support@archatl.com.