THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

Memo

Date: March 26, 2018

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

From: Tom Hardy, Director, Office of Information Technology

Re: Ransomware Attack Alert

As I'm sure most of you have heard by now, much of the City of Atlanta's IT infrastructure was exposed to a ransomware attack within the last two weeks that could prove to be devastating to their services both, financially and operationally. Keeping in mind that this can happen to organizations big and small; private or public; local or distant; etc., the Office of Information Technology thought it would be a good time to share some of the following information to help keep this threat top-of-mind with everyone.

Ransomware is a type of encrypting malware that locks important company files and holds them for ransom. Ransoms typically range from hundreds to thousands of dollars. Cybercriminals made over $1billion dollars last year from businesses attacked by ransomware and since these cybercriminals have learned to monetize attacks; their frequency and severity of attacks will continue to grow exponentially.

You should be aware that most ransomware attacks come in the form of an email attachment and users should exercise extreme caution when opening any e-mail attachment. **Never open an attachment in an email you were not expecting to receive or one that you do not recognize the sender.** You should use the same caution when presented with URL's (i.e. embedded links) that you do not recognize or that may have come from an unknown sender.

With today's advanced ransomware techniques you only have to visit a website to become infected with ransomware. Let me make that clear. You DO NOT

have to click anything on the website to infect the company with data encrypting ransomware.

In 2017 alone:

- Ransomware emails spiked 6,000%
- 40% of all spam email had ransomware
- 59% of infections came from email
- 92% of surveyed IT firms reported attacks on their clients

These numbers are scary but important for you to know. As an employee of the Archdiocese (or a user in regular contact with Chancery employees), you are our first line of defense against ransomware. Please also remember to be vigilant when using home systems or other devices you may be using to connect remotely to our Chancery systems.

Remember, for the organization's safety, we feel that it is your responsibility to be sure you have appropriate anti-spam and anti-virus applications running on these systems and that it is kept updated and functioning. Should you need any assistance with the purchase of these tools for your personal/home equipment, please contact the IT department for recommendations.

Please follow the best practices as outlined in this email to ensure you do your part to keep ransomware off of our networks and systems. Failure to do so could result in significant downtime and monetary cost to the archdiocese and we all need to be prudent in stopping these attacks.

If you have further questions about ransomware and how you can help prevent it from infecting the Archdiocese's infrastructure, please feel free to reach out to support@archatl.com.

Thank you!