**Dennis Honan**

---

**From:** Dennis Honan
**Sent:** Friday, April 3, 2020 1:50 PM
**Subject:** CYBER SECURITY ALERT - VIGILANCE DURING PANDEMIC and FBI WARNING

# *DIOCESE OF MANCHESTER CYBER SECURITY ALERT*

**To:** Priests (via Digest), Permanent Deacons, Bookkeepers, Business Managers, Principals, Diocesan Administration Staff, Camps, CCNH Security Group

**From:** Diocesan Administration

**Type:** **VIGILANCE DURING PANDEMIC**

**Description:** With the pandemic, cyber criminals are increasing their attacks, hoping to take advantage of confusion and the migration to a remote work environment. The FBI has issued special warnings related to the Covid-19 Pandemic.

**For more information contact**

- Dave Kenney (603-663-0124, ithelp@rcbm.org)
- Dennis Honan (603-663-0112, dhonan@rcbm.org)

**Or visit https://www.catholicnh.org/security**

**With the pandemic, cyber criminals are increasing their attacks, hoping to take advantage of confusion and the migration to a remote work environment. It is important to be extra careful and very vigilant! Recent scams have included:**

- Requests to call, email back, send gift cards, transfer funds, have an invoice paid (that may be attached), perform wire transfers, or change payroll direct deposit.

- Requests to connect to a webinars, online conference call, or other communication. These are usually accompanied by an invitation to download a communication tool (like Zoom or GoToMeeting), but in reality is a virus that can take over your computer and your network to gain access to your files, banks, credit cards, etc. At times they will demand a ransom to get your files restored (known as ransomware).

- Scams and attacks using apps such as Zoom and GoToMeeting. The FBI's has warned about potential vulnerabilities in the apps, mainly that your meeting can be "Zoombombed" – joined by someone who wasn't invited or an inappropriate video added. Zoom and others are working on these vulnerabilities. People have posted screenshots of meetings in real-time on social media, which lets anyone see your Zoom, GoToMeeting, or Microsoft Teams meeting number and opens meetings up to uninvited people.

**Furthermore, the FBI has issued warnings about being vigilant during the Covid-19 pandemic** – you can read more here: https://www.fbi.gov/coronavirus.

From the FBI: As the United States and the world deal with the ongoing pandemic, the FBI's national security and criminal investigative work continues. There are threats you should be aware of so you can take steps to protect yourself.

- Children who are home from school and spending more time online may be at increased risk for exploitation.
- Anyone can be targeted by hackers and scammers.
- Protecting civil rights and investigating hate crimes remain a high priority for the FBI.

Use the resources at https://www.fbi.gov/coronavirus to help keep yourself and your family safe from these threats.

**Be diligent**

- Anytime there is a request to get money, always call the person personally - never rely on email.
- Always check for clues that a communication may be fraudulent:

1. It is from a non-diocesan, school or parish email address (i.e., headoffice27@aol.com). Even though it may say this is from "Bishop Libasci" for example, the email address is from something like thebishiop@gmail.com.
2. Check for unusual language and misspellings.
3. Sometimes they will say "I can't talk on the phone," or similar language. This is a major clue that it is fraudulent.
4. For diocesan mail, if you see this warning at the bottom of the email: *** WARNING: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. ***, **be especially careful.**

**Best practices**

- **DO NOT RESPOND under any circumstances**
- **LET YOUR PARISH, SCHOOL or ORGANIZATION KNOW:** Put announcements in bulletins, newsletters, and periodically remind people from the pulpit (livestreamed) or at group online meetings that neither the pastor, principal, or any staff members will ever ask for money, donations, gift cards, etc. via email. If you are promoting capabilities such as online giving, contributions, etc. – always refer people to your website only. If you are using websites such as "Go Fund Me" or PayPal for contributions, only do this via links from your website, not from an email.
- Use resources and information from the FBI https://www.fbi.gov/coronavirus
- **BE CAREFUL DURING ONLINE CONFERENCES/CALLS** and using apps such as Zoom and GoToMeeting. The FBI's has warned about potential vulnerabilities in the app, mainly that a meeting can be "Zoombombed" – joined by someone who wasn't invited or an inappropriate video added. Zoom and others are working on these vulnerabilities. Do not post screenshots of meetings in real-time on social media, which lets anyone see your Zoom, GoToMeeting, or Microsoft Teams meeting number and opens your meeting up to uninvited people.

## Additional Cyber Security Best Practices

Given the Covid-19 pandemic and recent scam attempts, it is probably a good time to reiterate cyber security best practices to keep in mind. Failure to follow these rules can have significant negative financial and other impact to your parish, school, organization, or the diocese, can take large amounts of time and cost to correct, and can put our network at great risk!

1. **SCREEN FOR COMMON SCAMS**: Match the email address of the sender to the name of the person who is requesting something from you. Read the email for unusual grammar or sentence structure. Be on the alert for any email asking for funds, gifts, or confidential information such as bank account numbers. Some common scams are just to get you to reply with questions "Are you in?" "Can you talk now?" and similar comments to engage you in further email exchanges. Once you have replied, they will try to convince you that they are who they say they are and get you to perform some kind of transaction. Some request wire transfers, gift cards and changes to an employee's payroll direct deposit.

2. **DO NOT RESPOND TO SUSPICIOUS EMAILS**: If an email requests funds, cash equivalents (gift cards, etc.), or sensitive information, and this is an unusual request, then it is likely a scam. Do not respond. Do not forward the email unless you wish to alert others of the potential scam. In most cases the best option is to delete the email and report it as a scam to your supervisor.

3. **CONFIRM VERBALLY WITH SENDER BY PHONE:** If the sender claims to be the pastor or other employee of authority and you think there is a possibility of legitimacy to the email, then prior to responding to the email, contact the sender by phone.

4. **DO NOT CLICK ON ANY LINKS IN AN EMAIL** unless you know that the email is from a trusted source and you are expecting it. If you have any doubt, do not click on the link before calling the sender to make sure it is legitimate.

5. **DO NOT DOWNLOAD OR OPEN ANY ATTACHMENT IN AN EMAIL** unless you know that the email is from a trusted source and you are expecting it. If you have any doubt, do not download or open the attachment before calling the sender to make sure it is legitimate.

6. **NEVER ENTER YOUR PASSWORD** except:
    a. When logging into your computer
    b. When accessing your email via OUTLOOK, your phone app, or a browser. Make sure the app is one that you installed. On a browser, make sure it is the correct URL (e.g. gmail.com, Microsoft.com, etc.). Scammers can make a site look legitimate to try to obtain your password. This has happened with email, banks, PayPal, eBay, credit card, and other sites. Always check the URL to make sure it is really the site that you think it is.

7. **NEVER PROVIDE YOUR PASSWORD TO ANYONE**. You should not give your password to anyone either via email, on the phone, on a website, or verbally unless it is a trusted

and known technology person helping you with a problem. Legitimate help desks will NEVER ask for your password – do not give it to them. Do not leave your password on or in your unlocked desk or anywhere it can be easily seen (like on a sticky note).

8. **NEVER PROVIDE ACCESS TO YOUR COMPUTER TO ANY OUTSIDE COMPANY**. A popular scam is to provide a popup on your computer from a website that you are visiting that indicates there is a problem on your computer and to call an 800 number and talk with a Microsoft support agent. There are variations of this scam, but they tend to be similar. The scammer will download software to your computer that allows them to access your data and passwords. There have also been instances where the software they planted has infected an entire network and they demand a ransom to allow you to access your own data. Never call an 800 number for assistance with your computer. The only people you should be talking with about accessing your computer is a trusted and known technology person.

9. **NEVER SEND MONEY, GIFT CARDS, or any other PURCHASE REQUEST** from anyone requesting these via email. In all cases these have proven to be scams! If you think it is legitimate (and it probably isn't), then CALL the person first.

10. **BE CAREFUL DURING CONFERENCE CALLS** and using apps such as Zoom, GoToMeeting. The FBI's has warned about potential vulnerabilities in the app, mainly that a meeting can be "Zoombombed" – joined by someone who wasn't invited or an inappropriate video added. Zoom and others are working on these vulnerabilities. Do not post screenshots of meetings in real-time on social media, which lets anyone see your Zoom, GoToMeeting, or Microsoft Teams meeting number and opens your meeting up to uninvited people.

11. **DO NOT RESPOND TO REQUESTS TO CONNECT TO UNKNOWN WEBINARS, ONLINE CONFERENCES/CALLS OR OTHER COMMUNICATIONS**. These are usually accompanied by an invitation to download a communication tool (like Zoom or GoToMeeting), but in reality is a virus that can take over your computer and your network to gain access to your files, banks, credit cards, etc. At times they will demand a ransom to get your files restored (known as ransomware).

12. **ENSURE THAT YOUR IMPORTANT DATA IS BACKED UP** to an offsite location. If they are not stored offsite, they can be lost or rendered unusable in the case of an attack.

11. **PASSWORD PROTECT ALL DEVICES.** If you are accessing our system either for email or via VPN, make sure all your devices (e.g., smart phones), are password protected with phrases that are hard to figure out. Longer passwords are best (e.g. "watchnbcsportsifyoucan!"). Change your password at least every 90 days.

12. **USE MULTI-FACTOR AUTHORIZATION** wherever available. For example, when logging in from a new device, the system will send a security code to your phone or email before allowing access.

13. **USE BCC:** When you send out an email to a distribution list, send it via blind copies (i.e., bcc). That way potentially scamming recipients (or one who has been hacked) does not have access to a large list for fraudulent emails.

14. **LET YOUR PARISH, SCHOOL or ORGANIZATION KNOW:** Put announcements in bulletins, newsletters, and periodically remind people from the pulpit or at group meetings that neither the pastor, principal, or any staff members will ever ask for money, donations, gift cards, etc. via email. If you are promoting capabilities such as online giving, contributions, etc. – always refer people to your website only.