DIOCESE OF FALL RIVER
CHANCERY FINANCE OFFICE

To: Diocese of Fall River Pastors

From Chancery Finance Office

Date: January 12, 2023

Re: Cybersecurity Tips

Every day the news is filled with stories of cyber-attacks. These attacks can take many forms, including phishing attacks where the bad actors trick users into giving out sensitive information or clicking on malicious links that are cleverly disguised in emails sent to unsuspecting users. In Bristol County the Swansea Public Schools were recently forced to cancel classes as a result of a ransomware attack, and Bristol County Community College reported a cyber-attack that was discovered right before Christmas. Our parishes, schools, and related entities are inviting targets for cybercriminals targeting small businesses they believe are susceptible and the damages can be extensive.

We'd like to share a few tips for you to best protect your parish or school from these threats:

1. **Enable Dual Factor Authentication (DFA):** We strongly recommend that parishes and schools enable dual factor authentication whenever possible. DFA is a layer of protection where the software program verifies that you are really "you" and not a bad actor that has secured your password.

   Last year we published instructions on setting DFA up on your QuickBooks accounts. Please share this link with your point of contact responsible for entering transactions into QuickBooks:

   https://www.fallriverdiocese.org/wp-content/uploads/2022/10/Quickbooks-Dual-Factor-Authentication-rev-10-22.pdf

2. **Require passwords … and make them strong**: Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places. You can use tools to check how secure your passwords are using the following link:

   https://www.security.org/how-secure-is-my-password/

3. **Avoid opening suspicious emails or clicking on suspicious links in emails**: If an email looks suspicious, don't open it because it might be a phishing scam to gain access to your personal information. Sometimes the emails may also include attachments or links that can infect your devices - never click these links or attachments. Doing so may provide a bad actor an opportunity to download malicious software onto your computer.

4. **Be on the alert for suspicious requests received via email**: Bad actors take advantage of busy people. Staff may get a request from a bad actor pretending to be a priest, and the staff may try to quickly help the "priest". Here are some recommendations if you receive a "suspicious" request:

a. Never wire or ACH funds (this is Diocesan policy), even if the "priest" tells you it is urgent (bad actors prey on our desire to be helpful).
b. Stop, look, and think! Bad actors prey on busy people trying to get multiple things done at once. Slow things down if it is suspicious.
c. Verify verbally – call or speak with the priest (if necessary get contact information from somewhere other than the email)

5. **Keep software up to date**: Updating to the latest version of your software can protect you from new or existing security vulnerabilities. This includes apps, web browsers and operating systems.

6. **Reconcile all bank accounts**: This is one of the most important controls of any business. This will not prevent an attack, but it will make you aware if a bad actor has somehow managed to get access to your account or if any fraudulent activity has happened. If you do see any fraudulent activity contact the Chancery ASAP (jharrington@dioc-fr.org; 508-985-6503).

If you have questions on any of these items, please do not hesitate to contact IT Specialist Laura Bradbury at the Chancery (Lbradbury@dioc-fr.org; 508-730-2986), or me at (jharrington@dioc-fr.org; 508-985-6503).

Sincerely,

Joseph Harrington

Joseph Harington
Director of Finance
Roman Catholic Bishop of Fall River