Treasurers Communique 2018-2020/06

January 5, 2020

Happy New Year to all the treasurers who work hard at being good stewards.

Most parish councils hold their Annual General Meetings in January, so there should be annual financial statements presented to the members at this time.

FINANCIAL STATEMENT REVIEW:

January is also a good month for diocesan treasurers to get everything together for sending to whichever accountant prepares your reviewed financial statements. For accounting geeks (Like me), there is a difference in the scope and extent of work (and price) between a review and an audit. By law, we have to make the reviewed financial statements available to our members at least 21 days before our Annual General Meeting (Convention). So the sooner we get our data to the firm doing the review, the easier it is for them to have everything ready for us to fulfill our legal obligation.

FINANCIAL FRAUD:

My home parish council hosted a talk by Randy Tabada, who is an RCMP officer working in the Commercial Crime division. This talk was very relevant, especially after the news of the data breaches at Desjardins Bank and at Life Labs. We all need to protect ourselves from fraud and scams. Randy gave us this handout:

Objectives
To learn how to identify and prevent common types of fraud

TYPES
Subscription Traps ▪

- Don't accept "free" or "low cost" trials for products or services.
- Once your credit card info is given to pay for shipping, you are unknowingly locked into a monthly subscription.

TIPS: before you sign up for a free trial, research the company and read reviews

Identity Theft

- Scammers are always looking to obtain your personal information to commit frauds.
- Identity theft could occur from online or through obtaining your personal information from the trash or mail.
- Fraudsters are interested your credit card info, bank account details, full name details, Social Insurance numbers (SIN), date of birth, and driver's licence.

TIPS: never provide personal information over the phone, via text message, email or the internet.

- Avoid public computers or Wi-Fi Hotspots
- Create a strong password for your home Wi-Fi Network
- Password protect your devices
- Always shield your PIN when using your card.
- Shred documents that contain your personal information

Romance Scams ▪

- Fraudster who preys on individuals who are lonely and looking for companionship
- They can use social media to do a background check on potential victims

TIPS: Never send or wire money to help potential friend move or obtain items

Phishing and Smishing Scams

- Phishing is unsolicited email that claims to be from a legitimate organization, financial institution, businesses or government agencies.
- Scammers ask you to verify your personal or financial information by clicking a weblink or by providing your credit card number, password, and SIN.
- Smishing is the same but it is done through text messages.

TIPS: know that legit organizations will never ask you for your personal information through email or text.

- Ignore text messages or emails from unknown contacts
- Do not click on unknown hyperlinks
- Update your antivirus program on all your devices and computers

Tax Scams

- Beware of any communication via text message or an email from the Canadian Revenue Agency (CRA) The CRA only communicates by mail
- If you get a call email, letter, or text message saying you owe money or get a refund confirm the information through your online account or call 1-800-959-8281

TIPS:

The CRA will never threaten you with the police or ask you to repay taxes via gift cards or e-transfers. The CRA will never ask or provide financial information

FRAUD WARNINGS

- Wire transfers – Do not send money via third party institutions like Western Union or Bitcoin
- Overpayment - When you are selling an item, and someone overpays for the item do not pay overpaid funds
- Personal Info – do not send requestors any passwords, login information, or personal information
- Too good to be true – Some deals are too good to be real. Beware of false ads and goods.

REPORT A SCAM / INFORM YOURSELF

Canadian Anti-Fraud Centre - Website: www.AntiFraudCentre.ca
Telephone: 1-888-495-8501

In addition to the tips above there are a few other items to be aware of:

1. Just after our CWL meeting, one of my neighbours told a group of us about a phone call she got from "Microsoft". She was told to send a wire transfer to pay for the "security upgrade" that she desperately needed. Fortunately, her bank stopped her from buying the wire transfer. The real Microsoft NEVER calls individuals.
   I have turned on the "Automatic" upgrade on my computer, so that when Microsoft does have legitimate upgrades, they get installed automatically. And when "Microsoft" calls, I tell them that I know they are scammers before I hang up.

2. The other famous phone call is from a "grandchild" who is stranded in a foreign country or is in jail and needs money. Hang up and phone the parents of the grandchild to confirm the story.

3. Make sure you have strong passwords. Eight characters can be hacked in about 30 minutes. It takes days to hack a 12-character password. And, yes, you do need to update these regularly, and make sure that you don't use the same password on everything. (This one is really hard to do.)

4. If you have family or friends who might be targets of scammers, talk to them. Give them a copy of the Fraud handout, so they become aware of what to do or not do.

5. Remember that scammers tend to target the elderly who they think are more trusting.

I hope some of this is of help to you and your members.

May Our Lady of Good Counsel bless us all.

Suzanne Eng
Treasurer