TREASURE TROVE

APRIL 2021

THIS EDITION: OFFICER'S DESK REFERENCE
PROTECTION OF MEMBERSHIP AND FINANCIAL INFORMATION
THE FORUM
- IDENTITY THEFT
OTHER PUBLICATIONS
INDEX (ARTICLES OF INTEREST IN PAST NEWSLETTERS)

WORTHY COUNCIL FINANCIAL SECRETARIES & TREASURERS

Welcome to *TREASURE TROVE* is dedicated to all Council Financial Secretaries & Treasurers but shared with the Council Grand Knight and all District Deputies. You may share this with anyone in your Council, but it relates strictly to your responsibilities in the Council. It is designed to provide Financial and other information on the Rules and Laws of our Order.
Remember…it is your responsibility to ensure that the Council Executive knows, understands, and follows these Laws and Rules.

Sources of Information

Several sources of information are used in the preparation of this bulleting:
- Supreme's Charter Constitution and Laws of the Order. This booklet is printed annually as there may be amendments to the contents…so request the latest on-line version from your Council Advocate.
- Officer's Desktop Reference (ODR) – this is a section on Supreme's website containing expanded information on the Rules and Laws of the Order. If you do not have access to the ODR website, ask your Grand Knight to set you up with Supreme.
- State By-Laws

OFFICERS DESK REFERENCE (ODR)

The Officers Desk Reference (ODR) is a guidance on the interpretation of the Constitution and Laws of the Order, Laws and Rules Governing the Fourth Degree, Council and Assembly governance. It is not intended to be legal advice upon which any

person can rely for securing rights or remedies cognizable under the law of any jurisdiction.

The ODR may be accessed off the Supreme website at ***kofc.org***. It is available to Grand Knights, Financial Secretaries, and Advocates at the Council level. The following also have access to the ODR…all District Deputies, State Membership Director, State Program Director, Executive Secretary, and all State Officers.

If you do not have access, then please contact Supreme and obtain the proper access credentials for this site. The ODR provides a wealth of information and complements the Charter, Constitution, and Laws booklet which every Council should also have a copy.

PROTECTION OF MEMBERSHIP AND FINANCIAL INFORMATION

Councils, and this includes State and Local Councils, Assemblies, and Chapters, should take reasonable measures and safeguard to ensure all their membership information and financial information is not improperly disclosed or misused.

Membership information and financial information should not be published or distributed in hard copy or electronic/digital format (email, website, social media), unless required for ordinary fraternal business, and only the minimum amount of information should ever be disclosed. Never publish or distribute personally identifiable information such as date of birth, or bank account numbers or balances. If, for some reason, personally identifiable information needs to be transmitted or distributed electronically, the information should be encrypted.

During business meetings, officers may disclose information, to the extent that it is relevant and necessary, in the course of delivering a report. Officers should use care when including membership information and financial information in published meeting minutes, including such information only when necessary.

There is no reason to ever request or store a member's social insurance number. At one time a previous version of the Form 100 included a space for an applicant to disclose his number, the form has been changed so that this information is no longer requested. To the extent that Councils have stored documents (in hard copy or electronic/digital format) that contain the social insurance number of any member or applicant, that information should be deleted or redacted.

Best Practices for Safeguarding Information

To help Council's safeguard membership information and financial information, Council officers should consider implementing the following best practices:

- Use the blind carbon copy (bcc:) feature when sending broadcast emails to multiple recipients.

- Exercise care and caution where it is necessary to exchange sensitive membership and financial information online. If such information, including personally identifiable information is transmitted or distributed electronically, the information should be encrypted.
- Write "*Confidential*" in the subject line when sending such information via email and ensure that only the correct recipient(s) receive the email. Alternatively, officers may consider using a secure file-sharing website/interface or a password-protected website to exchange sensitive information securely.
- Utilize the Order's tools such as Officers Online/Member Management, which have built-in security features.
- Remove metadata and geographic data from posts on Council social media pages. **Councils and members should understand that posting ANY information or materials online creates a permanent record. It can NEVER be deleted/removed!**
- Establish a dedicated email address for the Council that is accessible by the principal officers… the Grand Knight, Deputy Grand Knight, Financial Secretary, and Recorder (e.g., kofcCouncilXXXX@gmail.com).
- Establish dedicated email addresses for each Council officer position (e.g., kofcCouncilXXXXadvocate@gmail.com).
- Be sure to use a unique and complex password for any email account and to utilize security questions that are not easily guessed.
- All passwords should be changed whenever there is a change of officer(s) and at the start of each new Columbian year.

Signing up for an email address (such as a *Gmail* or *Yahoo* account) is free and simple to do. A Council email account can serve as an archive for the present and future principal officers of a Council. Moreover, because Council email accounts may be accessed by multiple officers, the information stored on these accounts would be immediately available to other officers in the event that one of the officers is incapacitated.

Membership Directories

Councils may create a roster or directory for contacting members about Council business and events. If the Council wishes to distribute a roster / directory to its members, the Grand Knight must notify the members of his intent to do so and provide reasonable time for any member to opt out of having his information published in the Council directory.

Councils and members may not, under any circumstances, distribute or make available membership rosters or directories to persons who are not members of the Council.

If State, Local Councils, Assemblies, and Chapters decide to publish on its website the names and contact information of its officers (i.e.; District Deputies, Financial Secretaries, State appointed Chairmen and Directors, Presidents, or other members) this information must be on a password-protected section of the website, accessible only to current

members. If the Council's website does not have this protective functionality, then such information should not publish at all regardless.

For additional information on this topic please refer to the Officer's desktop Reference on Supreme's web site www.kofc.org

---

THE FORUM

This section is designed to share information and feedback with Councils from comments or inquiries sent to the author.

Identity Theft

I wanted to bring this to everyone's attention as it is becoming more common than we like to admit. With cybersecurity breaches at big companies and a range of scams targeting unknowing consumers, your personal information is more valuable than ever.

Security breaches regularly make headlines, and it can seem as if our personal information is in constant danger of being stolen by thieves. But there are ways to make your personal information difficult for thieves to get their hands on. Here are a few to consider.

1. Your Social Insurance Number (SIN) is the key to all your personal financial records from credit reports to your tax returns. Created in 1964 its sole purpose was to identify a person to the Canada Pension Plan and various Government of Canada employment insurance programs. But its use has expanded to virtually all transactions between you and the government.
   Unfortunately, with no legal restrictions on who may request your SIN many private-sector organizations do ask and, unfortunately, we oblige… and that is where the problems start!
   Legitimate requestors are your employer (so they may issue you a T4) and financial institutions such as banks, insurance companies, and investment firms as they issue a T5 and T3 at year-end for tax purposes. No one else needs it… so protect it.
   If someone is persistent ask them why they require your SIN.
   Remember the more your SIN is floating around the more likely it will be stolen and sold on the "dark web" (the sinister underbelly of the internet!).

   If you believe your SIN has been stolen, file a complaint with police and make sure to obtain the case reference number, the officer's name & badge number, and a telephone number. Contact the Canadian Anti-Fraud Centre (CAFC) for further advice. Every few months obtain a copy of your credit report from one of Canada's

two national credit bureaus, Equifax and TransUnion and review it for suspicious activity. Consider placing a credit alert on your file requesting you be contacted if anyone tries to open a new account, take out a loan, or a new credit card in your name.
Remember it can take months and sometimes years to clear your name once someone steals your information and starts to make purchases in your name that you are now on the hook for payment.

2. Passwords: Apparently Canadians are abysmally poor at keeping our online profiles secure. A study was performed last year on several million user passwords. Not surprisingly it was found that the most commonly used passwords involved strings of sequential number (for example: "*123456*") and the most common word was "*password*". Other common passwords included: "*I love*" followed by the person's name, and dates (like someone's birthdate: "*4/15/78*"). The use of recognizable words or strings makes your accounts vulnerable to hackers who employ guessing software that can search millions of possible passwords per second.

   The most secure and memorable password is one that uses a string of letters, numbers, and characters derived from a phrase. For example, ("*ih2pa&nocg!n*" which translates to: "*I have two private accounts and no one can guess its names*").
   And the more accounts you have the more unique passwords you will need. If you use the same password for several accounts, you increase your potential exposure to hackers.
   If you cannot remember which password is for which account but want some protection, consider using a free password manager like LogMeOnce or pay sites like top rated Dashlane, NordPass and 1Password. There are others so find one you like and use it…. It is much cheaper than being hacked.

3. Malware, short for "*malicious software*", is a generic term for software (a computer program) designed to disrupt the way your computer operates, gathers information without your permission or knowledge, gains unauthorized access to your computer, and potentially causes other abusive or damaging behavior. Malware includes viruses, spyware, and other types of harmful software. Why should you care about malware? Well, it can…
   - Provide hackers access to your computer.
   - Monitor your computer activity, web habits, and even your keystrokes (including passwords) and transmit this information without your knowledge.
   - Lead to **identity theft.**
   - Hackers can demand ransom to unlock or restore your compute (only to do it again later!)

- Delete files, format disks, lock you out of your computer, or affect your computer's general performance.

Always be wary about opening files or clicking on "*mystery links*" sent to you via to email, text, instant message (IM), social networking sites such as Facebook or Twitter, ads and pop-ups. Links, files, and attachments may contain or lead to harmful programs that can damage your computer and its many files.

- Delete spam and suspicious emails/texts without opening or activating any attached files or links. Do not open, forward or reply to the message. You should be suspicious if:
  - A link or attachment is unexpected or unsolicited.
  - The email is not addressed to you by name.
  - You do not recognize the sender, or the message says it is from a "*friend*".
  - You cannot determine why the file or link was sent to you.
  - The file name of the attachment ends with EXE, HLP, LNK, MDB, MDE, URL or VBE
- Do not click on ads or pop-ups offering anti-virus software or warning you that your computer is infected. These are scams and can infect your computer or cause other harm.
- Make sure your computer's operating system (ie.; Windows 10) and applications are updated frequently.
- Do not download or install unknown software or software from an unknown source. Even if it is "free", you may get more than you realized (e.g., spyware, adware, etc.).
- Back up your important data and mobile devices and store the backups in a safe place.

4. Other types of threats…

   Computer worm: A computer worm is a software program that copies itself from one computer to the next. It does not require human interaction to create these copies and can spread rapidly and in great volume.

   Spam: Spam refers to unwanted messages in your email inbox. In some cases, spam can simply include junk mail that advertises goods or services you are not interested in.

   Phishing: Phishing scams are created by cybercriminals attempting to solicit private or sensitive information. They can pose as your bank or web service and lure you into clicking links to verify details like account information or passwords.

What is available to help you…

- Install anti-malware software on your computer and set it to auto-update as frequently as the settings will allow.
- Periodically double-check to see if your anti-virus/anti-malware software is up to date by opening the program and checking the "*Last updated*" date.

OTHER PUBLICATIONS

Here are other newsletters I published. I encourage those Council Executive members holding the respective position to access these newsletters to assist in performing their position's duties.

- "***Warden's Corner***", and
- "***The Advocate***".

All newsletters are also available on our State website ***kofc.ab.ca*** under… *Publications*.

Your feedback is invaluable**.** If anyone has any questions or comments on anything drop me a line. Also, if there is a topic you wish covered in future newsletters just send a note to st2019@kofc.ab.ca

Thank you for your attention…and God Bless.

Vivat Jesus
Sir Knight John Onyskiw
State Treasurer

INDEX