THE ADVOCATE…

MARCH 2019

FEATURE ARTICLES: *DISPOSITION OF COUNCIL INFORMATION & MATERIALS*
FORUM
INDEX (ARTICLES OF INTEREST IN PAST NEWSLETTERS)

Welcome to THE ADVOCATE….dedicated to all Council Advocates but to be shared with the Council Executive, and all District Deputies. Please do share this with all the members in your Council but it relates strictly to your responsibilities in the Council. I will endeavour to keep every missive short but they are designed to inform and educate. Remember…it is your responsibility, Worthy Council Advocates, to ensure that you and your Council knows and follows our Charter, Constitution, Laws and Rules, and also your Council's By-Laws.

Please refer to the *INDEX* section … it lists articles published is previous issues of this newsletter.

DISPOSITION OF COUNCIL INFORMATION & MATERIALS

Every Council is charged with the safeguarding of membership, financial, meeting minutes, and ceremonial information. But there are times when we overlook our responsibility and inadvertently, and hopefully unintentionally, dispose of information improperly or left behind that should have been filed, shredded or destroyed.

We have to be careful on how we dispose of Council documents and other literature that is proprietary to the Knights of Columbus. The Grand Knights and Financial Secretaries have access to tremendous amounts of personal information on its members. Protocol dictates Councils must take precautionary measures to ensure that no membership, financial or Council information is left in plain view for wandering eyes. If meeting minutes were distributed prior to a meeting they should be returned at the end of the meeting. Refer to my *September 2017* newsletter on the protocol governing Meeting Minutes and their disposition which may be found at www.kofc.ab.ca.

If you have a disc with Knights of Columbus information that is no longer required it must either be returned to our State Office or to be mutilated and destroyed. It was mentioned by a Grand Knight (the requestor of this article) that a member brought in a DVD of our First Degree Ceremonial. He had picked it up at Value Village for a dollar!

FORUM

Identify 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 and insurance companies as they issue a T5 and/or 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 a number of 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 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.**
   - 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. Don't 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 don't recognize the sender or the message says it is from a "*friend*"
     - You can't 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

- Don't 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 and applications are updated frequently.
- Don't 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.

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.

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 SA2017@kofc.ab.ca

Thank you …and God Bless.

Vivat Jesus
Sir Knight John Onyskiw
State Advocate

INDEX

	Applicants for Membership in the Order who have Criminal Records Petition for Reinstatement
January 2018	Resolutions – Part 1 Forum: Basketball Free-throw Council Signing Authority Praesidium Course – Multiple Youth Directors Including Multiple Recipients in an E-Mail
February 2018	Resolutions – Part 2
March 2018	Roberts Rules of Order (overview) Motions
April 2018	Elections Movie Nite Forum: State Council State Board
May 2018	Council Elections
July 2018	Council Advocates Praesidium – Safe Environment Program Council By-Laws
August 2018	Praesidium…Safe Environment Compliance Council Advocates - Access to Officer's Desktop Reference Website Forum: Council Executive Responsibility
September 2018	Praesidium…Safe Environment Policy Update IT Security Policy Forum: Council Chaplains
October 2018	Protection of Membership and Financial Information Forum: Praesidium / Armatus Reports
December 2018	Praesidium Training & Safe Environment Program ... Update
January 2019	Praesidium – Background Checks Resolutions
February 2019	Nominations for State Board and Supreme Convention Delegates