FEBRUARY 2022

THE INFORMER

NEWSLETTER

Welcome to the February issue of *THE INFORMER*. This issue continues with defining the responsibilities of the Council Executive and goes on with a special article on Identity Theft, something we all should be vigilant about.

Lastly, I ask that the Council Grand Knight forward this newsletter to all their members.

THIS ISSUE:

Several sources are used in the preparation of this newsletter. These include:

- 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 version from your Council Advocate.
- Officer's Desktop Reference (ODR) – this is a section on Supreme's website containing expanded information on the Constitution, Rules and Laws of the Order.
- Grand Knights Manual

COUNCIL EXECUTIVE

Over the years and travels to many Councils, I encountered Council Executive members inquiring what are their responsibilities and how to perform their new duties. This section is dedicated specifically to the Council Executive members on these items. I will cover each position over the next several issues.

THE DEPUTY GRAND KNIGHT

1. Preside at meetings in the absence of the Grand Knight.
2. Be available and ready at all times to take the place of the Grand Knight.
3. Be valuable to the Grand Knight as a close advisor and strong supporter.
4. Be familiar with the current version of the Supreme Charter, Constitution, and Laws of the Order as well as bylaws of his own Council.
5. Be familiar with the Grand Knights Manual.
6. Perform such other duties as the Grand Knight may request or the Order may impose.

FORUM

Identity Theft

Identity theft is a serious crime where your personal information, anything from your name, driver's license, or Social Insurance Number has been compromised by an imposter who intends to commit fraud in your name. With your Social Insurance Number, someone can easily obtain false lines of credit and rack up significant debt in your name. With a stolen identity, someone might hide behind your name in a legal matter, leaving you with a false criminal record. Identity fraud is a major problem, and it happens more often than you might think.

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 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 *LastPass* or *Bitwarden*, 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". This 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 or 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 4.
- 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.

4. Phishing. This is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in Identity Theft and financial loss.

Generally, emails sent by cybercriminals are masked so they appear to be sent by a business whose services are used by the recipient. A bank will not ask for personal information via email or suspend your account if you do not update your personal details within a certain period. Most banks and financial institutions also usually provide an account number or other personal details within the email, which ensures it's coming from a reliable source.

Here are a few ways to protect yourself…

- Many websites require users to enter login information while their image is displayed. This type of system may be open to security attacks. One way to ensure security is to change your password regularly and never use the same password for multiple accounts.
- Banks, financial institutions, and the Federal and Provincial Governments use monitoring systems to prevent phishing. If you feel you have been a victim of a phishing scam report it to an industry group where legal action can be taken against these fraudulent websites.
- Change your browsing habits. If verification is required always contact the company personally before entering any details online.
- If there is a link in the email, hover over the URL (the web / internet address line) first. Secure websites that are valid have what is called a Secure Socket Layer – an SSL Certificate and begin with "*https*". The last letter in "*https*" (the '*s*') signifies it is a secure site.

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

- for Council Wardens, the "***Warden's Corner***",
- for the Council Advocate, see newsletter "***The Advocate***",

- for Council Treasurers and Financial Secretaries, check out the '***Treasure Trove'*** newsletter.

All newsletters are also available on our State website: ***kofc.ab.ca***
Go to "Publications" for the full list.
If you have any questions or comments, please sent them to: **ss2021@kofc.ab.ca**

Until Next time.

Vivat Jesus!
Sir Knight John Onyskiw
State Secretary

INDEX
(of past issues)

December	Supreme Representative - District Deputy Fraternal Survey of Fraternal Activity Tech Corner Other publications
January	Council Executive - Grand Knight Volunteer Opportunities for Youth A Legal Matter Other publications