**This assignment will give you opportunity to become knowledgeable of different types of Internet Fraud.  The Canadian Bankers Association has a Web site full of useful tips on this topic (cba.ca).  Your assignment is to choose five (5) of them and report your findings using the outline below:**

* Identify the type of scam/fraud
* How the scam/fraud works
* How to stop/prevent the scam/fraud
* What to do if you have been scammed

Assignment #6 Marking Scheme (20 marks)

* 5 topics \* 4 marks each = 20

**Topic 1:** How to Protect Yourself from debit Card Fraud

<https://cba.ca/debit-card-fraud>

Where is the cash? Do we even own any of those plastic currency nowadays, when we live in the era of electronic transactions especially with credit/debit cards? Debit cards have become part of everyday life for our Canadians, and according to cba.ca we are the highest users in the world. Although, debit cards is safe to use; there are cases in which debits cards may easily be duplicated and misused. In year 2018 alone, about 4.4 million dollars were lost to debit card fraud(interac) and 8000 card holders were reimbursed. You would know you’re being scammed if there many unrecognized transactions or less money in your account.

Debit card frauds happen in three ways

* + when a thief/attacker duplicates your debit card by using the information from the magnetic strip behind the card.
  + When your PIN is memorized by the thief to access your account
  + Or if you lose your card, and your PIN is left unprotected.

Debit Card Fraud is mostly uncommon with all the advances in technology (chip technology) in Canada. Your cards are protected by the Canadian Code of Practice for Consumer Debit Card Services, that return your stolen money back. Debit cards frauds have dropped 92 percent in the recent years. In case, if you are a victim of Debit Card Scam, contact your bank immediately and the rest is taken care of by the bank. To avoid being scammed:

* + Don’t give your card or pin to anyone
  + Choose a secure pin
  + Check your transactions
  + Don’t give your card number to unnecessary people
  + Change your pin periodically, like how we have to change our uwinsite password every three months.

**Topic 2:** How seniors can avoid the grandparent scam

<https://cba.ca/grandparent-scam>

Most of childhood memories consist of spending time at our grandparent’s house. Criminals have taken advantages of this and started blackmailing grandparents for money, especially in the summer season. The scam starts off with a call, “Grandma, do you know who this is?”, allowing the senior to assume it’s one of their grandchildren. So, they answer, “yes, it’s John” Now that the criminal has the grandchild name, they gain more credibility with the victim and they will ask for money by saying that their grandchildren is in danger (car accident, arrested and etc.). The criminal impersonates him/her to be professional making the grandparents assuming the call to be real and serious that prompts them to withdraw money from their banks and wire transfer it. If you get a call like this, report to your local police department. If you were one of the victims, you can protect yourself by various simple ways. For example

* + Don’t give out any unnecessary information (like your grandchildren name) to unknown callers
  + If you’re being blackmailed, stay calm and ask questions to the caller for information about your grandchild (like personal questions that only you and your grandchild know)
  + Spread the knowledge to others of the scam.
  + Don’t provide your credit card or bank account information to anyone

**Topic 3:** Wifi Hot-spot

<https://cba.ca/wifi-hotspot-scam>

We cannot live without glancing at your phone for a minute. In this texting era, Wi-Fi is a prominent word that plays a huge role in everyone’s life. Wi-fi connects us to the internet while we are outside playing soccer, walking or in a meeting and etc. We all want free wi-fi, but it comes with a danger as criminals can steal your information when you connect to unsecure public network. The scam all starts with when you connect to “Free Wi-fi” because it is a computer-to-computer network that could be a trap. So, whatever you do while connected that internet can be seen by the criminal. With this advantage, criminals can install spyware or access your files and personal data. If want internet, ask an official or staff for their network name or hotspot information, and don’t connect to networks that have two options with the same name. One simple solution is to not connect to free public wi-fi in local location other than legitimate places (airport, café or hotel), or check the description of the wireless network (not computer-to-computer network). Other solution includes disable file sharing capabilities, turn on your systems Internet firewall, and don’t process any financial information in a public network.

**Topic 4:** Protecting yourself from the cheque fraud

<https://cba.ca/protecting-yourself-from-cheque-fraud>

Most of your salaries are payed in the form of a pay cheque. According to financial institutions in Canada there has been a decline in cheques being issued, but many people still use it. However, cheque fraud does happen, when Criminals steal cheques and create fraud version of them or change the name or amount of the stole cheque. To protect yourself from cheques fraud, keep all your cheques in a safe place, review your bank account regularly, shred unused cheques. The best option is to switch to electronic payments rather than check, as it is hard to prevent cheque frauds in most cases. If your suspicious about the cheque your receiving, don’t accept it, check if it’s a valid check according to your country’s check regulations and requirements. It is your responsibility, to know if the cheque your depositing is valid or not, else you have to pay the funds you used form it to the bank. Some other ways to prevent cheque fraud include:

* + Check if the cheques are dated properly and completed.
  + Accept computer printed cheques, not altered with ink ones.
  + Accept cheques written to your name

**Topic 5:** Vacation Fraud without the Vacation

<https://cba.ca/phoney-bank-inspector-scam>

I am really going to get the vacation I need before fall semester kicks in, since I am taking a full course load this semester (summer). Vacation excites everyone, so we go to the internet searching for hotel discounts, trip discounts and etc. The vacation fraud is when criminals email all your family members, friends and mail contacts about your stuff getting stolen in vacation and how you’re in desperate need for money and help. The scammers hack into your email and send this information to everyone, it is not only you that is being hacked but even those email recipient’s also and from there it is a ripple effect. The best solution is to set a unique and secure password for your email, when using public computer with your email (logoff). If you are a victim, help others by informing them about this scam. If you receive this type of email, don’t send any money to your friend before conforming about this situation. Along, with this type of scam, there exists the free vacation scam that involve money (everything is about money). Now that I read this article, I need to be careful when I plan my vacation.