Avoiding Frauds and Scams and Setting Your Computer Optimally

The following fact sheet will help you recognize known scams and fraudulent acts committed against seniors. (Prepared by Halton Regional Police Services and augmented by Gary Bridges)

GRANDSON SCAM - The scam occurs over the telephone and targets the elderly.

- The caller identifies himself as the victim's grandchild, usually by saying, "Do you know who this is?"
- The caller will wait for the victim to respond with something to the effect of, "Oh John Is that you?" thereby identifying the grandson for the fraudster.
- At times, the fraudster will identify themselves by name. It is believed that in these instances, the information was obtained from published sources such as obituaries, classifieds, and social networking websites.
- The caller usually indicates that he has been involved in a car accident or has been arrested and charged with a criminal offence and is thus in urgent need of cash to cover legal fees

Tips to Avoid Becoming a "Grandson Scam" Victim

- Ask the caller for a callback number. This gives you time to verify information.
- Ask the caller a personal question only your grandchild could answer, such as their date of birth.
- Speak to another family member about the matter before sending money or contacting the police.

BITCOIN SCAM

How the Scams Work: Scammers will contact you and state that there is some sort of problem or emergency and that they require you to send them a payment using Bitcoin. Common scams can include:

- A warrant for your arrest has been issued
- You haven't paid enough taxes
- There are pending immigration fines
- There are outstanding police or legal fees
- Online romantic interest starts requesting money
- In order to claim your lottery winnings, and
- Deposit or payments on a property is required

Note: The Canada Revenue Agency or the Canadian Government will never ask for Bitcoin as payment and neither will a legitimate business.

BANK INVESTIGATOR SCAM

Fraudsters call consumers claiming to be a financial institution or major credit card provider. The fraudsters inform the consumer that they are investigating unauthorized activity on their account. The fraudsters ask the consumer to help them catch the criminal by providing access to the consumer's account.

Warning Signs - How to Protect Yourself

- Financial institutions will never ask for assistance from the public for internal investigations.
- Financial institutions never ask you to transfer money to an external account.
- Never provide remote access to your device to unknown callers.
- Never provide personal or financial information over the phone unless you called your financial institution.
- Don't purchase Google Play, iTunes, or gift cards or use Bitcoin for payment – These items are not legal tender.
- Check your bank statement frequently and report any irregularities to your bank as soon as you notice them (see note Re locking your cards under E-Commerce Tips further on).

DEBIT CARD FRAUD

Always protect your banking Personal Identification Number (PIN). By taking the following precautions, you can help protect yourself from this increasingly common type of fraud.

- Be mindful of your surroundings when at bank machines and paying for store-bought items.
- Fraudsters will stay close to you while you withdraw money from ATMs, looking over your shoulder to see your PIN.

Take the Following Steps

- Cover the keypad when entering your Personal Identification Number (PIN).
- Avoid using a password number linked to you, such as a name, birthday or address.
- Never write your PIN on your card or a piece of paper in your wallet.
- Always shred personal information. Always protect your PIN or use TAP when possible.

EMAIL FRAUD

- Do not respond to offers of money, threats, legal action, or warnings about "compromised security".
- Be watchful of phishing emails that ask for personal or financial information.
- Never provide personal information to anyone via email.
- Be suspicious of email attachments from unknown sources. If you do not know the sender of an email, do not open the attachment.
- If a suspicious Email appears, hover your cursor (DON'T CLICK) over the responding link, look at the status bar at the bottom of your browser; you should see the URL path. Fraudulent paths will have a path that displays no similarity with the apparent WebSite the Email purports to be from (ie Bell, Costco, RBC, CIBC etc). Delete the Email.

E-COMMERCE TIPS

- Shop only from your home computer and not on public ones. It is much safer.
- Deal only with reputable companies you know and do your research. Legitimate merchants will have easy-to-find information about themselves, their location and contact numbers.
- Don't be pushed or rushed into buying an item, especially by "limited supply" or "limited time" warnings.
- Know what you are paying for, and all costs involved. Read the term and conditions of all contracts before buying.
- Ensure the merchants you deal with online have secure transaction systems (indicated by a padlock symbol at the bottom of your browser) before providing credit card or other sensitive information.
- Consider using a credit card with a low credit limit or single use payment card.
- Always print and save the confirmation page when completing online purchases.
- Monitor all bank statements and activity online. Report discrepancies to your financial institution immediately.
- Never provide your Social Security Number, date of birth or a driver's licence number to a seller.
- Always remember that if it sounds suspicious or too good to be true, it probably is.
- If you receive any credit card charge that you either don't recognize or appears suspicious, remember that you can sign-onto your Bank WebSite (from your cell phone App or Internet) and "lock" the credit card (also valid for the Bank Card). You don't have to call and wait; you can do this right away. This prevents further charges (from any vendor) being charged, because the card will be declined. This also gives you time to phone your Credit Card vendor and determine the best course of action: replace card as (stolen / compromised) or contest the charge.

THINGS YOU CAN DO TO PROTECT YOUR DATA AND COMPUTER HARDWARE

VIRUS/SPAM CHECKING SOFTWARE

We highly recommend the installation of Internet/Virus software. We have used Norton, Kaspersky, McAfee (available free for Bell Email customers), Microsoft Defender and others. We won't get into recommendations here (we have used them all) but you can easily find reviews and comparisons of these products on-line. Their sophistication has improved immensely over the past few years.

Some of these products have backup programs which you can use to backup your critical files and keep them safer on a separate memory device (don't put backups on the C:\ drive where the Operating System resides).

WHERE TO STORE YOUR FILES

We recommend that your "data" (information that is particular to you – images, documents, spreadsheets, etc) be kept (when working on them) on a separate hardware device (either a separate hard drive in your machine, an "external" drive (usually connected via a cable to a USB port) OR a USB stick – which are now being made in large sizes - 64Gb).

If any of you have had a computer failure/crash (machine won't boot, blue screen of death etc) we know how frustrating that can be. While restoring the Operating System is not a straight forward task, it is made even worse if your data is also gone. If you have kept your data on a separate drive, the chances are excellent that the OS failure will not have compromised it. You can then take it to another computer (wifes', childs', friends') and still have access to your critical files, while your broken device is diagnosed and repaired or replaced.

ONLINE PASSWORDS TIPS

Choose unique, yet memorable passwords, at least 8 characters long. Don't use your name or address as components.

- Generally most WebSites now require "strong" passwords with either 6 or 8 characters, especially Financial Institutions. Use a combination of letters (capitals and small case), numbers and special characters like #,$,%,@
- There are also WebSites that will generate a random series of characters and numbers
- If you use a desktop, then it may be convenient to have the browser memorize the ID and the password functions. Generally, being able to memorize the ID is a function of the WebSite ("Remember me" and a check mark) and the memorization of the password is a function of the Browser and can be set up with its' settings.

  This is not a good idea if you use a laptop and you travel with it. With a loss or theft, the thief has access to everything. Password protecting the computer log-in can provide some additional protection when travelling. Windows Pro has this built in and Windows Home can be configured with a Password every time it boots or being paused (no activity) for a period of time.
- **An additional powerful** security layer that is increasingly being used by many WebSites (CRA, Banks, Amazon, PayPal) is **2 level authentication**. You still sign-in with your ID and Password, but you are then prompted 1) to send a Text message with a six digit code (to a cell phone) OR 2) a call to a land line phone; which you receive right away; and enter the code into a field on the log-in screen. The system confirms the number as being valid and logs you in.
  This is becoming more and more popular with time. It DOES require that you have entered your cell/home phone number into the profile for that site.
- Never disclose your passwords to anyone, especially online.
- Change your password at least twice a year, to help protect the security of your information.

PROTECT YOURSELF: Never send money to someone you have not met. If you suspect you are being scammed, HANG UP THE PHONE and contact the Canadian Anti-Fraud Centre at **1-888-495-8501** or Halton Regional Police Service Regional Fraud Unit 905-465-8741

Thanks to Marcus Miller / Gary Bridges