IN CASE YOU SUSPECT FRAUD

In the event that you suspect that you have been a victim of fraud, you should complete the following steps as soon as possible to protect yourself from any possible fallout.

1. If you've given remote access to your computer to someone you suspect of fraud, turn it off and contact your local computer repair shop of preference and book an appointment to have your computer scanned and cleaned.
2. Make notes about the interactions with the person who you suspect, including the details about what information that you gave to them and the date(s) it occurred.
3. Contact your local police non-emergency line and file a report.
4. Any identification numbers that you gave them (such as credit card numbers, Social Insurance Number, or Drivers License) you will have to call the respective companies or public offices and alert them of the possible fraud. They will likely issue you new numbers or accounts to help prevent possible fraud.
5. Call Equifax and TransUnion credit reporting agencies and put a fraud alert on your files.
6. Call the Canadian Anti-Fraud Centre and report the fraud to them as well.

CONTACT INFORMATION & USEFUL LINKS

MasterCard Canada - Lost or stolen cards
Tel: 1-800-307-7309

Visa Canada - Lost or stolen cards
Tel: 1-800-847-2911

Canadian Health Care Anti-Fraud Association
www.chcaa.org

Canadian Revenue Agency
www.cra-arc.gc.ca

RCMP Scams & Fraud
www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

RCMP Seniors Guidebook to Safety and Security
www.rcmp-grc.gc.ca/pubs/ccaps-spcca/seniors-aines-eng.htm

Canadian Anti-Fraud Centre
Tel: 1-888-495-8501
info@antifraudcentre.ca
www.antifraudcentre.ca

Internet Scambusters
www.scambusters.org

EquiFax Canada
Tel: 1-866-892-2595

TransUnion Canada
Tel: 1-800-663-9980

AlphaGeek COMPUTERS INC

Computer Fraud and you...

a condensed guide to

Safety and Security

Alpha Geek Computers Inc.
Craig Nobbs
604 - 372 - 4335 [GEEK]
Support @ AlphaGeekComputers.ca

AlphaGeek COMPUTERS INC

UNDERSTANDING

Before you can begin to protect yourself from being a victim of fraud, you must understand that the majority of fraud happens because the targets are coerced into feeling strong emotions. Fear and worry, excitement and elation, and often a sense of an impending deadline help create pressure on the victim to act hastily before having a chance to think things through or to talk to someone else about the situation. There are many different scams that are used and they're mostly just old scams that have been updated and adjusted for use with modern technology. Regardless of the type of scam that they're using, there are steps that you can take that will help protect you from becoming a victim.

DON'T BECOME A VICTIM

There are four steps to remember, practice, and use. These are true in most aspects of life and may be things that you already use in other areas of your life. Just remember to put these in to practice. They can save you from becoming a victim of fraud.

1. "*If it seems too good to be true, then it probably is.*" This time tested adage still rings true today.
2. *Be skeptical.* For many people, this can be difficult as they may be the trusting type. As difficult as it seems, remember that just like scams run over the telephone, you don't really know who you're communicating with. You can literally claim to be anyone, even a Nigerian prince.
3. *Do not rush in to anything.* A common regret for victims of fraud is that they rushed into it because of the pressure that they felt. Even if the victims are normally cautious, the tactics used can be extremely effective when the right emotions are touched by the scammer.
4. *If you're not sure, call someone who you trust.* Sometimes we find it difficult to ask for help. Often it's because we feel like we're wasting the persons time with a "dumb" question. You shouldn't feel that way because you don't know something. Just remember: *there is no shame in asking for help.*

PRACTICAL STEPS FOR PREVENTION

As well as the four previous steps to help keep you safe, there are also practical precautions that you can take. Most of these are fairly straight forward and don't require much experience to accomplish. That being said, if you don't know how to do something, remember step four from the last section: "*If you're not sure, call someone who you trust*". Below is a list of items that you can implement to help you keep safe.

1. *Install an antivirus and keep it up to date.* There are many free antivirus programs and some of them are actually really good. In fact, some of the free versions rate higher in detection, prevention, and removal than other companies' paid versions.
2. *Keep your operating system and programs up to date as well.* Make sure that you install Windows Updates when the notification pops up. You don't need to do them that very moment, but you shouldn't wait too long to install them. Also, other companies' products, such as Adobe, Apple, Oracle, and other Microsoft products should also be updated sooner rather than later when they notify you.
3. *Any email that has any outlandish claims is a scam.* Delete it and forget about it. Seriously. Over 50% of all email traffic on the internet is spam. While the vast majority of it is automatically filtered and never reaches its intended target, some of it will. In these cases, just remember the four previous steps and delete anything that seems fishy. Also, keep in mind that many scam emails pose as legitimate companies that you may deal with regularly. Don't click links in emails. Open your web browser and go to the website the way you normally would.
4. *Don't open email attachments from anyone unless you were expecting them.* This is one of the most common ways for people to get infected with malware and viruses. Malicious programs will send email from infected people using their contacts list. This makes it more believable and people are more likely to open attachments from people that they know.
5. *The internet lies… Don't trust it.* When browsing the internet, if a notice says that you have an infection but then requires that you download something to clean that infection, know now that it's a lie and it's trying to scam you. Closing your web browser or rebooting your computer will resolve this, so long as you didn't download what the popup was attempting to get you to download.
6. Your computer is like every other machine you own and it needs to be maintained. Just like your fridge or your vehicle, your computer needs to be maintained by a professional. Depending on which professional you ask as well as your usage of the computer, you should have it looked at every six to twelve months.