The Computer Store

The Computer Store, P.O. Box 6568, 9907 – 100 Ave., Peace River, AB, T8S 1S4 PH: 780-624-9221
http://www.thecomputerstore.ca

Tech Support Phone Scams and Fake Virus Alerts

Scams seem to be everywhere these days, from phone calls claiming to be from Microsoft or Windows Support to webpages with fake virus alerts that pop up alarmingly on your computer to the relatively new threats of ransomware. Sometimes just surfing can get a little frustrating.

Hopefully we can help.

Rule # 1 - NO LEGITIMATE COMPANY WILL EVER CALL YOU TO TELL YOU THAT YOU HAVE COMPUTER ISSUES.

Rule # 2 - NO LEGITIMATE ANTIVIRUS OR MALWARE COMPANY WILL HAVE A POP UP THAT ASKS YOU TO CALL A PHONE NUMBER FOR SUPPORT.

Regarding scam phone calls:

No legitimate company will ever call to let you know you are infected. Not Microsoft, not Norton, not anybody. You can safely assume that if you get a call warning you of issues on your computer that it is a scam. Just hang up, do not respond in any manner at all or have a conversation. Simply hang up.

Microsoft has a good link regarding these scams, here: https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

Regarding pop up virus warnings:

It's frightening when it happens. A page or windows pops up in front of you announcing that you are infected with a serious virus, many times accompanied by sirens, loud irritating sounds or voices. These scam warnings come in a variety of shapes and sizes but have some common characteristics. They may ask you to click a button to do a scan or to call a phone number – **DO NOT CLICK ANY BUTTONs. DO NOT CALL ANY PHONE NUMBER.**

The first thing to do is stop after the pop up is nothing. That's right, do absolutely nothing for a little bit. After this, take a moment and turn your speakers down or off and relax. So far, there is likely no harm done but there are now a few steps to take to minimize any possible damage. Again, in any case, **DO NOT CALL THE NUMBER** or click the button. Even if the warning appears to be from an Antivirus program that you have installed, if it has a phone number to call it is a scam.

And now, after you've calmed down it's time to proceed.

Turn off your computer even though the website specifically tells you not to.

Often, steps are taken by the scammers to make shutting the computer off more difficult. You may find that you cannot close the webpage. Or you may not be able to use the old reliable Ctrl-Alt-Delete process to bring up task manager and then shut down. You may also not be able to use the start button in the bottom left hand corner. No worries, on most laptops simply holding the power button down for 10 or so seconds will shut down your computer. On laptops, pulling the power plug will have no effect as the laptop will just switch to battery power. You may need to remove the battery although some new laptops do not have removable batteries.

On most desktop PCs holding in the power button for 10 seconds will do the same. If it does not, simply pull out the power plug. The reason you are told not to turn your computer off is that you probably won't be able to get back to their scary web page where they can continue to try to scam you. Remember, you likely got the "virus" page by clicking a Facebook link, or doing a Google search and landing on a hijacked or infected page. Many of these scammers will buy domains with names that are very close to popular pages in hopes that someone will misspell the page, or they will set up a page that contains terms that are popular in searches. For whatever reason you got to the page and now we have a little more work to do.

Restart the computer.

Do what you normally do to get to the Desktop but do not open up Internet Explorer, Chrome, Firefox or any web browser just yet.

If the infected page pops up on its own then you are infected and likely need more assistance from a qualified technician. In most cases however the page will not reappear on its own.

Now is the time to reopen the browser by following the instructions below.

In Windows 8 or Windows 10, go to the search and type in http://www.google.ca and then hit the enter button. This should open up your browser to the Google website. Then close the browser and re-open it. If it all looks normal you are likely all OK.

In Windows 7, click the start button in the bottom left corner and type in http://www.google.ca and then hit the enter button. This should open up your browser to the Google website. Then close the browser and re-open it. If it all looks normal you are likely all OK.

After you have opened your browser successfully and the infected or hijacked page has not come up again you are probably in the clear but it is a good idea to do the following:

1) **Protect and scan your computer with a reputable antivirus. If you need a free one for home use, the following are very good:**

Sophos Free and Bitdefender are available from our websites Free Software page at: http://www.thecomputerstore.ca/free-software.html

2) **Consider changing passwords on your accounts.**

This is a good thing to do once in a while in any case especially regarding accounts with financial information. These including banking sites, PayPal, eBay and your email accounts. Many people do not consider their email accounts but most financial sites use an email account to authourize changes so if a scammer or criminal has your email account and password they may have easy access to hijacking your other information.

3) **Ensure that you have good backups for your data**

Backups are always a good idea. All hard drives will fail given time. They are like tires on a car; some will last quite a while and others will fail sooner. But when they do, your data including your pictures and important documents is likely gone. And a backup means keeping your data in a minimum of two places. Often we hear from our clients, after the fact unfortunately, that they copied all of their documents and pictures, music etc. to an external drive and then deleted it from the computer to make space on the hard drive. Once the original data is deleted, just like when you use your spare tire, you no longer have a backup. If the external drive fails which, given enough time, it will then your data is gone. You need to keep the data in two or more places.

What can happen if you call and allow access: We cannot stress the importance of not calling the number enough. Once a scammer accesses your computer, they can a) encrypt your data and hold it ransom holding your important documents and pictures as hostage for large money demands, b) encrypt and password lock you or anyone else out of your computer gain to hold your data hostage, c) scan your computer in the background for email and online account information and passwords which may put you at risk for identity theft and financial losses and, at a minimum, charge you exorbitant amounts to clean up the computer that they infected solve non-existent problems.

A new scam has started up with some of these scammers. It's called a refund scam.

After they have called and worked on your computer they will call back and say that they made a mistake and need to refund money to you, then they ask for your bank information or your PayPal information and then take more of your money. Click the link below for some first-hand reports:

See https://reportscam.com/computer-tech-helpcom/

Again, DO NOT CALL ANY PHONE NUMBERS FROM POP UPS and DO NOT CLICK ANY POP UP BUTTONs.

If you are reading this after you have already called a number and they have already accessed your computer or you have paid the scammers then **call a qualified technician for assistance**. The scammers may have left software on your system allowing them to record your keystrokes or to access your computer any time they wish to gather other data, and, it is a good idea to also call your bank or financial institution to ask for assistance in protecting your accounts.

Please share this information with your friends to help them stay protected.

For more information on keeping your computers and data safe, or if you need assistance with these instructions, call us anytime at 780-624-9221.

We have options available to protect home users and businesses from data loss and we have continuity options to keep you or your business up and running in the event of computer failures or ransomware events.