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

Ransomware – Protect yourself

What is ransomware?

Ransomware is software that prevents you from accessing your data, usually by encrypting your data and in some cases password locking and encrypting both your computer and data. Without access to the "key" to unlock the system and/or the data it is unusable to you. The criminals then demand a large amount of money to provide you with the "key" to give you access to your own data.

The criminals keep themselves safe by demanding that the payment be paid using untraceable methods such as cryptocurrencies including Bitcoin and others or Ukash and other variants.

More information on Ukash and cryptocurrencies and Bitcoin can be found here: https://en.wikipedia.org/wiki/Ukash, https://en.wikipedia.org/wiki/Cryptocurrency , https://en.wikipedia.org/wiki/Bitcoin

It needs to be noted that, even if the ransom is paid, that you may not get your data back. Many victims have paid and received nothing in return.

So, the best method of defense against ransomware is to protect your computer and data before you are infected.

The first step is not to get infected.

Many ransomware attacks come from scam emails that pretend to be from someone you know, a reputable business or shipping companies such as FedEx, Purolator or the Post Office. These emails will usually have a link to click on, or an attachment to open. They also have a comment, the bait, that seems to make it important to click, An example might be something like "You have not applied for your refund" or "Tracking number for your gift" or they may be as simple as getting an email from a friend that says "You'll love this, funny" with a link attached. Be very careful clicking on any links or documents on emails you are not expecting. Even if you are expecting a shipment or gift, be very careful clicking on the links. In many cases, you can out the mouse arrow or cursor over the link without clicking and it will show where the link goes to. If it says anything different that the official site do not click.

Attachments are an issue because, if your computer is set up to hide common file extension, which many are, then you could possible see a file that ends in .pdf but actually ends in .exe, .bat or .com or other executable which, when clicked, will activate the infected payload.

Another source is redirected, hijacked or phony websites. These can be websites with names that are very close to common sites. The scammers will register a site that is on letter off of the legitimate site (think www.gogle.com not google.com – not an actual infected example) so be careful when typing domain names. Also in some cases legitimate sites have been hijacked an infected by the criminals.

Unfortunately, in many of these cases, you won't know if you have been infected until you attempt to open a document or view a picture at which time you will likely see a text file open or in the folder explaining that you are infected and must pay the ransom. Which takes us to our next step.

Protect and scan your computer with a reputable antivirus.

I'm still surprised by the number of people who tell me that "I don't have an antivirus on my computer because I'm careful and don't need one" or "I've never been infected so I don't need one." Again, to use a familiar analogy, that would be like driving without a spare tire because you've never had a flat. It's only a matter of time. For home users there's really no good reason to go without an antivirus program as there are a number of very high quality free programs available.

If you need a free one for home use, Sophos Free and Bitdefender Free are available from our website's Free Software page at: http://www.thecomputerstore.ca/free-software.html

For businesses, many very good programs cost less than $50.00 to protect 3 PCs. That's pretty good low cost insurance in my opinion. Call us for commercial options.

And now, when it comes to ransomware as well as computer and hard drive failure, perhaps the most important step in protecting yourself.

Ensure that you have good backups for your data.

Backups are always a good idea fi you have data that matters. All hard drives (and computers) 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, to be very specific, a backup means keeping your data in a minimum of two places. On your computer and on a separate backup device or fi the data is off your computer and on an external storage medium or device that you have two copies.

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.

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

For ransomware, the backup needs to be kept separate and inaccessible to the ransomware. Unfortunately this means that attached external hard drives are not the best answer, un less you are prepared to do some manual tasks to ensure air-gapping as some forms of ransomware will propagate to connected drives and networked shared folders, encrypting the data on the backup also.

Air gapping means attaching and reattaching the external drive before and after the backup process is completed to keep it disconnected when the source is infected. Our experience with the air gapping process is that it usually doesn't work because of human issues; the user forgets to disconnect the drive after the backup or forgets to connect it prior to the backup or, after a while the whole process is ignored completely.

Which brings us to cloud storage options.

These work very well for data backup, and protect very well against ransomware, but which one is the best option for you is not as simple as it appears. Some determining factors include what kind of data is being protected, is the data personal or medical, are my files large or small, and are there file types that are not included in the protection, do I need to protect the whole computer or just some areas, do I need redundancy as well as backup etc.? Please call us if you need these questions answered. We'll be happy to help.

Backups for business also need to take in to consideration the amount of time that you can keep running the business without having access to the affected data.

If all of your data is on a shared drive or server you need to ask yourself "What would happen if the server or shared folder was corrupted or encrypted?" "How long would it take to rebuild or recover the data and get everyone connected?" "Will my Point of Sale (POS) system function if the server failed?"

Options are available for home and business users to resolve and mitigate these issues but which options are best for you or your can only be answered after a few questions are asked.

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

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 instruction, call us anytime at 780-624-9221 or drop by for a discussion. 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. Call us for details.