Planetrehab Ransomware Bulletin
Friday, August 25th, 2017

Lately there has been a sharp rise in advanced computer virus programs called ransomware, also sometimes referred to as cryptoware. Ransomware has quickly become the most prevalent of the viruses spread in the tech world. Search the term ransomware and you will find numerous articles about its destructiveness. Ransomware locks and/or changes a user's files by encrypting them so the user cannot access those files until a ransom is paid. Once the ransom is paid, the user gets a key to decrypt their files. It is nearly impossible to recover the user's data once it has been encrypted unless the user has a backup and/or a restore point on their system. Virus protection software is virtually useless because ransomware creators are far ahead of virus protection software creators.

The way almost all infections happen is via email attachments that a user opens. The user gets an email that looks legitimate and opens the attachment. Often the attachment is disguised as Fed Ex or DHL shipping documents or invoices that appear real. Once the attachment is opened, the infection happens and there is no reversing it. Again, once a computer is infected (encrypted), it cannot be cleaned without the decryption key. Keep in mind, reputable companies will not send unsolicited emails with attachments. If you get an email from someone or a company that you do not know or did not ask for, be very skeptical.

Another way ransomware is distributed is via a link on a website, which is prevalent on Facebook and other social networking sites. If you click on a link on a webpage and are prompted to download a file, do not do so unless you are positive you want to download the file. And always choose the Save option and not the Run option. Saving the download gives you an opportunity to research and evaluate the downloaded file and gives your virus protection software a chance to scan the file. Again, do not agree if prompted to install anything unless you are sure the file is safe and you want to install the software. Remember, these viruses spread through trickery, so do not fall for their tricks. Do not blindly click on email attachments and/or suspicious links.

So, how do you protect yourself from ransomware?

1. The absolute best protection is to do regular backups of your critical data. Daily backups are necessary due to this increased threat.
2. Do not open attachments in email messages that you are not positive are safe. If you are unsure, do not open it. You should only open email attachments if you are expecting the attachment. If you get an unexpected email from someone you trust that has an attachment, contact the person that sent it to you BEFORE opening it to verify it is legitimate.
3. Do not agree to install any software that you are not expecting. Only install software that you are sure is virus free.
4. Keep your operating system up to date.
5. If you are a victim of ransomware, your best option is to restore from a backup or a restore point. The next option is to clean your computer and abandon your files. This is painful, but you must clean your computer before proceeding. The last option is to pay the ransom to be able to decrypt your files. All the experts strongly recommend that you do NOT pay the ransom. You are not guaranteed to receive the decryption key and it could possibly make you a future target. Also, do not fall for companies claiming they can decrypt your files for a nominal cost—they cannot.

We have configured Planetrehab in such a way that it is virtually immune from ransomware. Even if your computer is infected with ransomware, it will not affect your Planetrehab data. For Planetrehab users that are using the server version, your Planetrehab data is protected, but other files will not be protected. Any scanned

documents and Planetrehab formatted templates may be unprotected. That is why we urge all server version users to **regularly backup their scanned files directory and their pr_templates directory**.

Additionally, for all server version users, over the next week, to protect your data and server, we will be removing the internet browser from your server. After we remove the browser, you will not be able to access the internet via the browser. If you need to discuss this change, please call us at 800-982-5447 ext. 314 or by email at info@planetrehab.com.