You are receiving this newsflash because of the critical nature of this topic! The regular quarterly issue of the Running Computer newsletter will go out in June.
~ Julia Olson

Running Computers

Keeping your Technology Up and Running!

www.runningcomputers.net

Special Edition
April 2015

Important information regarding "Ransomware"

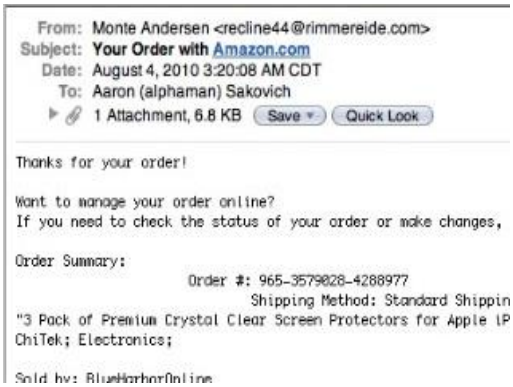
"Ransomware" You may have heard the term on the news lately, but wondered "what is this new virus threat?" "Ransomware" is more than a new virus and more than a threat.

"Ransomware" is a blanket term for a number of viruses that can hijack your computer. At worst, it can make the pictures and documents on your computer inaccessible. They are held hostage until you pay the stipulated ransom and the perpetrators undo the damage.

"Ransomware" CANNOT undone by conventional security software. There is no way to fix your computer once the virus has encrypted your documents and photos. The only way to counteract this threat to your technology is prevention, quick response, and a reliable offsite backup.

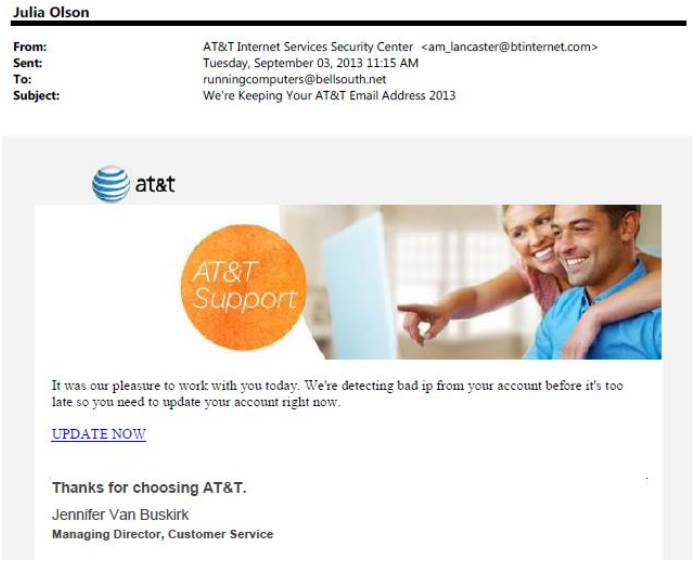
Prevention: Know the virus entry points and be careful.

1. **Email** Attachments: NEVER click on an attachment without verifying that the email is legitimate. Infected email most often looks EXACTLY like a missed delivery notice from FedEx, UPS, or the Post Office – official logos and all. (See the UPS example below.)
2. **Email Hyperlinks:** NEVER respond to an email that asks you to click on a link to "update" your information. This is called PHISHING. (See ATT example below.)
3. **Pop-Up Windows:** These may appear on the web or the desktop with a warning that you are infected and need to do something immediately. Don't even click on the X to close it!



The Amazon, UPS and ATT emails shown here are FAKE! They are actual PHISHING emails – they just used real company logos!

You'll notice that the grammar is slightly off in the text, and check out the bogus email addresses!



Response: Know what to do if you suspect you are already infected. Immediately turn the computer OFF with a hard shut down – press and hold the power button until the computer is off, usually 15-20 seconds. While not normally a recommended method of shutting down, this stops all activity immediately.

Disconnect the computer from your home network or your modem. Unplug the Ethernet cord or remove the wireless USB adapter.

Call a qualified professional to assess damage. DO NOT turn the computer back on.

The best thing you can do to protect yourself from "ransomware" is backup your computer using **Offsite Backup.**

If you are backing up with a local external drive, plugged in via USB, you may not be protected. If the virus occurs when the backup drive is connected, your external drive will be corrupted as well. A better backup option is a Cloud backup solution.

I recommend **CARBONITE**. At $60/year, it is a very affordable option for your peace of mind. Look at options on my website, www.runningcomputers.net, Carbonite Cloud Backup.