Ransomware: What you need to know

Global cyber chaos was spreading Monday, May 8th, as companies booted up computers at work following the weekend's worldwide ransomware cyberattack.

The extortion scheme created chaos in 150 countries and could wreak even greater havoc as more malicious variations appear. The initial attack, known as "WannaCry," paralyzed computers running Britain's hospital network, Germany's national railway, and scores of other companies and government agencies around the world.

PLEASE take this very seriously.

DON'T click on things you don't recognize.

CHECK the subject line. "Hi, this is funny" should make you suspicious.

WATCH out for messages from places like Pay Pal or Amazon that say things like "Your receipt is attached". "I don't remember buying anything, I better check this" **WRONG MOVE**. They will ask for personal info or ask you to download something. **IF** you don't remember purchasing anything, you probably didn't. **DON'T** go there! Contact them through **their** channels if you are still in doubt.

CHECK the email address of the sender, if you don't recognize it, **DELETE** the message. **DON'T** click on any attachments. **DON'T** download anything.

If the email is from someone you do know, check the address. Just because it says it comes from a friend doesn't mean the address is real. **Ask** the sender if they sent the message. **DON'T** forward the email! **DON'T** reply to the email, send a **FRESH** message to the friend using the address you usually use.

Keep your anti-virus software up to date!

Check for, and install, updates to your computer **NOW ! NOT LATER. NOW**

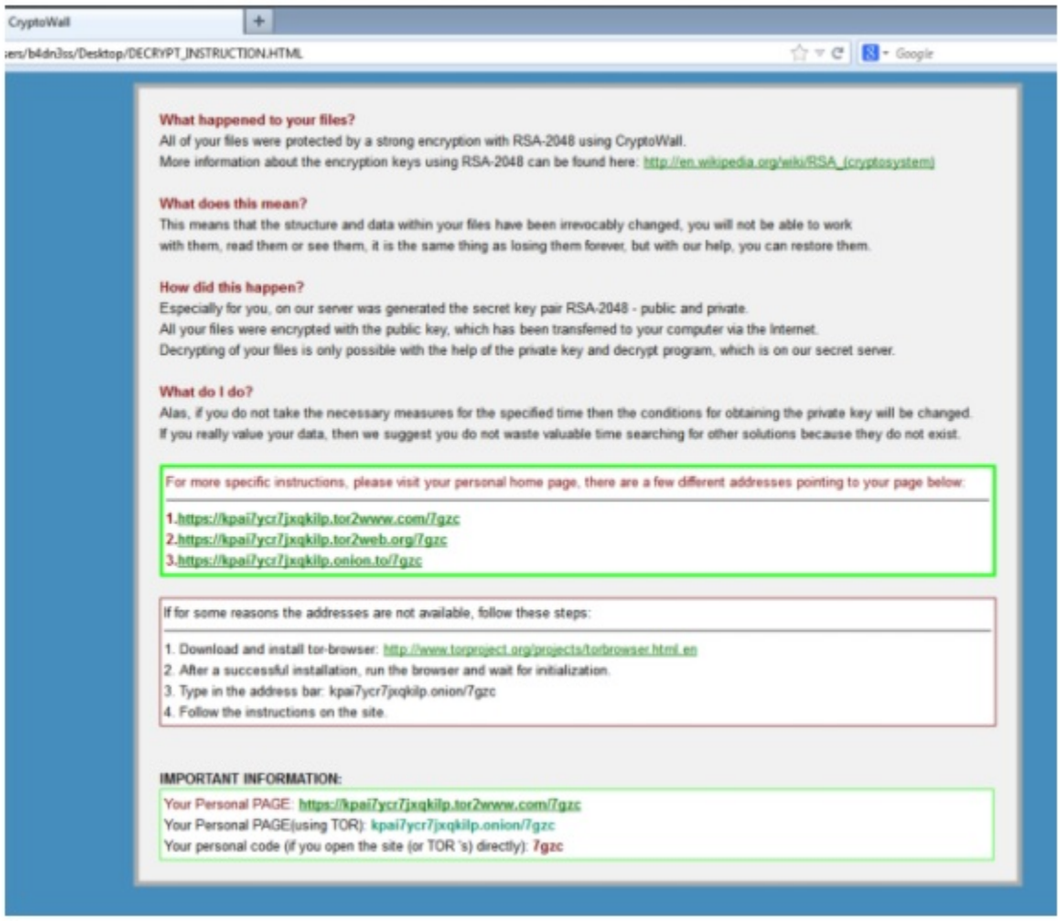
Russ Pastuch
Chair, Communications Committee

What is ransomware?

Ransomware is a form of malware or malicious software. It seeks out files on your computer and locks them to make them inaccessible to you. Cybercriminals demand money — a ransom — to unlock your files.

Some kinds of ransomware do that by encrypting the files. When you try to open the encrypted files, a warning pops up, demanding a ransom in return for a decryption code or key.

Most often, the files targeted by ransomware are photos, videos and business records like spreadsheets, documents and presentations — anything likely to be valuable to a person, family or business.



Firms are sent this encryption notice after hackers use CryptoWall ransomware to take files hostage and demand a ransom payment. (phishme.com)

Are files stolen from my computer?
No. The files remain on your computer and are not usually accessed. The cybercriminal is not looking for banking or other records. They want a ransom, not your files.

How much is the ransom?
As with any criminal enterprise, as much as the criminals think they can get. Typically, in North America, that’s $500 US, but paid in the untraceable cybercurrency bitcoins. If you don’t have any bitcoins, the ransom instructions explain how to get it. If a business, especially a larger one, is the target — the ransom can grow. The largest publicly recorded ransom demand was $800,000. Often, there is a time limit — typically 12 hours — before the ransom doubles.

How does your computer become infected?
Your computer is typically infected with malware such as ransomware when you open an attachment to an email or download software or apps. Such emails and software can appear legitimate enough to fool many users.

Is it just PCs?
The target is predominantly Windows-based computers and, increasingly, Android phones. But a number of tech security experts told CBC News that Apple devices are expected to become a much bigger target this year. Ransomware typically seeks files written in English, but has expanded to other major languages, including French, Spanish and Arabic.

How can you protect yourself from ransomware?
As with anything else, ensure you have virus protection and that it is up to date. Missing even one daily update can make you vulnerable because the type of malware keeps changing. Don’t open attachments or download software (often free programs or games to your computer or phone) that you can’t be sure are safe.

It's also a good idea to back up all your files on a hard drive that is not connected to your computer so that you have a clean and accessible copy of your files if your computer does become infected.

What should you do if you become infected?
You can’t remove the malware without destroying the infected files. If you have those files externally backed up, you or a computer technician can remove the files and the malware, and reinstall uninfected files from the backup. Of course, you shouldn't connect your external backup to your computer until the malware has been removed, or it could become infected too.

What if you haven't backed up your files? Should you pay the ransom?
If you pay the ransom, you will regain access to your files. But this may not remove the malware itself. There have been numerous instances of computers becoming reinfected.

As a result, some technicians recommend wiping your system and changing your IP address.

Also, remember that if you pay, you are funding a criminal enterprise and encouraging more attacks.

What happens if you pay the ransom?
If you pay the ransom, the cybercriminal provides a code, which triggers the decryption process. That can take days or weeks. Once files are decrypted, you'll be able to access them again.

If your computer is infected with ransomware, who should you report that to?
Police say if you have not paid the ransom, you can report the incident to the Canadian Anti-Fraud Centre at 1-888-495-8501, or by email to **info@antifraudcentre.ca**. If you have paid the ransom, you can report the crime to your local police force.

The content is courtesy of the CBC.

For more go to http://www.cbc.ca/news/technology/global-ransomware-cyberattack-1.4115065