Beware Of WannaCry Ransomware

On Friday, May 12, an unprecedented Trojan virus spread like wildfire through the internet, creating enormous damage and loss.

The WannaCry ransomware attacked 57,000 computers in more than 150 countries in less than a day.

As its name implies, ransomware works by holding a victim's data under "ransom." The virus encrypts the files on an infected computer and holds those files hostage unless the victim pays a ransom, in which case the files are promised to be returned, unharmed.

The WannaCry virus demands a payment of $300 in exchange for decrypting infected files. If the victim doesn't cough up the money within three days, though, the ransom doubles to $600. If a full week goes by without payment, WannaCry deletes all of the files and they are gone forever.

On Saturday, 22-year-old security researcher Marcus Hutchins became an instant hero when he registered a domain name within the virus' code in an attempt to track its spread, unintentionally slowing its progress.

Unfortunately, though, Hutchins's actions did not completely halt the virus. By Monday morning, more than 200,000 systems across the globe were reportedly infected. European countries were hit the hardest. Many large companies were forced to close their doors for several days, as were banks, hospitals and government agencies.

As of now, no one is sure who's behind the virus. However, most experts believe a group known as "The Equation Group" is utilizing a code written by the National Security Agency to exploit flaws in Microsoft Windows and create the virus.

There is no fix for WannaCry, though cyber-security experts are hard at work trying to decrypt infected files. If your computer is infected, it's best not to pay the ransom. Instead, restore backup files to your computer or seek help from a professional who specializes in restoring lost data. Paying the ransom doesn't guarantee the return of your files, and it encourages attackers to infect your computer again.

As always, the best way to protect yourself is to be proactive. Here are 5 steps you can take to keep your computer safe from WannaCry and other ransomware:

1.) Create a backup of your files

If you haven't already done so, invest in an external hard drive and get into the habit of making regular backups of your data. This will protect your files in case anything happens to your computer, saving you lots of time, money and stress.

You can also subscribe to a cloud backup service and regularly upload your most important data. There are multiple free cloud services you can use, such as Google Drive, Apple iCloud or Dropbox. All of them will store your valuable data (to a size limit) without charging you a penny.

2.) Patch your Windows with Microsoft's fix

Upon discovering that WannaCry spread through a weakness in Microsoft Windows, the software giant released a fix for the vulnerability. Protect your computer from this virus and other ransomware by using the fix to strengthen your computer's code.

3.) Update your operating system

While the discovered weakness in Windows now has an appropriate band-aid, no one knows if there are any other flaws that can be exploited for another virus. It's important to update your OS to the most recent version, preferably to Windows 10, as soon as possible. The more updated your software, the less likely it is that it contains vulnerabilities that can be abused.

4.) Use a firewall

A strong firewall will prevent ransomware from accessing your computer and will guard your online activity. No program or malware will be able to enter your system without your full consent.

Since malware is always evolving, it's important to update your firewall on a regular basis to ensure protection from the most recent viruses and malware. You can purchase your own firewall or utilize available security measures offered by Windows, being sure to check regularly for updated versions.

5.) Avoid suspicious websites and emails

It's too easy for hackers to infect your computer. All they need is for you to click on a flashing banner ad on your favorite shopping site and – oops! Malware is installed and it now has access to your entire computer and all your files.

Alternatively, following a link on a random email can infect your computer and destroy all your data. When browsing and checking your emails, always be on guard. Never visit suspicious-looking sites or click on any ads that look shady. Don't download anything you can't explain, and never click on links found in emails from people or companies you're not familiar with. A little bit of caution goes a long way toward protecting your computer.

No one knows when WannaCry will stop circulating the web, but it always pays to be careful. Once you're infected, restoring your data can be stressful, time-consuming, and costly. Taking steps to protect yourself, though, is painless and simple. By implementing the ideas detailed above, you'll help keep your computer safe from this and any other ransomwares looking to make a buck off your carelessness. Better to be smart and safe than sloppy and sorry!

SOURCES*:

http://bgr.com/2017/05/15/wanna-cry-ransomware-virus-windows-wannacry-explainer/

http://money.cnn.com/2017/05/13/technology/ransomware-attack-protect-yourself/

https://www.google.com/amp/s/www.purevpn.com/blog/how-to-protect-from-ransomware/amp/

https://www.google.com/amp/www.bbc.co.uk/news/amp/39920141

https://www.google.com/amp/amp.usatoday.com/story/101690214/

This article is for you complements of MembersAlliance Credit Union – 5/31/17

Please feel free to share!

MembersAlliance
CREDIT UNION
You can rely on us!

2550 S. Alpine Rd. Rockford, IL 61108 – Phone 815-226-2260

https://www.membersalliance.org/

* The contents of the external links contained within are for your informational purposes only and do not necessarily reflect the views of MembersAlliance Credit Union.