

Spread the word with daily online safety and preparedness tips on Google+, Facebook and Twitter. Use the following blog, or create your own, and post all throughout the month. Remember to include the hashtags **#COReady #cyberaware**

### Title: It’s Time to Talk Cyber Security

CryptoWall is a nasty threat known as Ransomware. You can't make this stuff up. Cybercriminals have figured out how to lock us out of our own computers, considering that some of us might pay a pretty penny to be able to get back in.

You might ask how they can keep you from getting to your files. Good question. It's kind of like when you were a kid and a much bigger kid took your lunch box and you knew there was no way you could take it back. It’s the same thing here, but with no teacher to help.

### Cybercriminals at Work

Remember when you clicked on the link to that cute little cat video you just had to see? That link was a lure sent by a cybercriminal. Clicking on that link set off a very painful chain of events. While you were watching an innocent video, malware was downloading onto your computer in the background. This is what the malware did:

1. It encrypted your files on your hard drive (scrambled the information so you can't make sense of or use it).
2. It sent a message back to the cyber criminal’s computer letting them know that you clicked on the link.
3. It established a few new accounts in the cloud on behalf of the cybercriminal. More specifically a short lived "bit coin" account and a short lived email address. (I will explain bit coin in a minute)
4. Your ransom time clock started.
5. The ransom price was set.
6. A message was posted on your screen that explained that your computer has been locked, that you have a ransom price to pay ($500 or more) for a magic key to unlock the computer and a deadline by which to pay it. Cool right? Back is good? Think again.

### What is Bit Coin?

Cybercriminals don't take checks, cash or credit cards. We have all seen the movies where the good guys follow the money and arrest the bad guys. Apparently the cybercriminals have seen those too. So they use a "bit coin." So what is bit coin? Bit coin is a way to convert real money into digital currency. You will be asked to set up a bit coin account, dig out your credit card and deposit your US dollars at the appropriate amount to equal the price of your data in bit coin. Don't worry; the site will do the math for you (how nice). Poof! All those bit coin and email accounts, and your money, are gone.

You will get the key and instructions on how to use it to free up your data, but sadly the magic key doesn’t always work. Sometimes folks have waited too long or made a mistake when using the key. Sometimes the key wasn’t really magical. You may be given one more chance to use the magic key, but there is no guarantee that the key will work the second time. The reality hits you that your data is gone, permanently. These folks are very clever cybercriminals. You can't trace the accounts and you won't get a refund even if the key doesn't work.

### What can you do?

You can file a complaint with the Internet Crime Complaint Center (IC3) at <http://www.ic3.gov/default.aspx>. The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center. By filing a complaint, they are able to track cybercrime trends.

If you have been unfortunate to have been hit by this nasty dilemma, there is a small glimmer of hope to regain access to your files. There is a chance that you have a way back to the land of the free and unencrypted.

First, it is important to know that CryptoWall actually creates an encrypted copy of your files and then deletes the originals. If you have been backing up your files regularly (hint, hint), you can use a Cryptowall malware removal tool and then restore your backup files. Most antivirus vendors, like Norton, Kaspersky or McAfee, can help you with that. Second if you are using the Windows operating system, and statistics say most of you are, you can use the restore feature (again hint:hint) to restore files to a previous version. There are more technical means to recover the deleted data but in any instance it may be worth calling an expert if your files are important.

I know this is just one of many threats we all face when we live in the cyber world. The doctors always tell us to exercise, eat right and wash our hands. In the cyber world, good cyber hygiene is just what the doctor ordered <http://www.staysafeonline.org/> . Remember, home computers are not the only thing that cybercriminals are after these days. Your cell phone, tablet and other online devices like gaming systems and even digital home security systems can be targeted by cybercriminals. Get yourself trained to be cyber secure!

### Related Articles

* <https://www.nytimes.com/2017/02/01/technology/personaltech/stop-hijacking-home-devices.html?rref=collection%2Ftimestopic%2FComputer%20Security%20(Cybersecurity)&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=8&pgtype=collection>
* <http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html?emc=edit_th_20150104&nl=todaysheadlines&nlid=68349526&_r=0>
* <http://www.nbcnews.com/tech/security/virus-wipes-out-new-hampshire-police-departments-computers-n126466>

*This is article is intended to provide awareness level information and is not meant to provide a how to reference for any topics covered. The mention of any private entity does not imply endorsement of a product or company. For technical assistance it is recommended that readers seek professional services.*

For more tips and preparedness information, follow us:  
On Twitter: [@READYColorado](http://www.twitter.com/readycolorado)  
Facebook: [www.Facebook.com/READYColorado](http://www.Facebook.com/READYColorado)  
Google +: [READYColorado](https://plus.google.com/100167075139424077484)  
YouTube: [www.YouTube.com/READYColorado](http://www.YouTube.com/READYColorado)