Protect yourself from Cyber Threats

Protect yourself from Cyber Threats | Tech Tips Podcast by PcCG

Subscribe via Itunes [1] | Subscribe via RSS [1]

CryptoLocker, Game Over Zeus and heartbleed have made 2013 and 2014 difficult years for the average Joe computer user. These viruses and exploits are serious, much more than most.

Typical viruses are more of a nuisance than a threat. They might cost you some money to get the virus cleaned up, but usually the worst that happens is windows needs to be reloaded – you may lose a program or two. That isn’t the case with these nasty guys.

CryptoLocker and GameOver Zeus are both actually the work of the same Russian cyber-gang. Agencies across the world, including the FBI, are on the hut for them; including Evginiy Bogachev reported mastermind of the viruses.

Game Over Zeus [2] can actually obtain banking information and transfer money from your bank account to the “hacker’s” bank account. To prevent this, you must change your password. Already the virus has stolen millions of dollars through these transfers. It’s causing a lot of alarm because unlike most viruses – it really can steal your money.

You MUST take the time to learn at least a little about the world you use on a daily basis. By taking just 15 minutes out of your day to review this article the average “Joe” on the internet will be far better off.

Exploits, Updates and Changing your Password

Heartblead is a flaw in software, not a virus. Bad guys often try to exploit flaws in order to gain control of systems or obtain information. This is why those annoying updates are so frequent – they fix flaws found in various software applications. Most critical in my opinion are Windows itself, Java and Adobe (Flash/Reader). It is possible that updates cause their own problems, but it's the lesser evil in my opinion.

The flaw in heartbleed allows hackers to possibly obtain passwords stored on a server – something completely out of the user’s control. If your information was compromised the only solution is changing your password.

Given all the security threats lately – it’s critical to change ALL your online passwords. If you read this, and don’t change your passwords – don’t act surprised if your email or bank accounts get hacked within the next year. – Trust me, I know it’s annoying, but is it worth risking your assets, email and facebook over a few minutes of changing passwords? We have an article for suggestions on creating strong passwords [3].

Being informed, smart internet users is key! Use your head!

It is becoming increasingly critical for everyday casual internet users to be at least a little informed about what is going on and how to prevent it. Believe it or not, almost zero viruses “automatically” jump from computer to computer. In nearly all cases the virus infects the computer as a result of the user clicking on something they shouldn’t have.

This essentially means that the majority of viruses are completely preventable if users simply knew what to avoid clicking on! That however is a topic that is difficult to cover primarily because the “bad guys” are constantly changing tactics. However some common sense goes a long way.

For example, several of our customers (as well as millions of people across the country) have received fake calls claiming to be representatives of Microsoft [4]. They claim to have found an infection on the user’s home computer and that they will be happy to assist in the removal of the infection. Users then grant the “bad guys” access to the computer! This gives them the opportunity to install virus-like software and/or extort the user for money, claiming to clean up something that really isn’t there.

What flags went up in this situation?

1. Microsoft is a company that has millions, likely hundreds of millions of computers installed with their operating system (Windows). They are certainly not interested in taking the time and tracking down every person that has a virus on their computer. This is WAY too time-intensive and just doesn’t make sense.
2. Microsoft is not going to clean up your computer for free.
3. How did “Microsoft” magically get your number?
4. Why is "Microsoft" watching your computer?

Now you might be thinking “well somehow they knew I had a computer and that it was acting weird lately.” However statistically we can assume that over 70% of homes in America have Windows computers, and of those 50% of them are going to at least feel like the computer is running slow. You can see how the odds are in the favor of the attacker!

Now that you know this however, you can use such information to prevent this and other similar attacks.

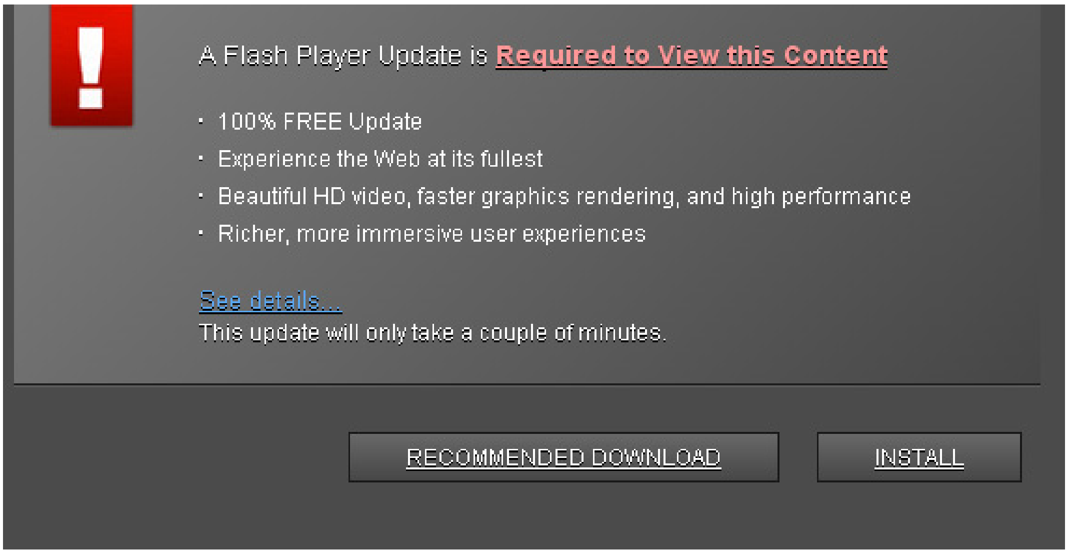
The key is to be smart, without being paranoid. You wouldn’t walk down a dark alley in a bad neighborhood at night would you? And you don’t have to be a security expert to know that’s a bad idea. I’m advocating the same “general common sense” with regard to computers.

If you receive an email with an attachment (the most common way viruses are transmitted), don’t open it right away, EVEN IF IT’S FROM SOMEONE YOU KNOW! Ask yourself if this attachment and email is likely to be real or fake? Did Sally say she was going to email you some pictures? If so - then it's most likely legit. But if you receive a tracking email from "UPS" that requires you download and open a zip file, something is wrong; even if you are expecting a UPS shipment! Again, statistics and random probability dictate at least some people receiving a message sent to thousands will actually be waiting for a UPS package.

Most viruses come in .zip or .exe format. If you get one of these, your guard should go up a bit.

If you are in doubt, simply call or email the person or company and ask them if they sent you the attachment before opening it. And obviously, don't trust phone numbers provided in the same email that may be a hoax if it's a company. Contact the company directly by googling their number or finding it some other way.

Banners, Updates and Lies (Real or Fake)



A Flash Player Update is Required to View this Content

- 100% FREE Update
- Experience the Web at its fullest
- Beautiful HD video, faster graphics rendering, and high performance
- Richer, more immersive user experiences

See details...
This update will only take a couple of minutes.

Don’t believe every banner you run across on the internet. This is another common way people get infections on their computers. A banner or flash advertisement claims your computer is running slow and they can fix it. But, how the hell do they know your computer is running slow? By going to a website are you giving the website permission to scan and analyze your whole computer? Of course not! (That is of course unless you are running outdated software that is susceptible to exploits! – hint hint – UPDATE).

AHA! But there’s a catch. MANY of these scams and fake ads, claim that you need to update!

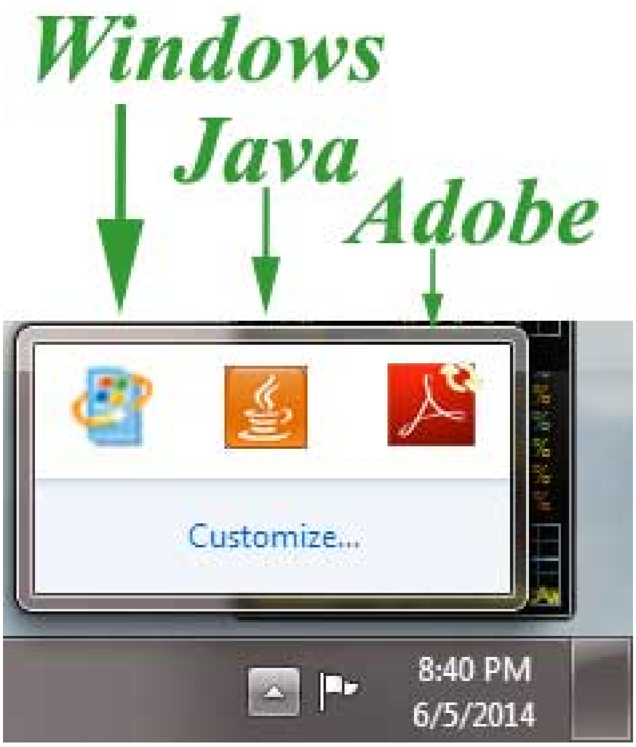
So, if the ad is telling you to update, and the computer guy told you to update, you should click on it right? WRONG! Why are you clicking on random messages popping up on your computer?! Do you trust the source of the message? If not, then don’t let them install ANYTHING on your computer!

Eeeeek!! So don’t update?

Nope! That’s not the solution either.

The solution is to update from sources that you know are legitimate, and avoid those that are not.

While this is not 100% foolproof, the advice I give to my clients is this…



If you get a message about updating, AND ALL of your web browsers are closed, then the message is probably legit.

This means there is no Internet Explorer, Chrome or firefox windows open at all. There should be 0 of them. If the message is still there with certainty that all browsers are closed, then it’s probably legit.

Usually these legit messages will pop up down in the lower right next to your clock. Typically you should see Adobe, Java and Windows popping up messages down there.

However do understand that bad guys COULD get down there! So that’s why I say it’s PROBABLY legit.

You might be thinking “well, that sounds like too much work, I just won’t update”. Just remember, that leaves you susceptible to exploits – software that is flawed that hackers know about and will try to use.

If you’ve made it this far in the article you are doing great. We’re almost done, and YOU are going to be better off on the internet for it.

Being safe and well protected going forward

The last two important things to highlight are my pinnacles of good computing… GOOD AntiVirus and Backup.

Antivirus

Most antivirus software suites are good enough. Some are better than others. Don’t marry your security suite, and price shouldn’t be your primary concern with it. Having a cheap antivirus that doesn’t do its job is pointless, isn’t it?

We recommend avoiding are McAfee and Windows Security Essentials.

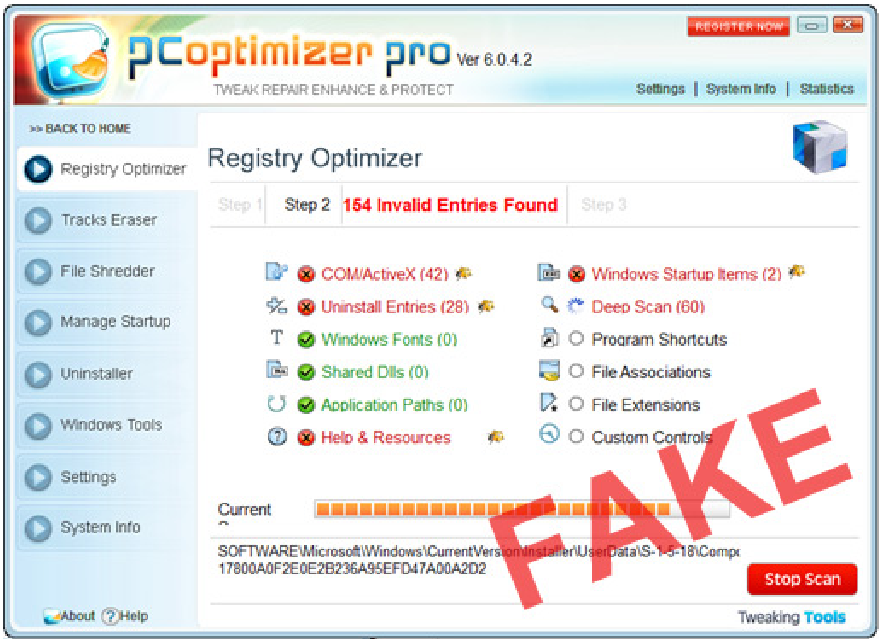
We encourage use of are Norton Internet Security, or Free BitDefender. Yes - we said Norton. If your reaction was "I used it a long time ago and it was terrible", then your reaction is most like from more than 5 years ago (a life-time in software). It was awful. It's not anymore. One day it may be again but as of 2014, it's good for MOST people.

Please understand that NO antivirus is 100%. The ones we recommend are lightweight and pretty effective, but not necessarily the MOST effective. Saying which AntiVirus is best is like saying which car is best... which should be impossible because a ton of questions follows such as “what do you want to use it for?”. We feel Norton and BitDefender (if you refuse to pay for one) are good all-around.

BACKUP

Once you have a good Anti-Virus you then need to think about backup. If you are NOT backing up your data, you are saying “I don’t care if I lose it.” For some people, they truly don’t! If it’s just used for facebook and checking email through Chrome, then that’s fine. But you must honestly assess that need for your information yourself. If you don’t want to lose it, BACK IT UP, and PLEASE, use a backup system. Spend a little money and get something that will work well. We use Acronis True Image, [5] but Carbonite [6] or a number of other options are good as well. Do not just “copy the files onto an external drive.” I had a client who did this… and all of his files on the external drive got encrypted as well – rendering his backup pointless. There are free backup solutions I’ve heard good things about but have not used them personally. Macrium Reflect [7]and Easeus Todo Backup are ones that I’ve seen a few times – but again have never personally relied on. Acronis True Image costs about $50 one time. Also we strongly discourage purchasing of Seagate external hard drives for your backup. Seagate drives fail too frequently for our liking. For more on backing up check out our podcast and article on Backup your data – Save your memories. [8]

Other Notes



Registry Optimizer

154 Invalid Entries Found

COM/ActiveX (42)
Uninstall Entries (28)
Windows Fonts (0)
Shared Dlls (0)
Application Paths (0)
Help & Resources
Windows Startup Items (2)
Deep Scan (60)
Program Shortcuts
File Associations
File Extensions
Custom Controls

SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Compo
17800A0F2E0E2B236A95EFD47A00A2D2

Please! Please!! Do NOT download Screen saver programs! Ever! They do nothing to protect modern monitors anyways and are OFTEN the source of infections.

Also AVOID Programs that claim they will magically speed up your computer. They almost NEVER do, and are again the cause of many issues. Research a program from trusted sources if you are unsure of it's authenticity. Just because it says it will make your computer run like a cheetah, doesn't mean it really will.

Also when you go to download ANYTHING make sure you don’t load 5 other programs with it. I have an example of that here: I didn’t install that but it’s there!

Did you find this article useful? Share it with friends and family with the share buttons below so that they too can be better informed internet-citizens.

Tech Tips [9]
Tech Tips Articles [10]
Tech Tips Podcasts [11]
Tech Tips Videos [12]

Source URL:https://www.pccomputerguy.com/Tech-Tips-Podcast-Protect-yourself-Online-Cyber-Threats

Links
[1] http://pccomputerguy.com/podcast/feed.xml [2] http://www.express.co.uk/news/uk/479840/Hackers-attack-sensitive-data-in-new-attack-on-computers [3] https://www.pccomputerguy.com/Tech-Tips-Videos-Create-Strong-Passwords [4] https://www.pccomputerguy.com/Tech-Tips-Podcast-Microsoft-Phone-Scams [5] http://www.pcworld.com/article/2047651/acronis-true-image-2014-review-still-powerful-and-feature-rich-now-easier-to-use.html [6] http://www.carbonite.com/ [7] http://www.macrium.com/reflectfree.aspx [8] https://www.pccomputerguy.com/Tech-Tips-Podcast-Backup-Save-Memories [9] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [10] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles [11] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Podcasts [12] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Videos