Presented by:

Craig Mayfield & Joey Police

What solution works best for you?

AntiVirus & Malware

Understanding what you're up against

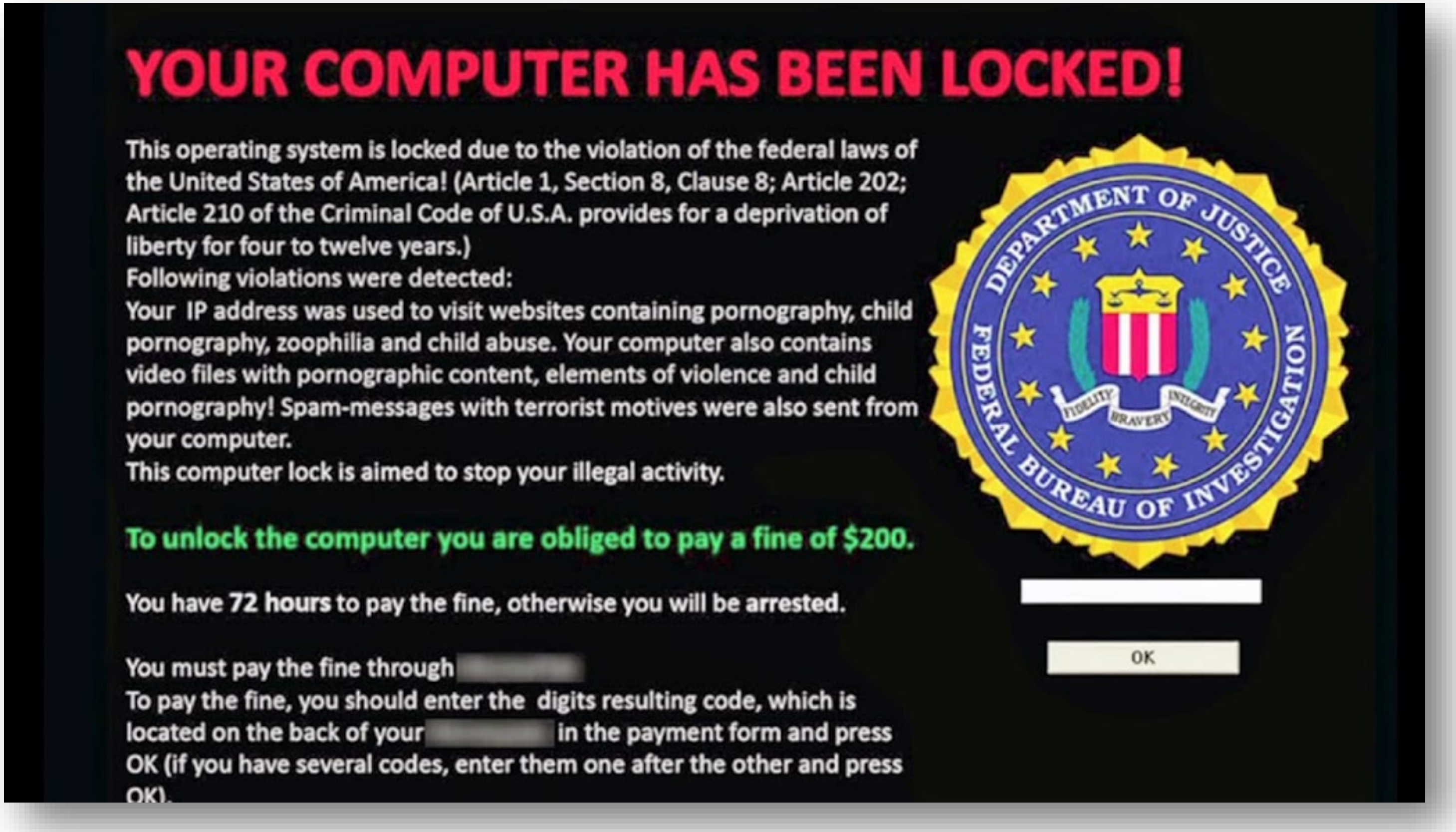
1 Viruses

2 Malware

3 Worms

What is the difference between all of these?

Our newcomer of late… **RANSOMWARE**



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

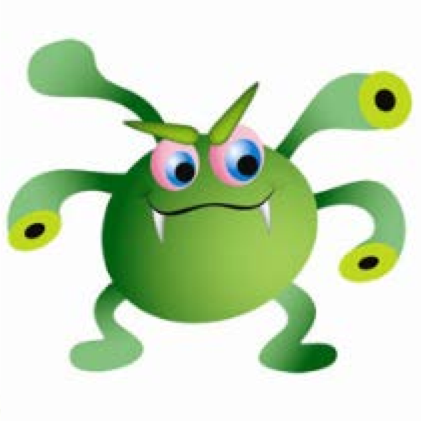
You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

How much is your data worth?

1

Virus: What is it?



Viruses Wreak Havoc On Your Files

VIRUS

The term computer virus is often used interchangeably with malware, though the two don't actually have the same meaning. In the strictest sense, a virus is a program that copies itself and infects a PC, spreading from one file to another, and then from one PC to another when the files are copied or shared.

Most viruses attach themselves to executable files, but some can target a master boot record, autorun scripts, MS Office macros, or even in some cases, arbitrary files. Many of these viruses, like CIH, are designed to render your PC completely inoperable, while others simply delete or corrupt your files—the general point is that a virus is designed to cause havoc and break stuff.

You can protect yourself from viruses by making certain your antivirus application is always updated with the latest definitions and avoiding suspicious looking files coming through email or otherwise. Pay special attention to the filename—if the file is supposed to be an mp3, and the name ends in .mp3.exe, you're dealing with a virus.

Now, let’s look at malware…

MALWARE

What is Malware?
The word Malware is short for malicious software, and is a general term used to describe all of the viruses, worms, spyware, and pretty much anything that is specifically designed to cause harm to your PC or steal your information.

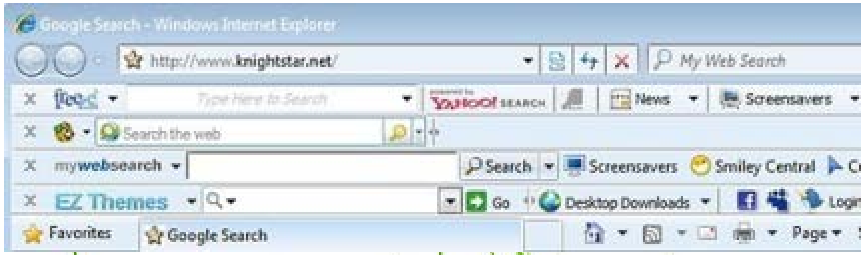
Spyware, scareware and worms oh my!

SPYWARE STEALS YOUR INFORMATION

Spyware is any software installed on your PC that collects your information without your knowledge, and sends that information back to the creator so they can use your personal information in some nefarious way. This could include keylogging to learn your passwords, watching your searching habits, changing out your browser home and search pages, adding obnoxious browser toolbars, or just stealing your passwords and credit card numbers.

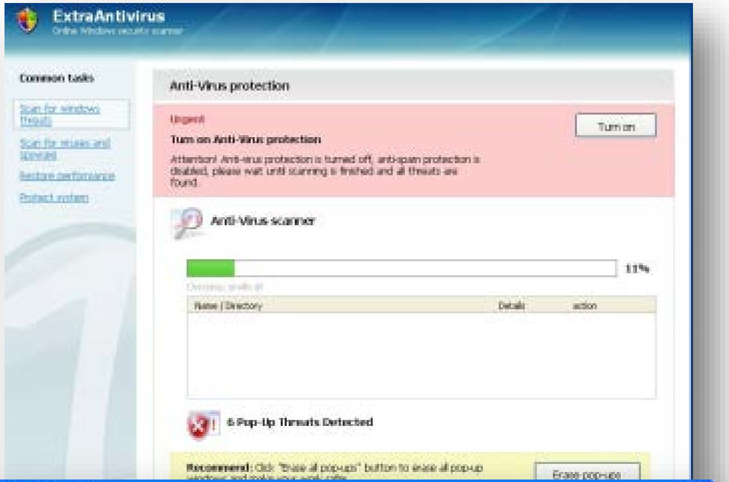
Since spyware is primarily meant to make money at your expense, it doesn't usually kill your PC—in fact, many people have spyware running without even realizing it, but generally those that have one spyware application installed also have a dozen more. Once you've got that many pieces of software spying on you, your PC is going to become slow.

What many people don't realize about spyware is that not every antivirus software is designed to catch spyware. You should check with the vendor to make sure the application you are using to protect you from malware is actually checking for spyware as well. If you come across a PC that is already heavily infected, run a combination of MalwareBytes and Combofix to clean it thoroughly.



Trojans and worms…

Scareware Holds Your PC for Ransom



ExtraAntivirus
Online Windows security scanner

Common tasks

- Scan for windows threats
- Scan for viruses and spyware
- Restore performance
- Protect system

Anti-Virus protection

Urgent

Turn on Anti-Virus protection

Attention! Anti-virus protection is turned off, anti-spam protection is disabled, please wait until scanning is finished and all threats are found.

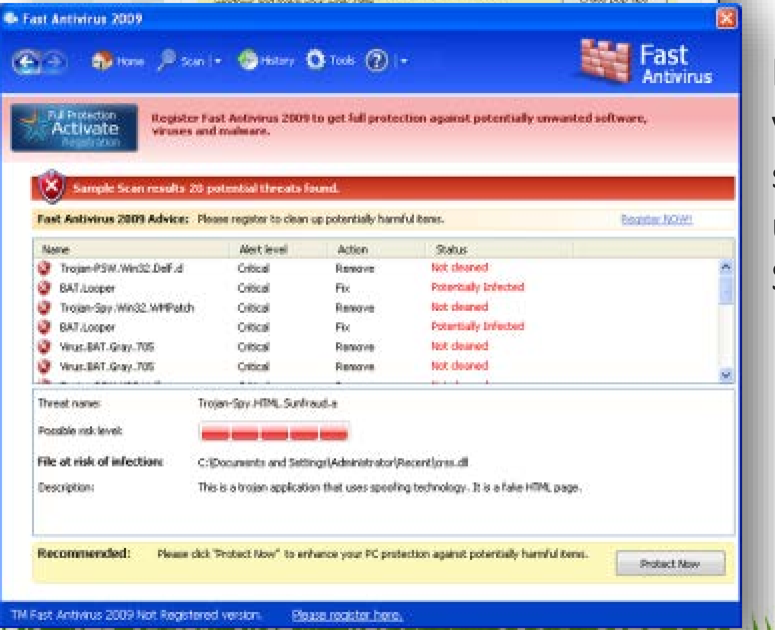
Anti-Virus scanner

11%

Name | Directory	Details	action

6 Pop-Up Threats Detected

Recommend: Click "Erase all pop-ups" button to erase all pop-up



Fast Antivirus 2009

Register Fast Antivirus 2009 to get full protection against potentially unwanted software, viruses and malware.

Sample Scan results 20 potential threats found.

Fast Antivirus 2009 Advice: Please register to clean up potentially harmful items. Register NOW!

Name	Alert level	Action	Status
Trojan-PSW.Win32.Delf.d	Critical	Remove	Not cleaned
BAT.Looper	Critical	Fix	Potentially Infected
Trojan-Spy.Win32.WMPatch	Critical	Remove	Not cleaned
BAT.Looper	Critical	Fix	Potentially Infected
Virus.BAT.Gray..705	Critical	Remove	Not cleaned
Virus.BAT.Gray..705	Critical	Remove	Not cleaned

Threat name: Trojan-Spy.HTML.Sunfraud-a

Possible risk level:

File at risk of infection: C:\Documents and Settings\Administrator\Recent\cnss.dll

Description: This is a trojan application that uses spoofing technology. It is a fake HTML page.

Recommended: Please click "Protect Now" to enhance your PC protection against potentially harmful items.

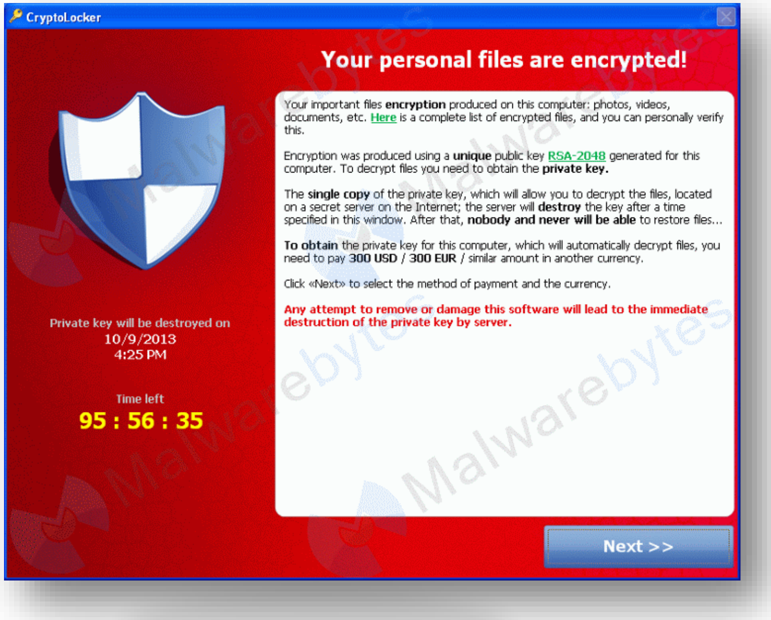
TM Fast Antivirus 2009 Not Registered version. Please register here.

Scareware is a relatively new type of attack, where a user is tricked into downloading what appears to be an antivirus application, which then proceeds to tell you that your PC is infected with hundreds of viruses, and can only be cleaned if you pay for a full license. Of course, these scareware applications are nothing more than malware that hold your PC hostage until you pay the ransom—in most cases, you can't uninstall them or even use the PC.

If you manage to come across a PC infected with one of these, your best bet is to Google the name of the virus and find specific instructions on how to remove it, but the steps are usually the same—run a combination of MalwareBytes, SuperAntiSpyware, and maybe ComboFix if you need to.

Worms and Trojans…

RANSOMWARE… How much are you willing to pay?



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

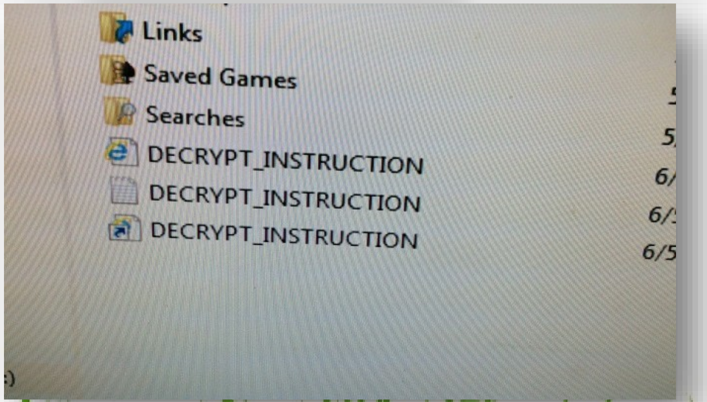
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35



Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.

Most Commonly:

- Encrypts most of your data files like (pictures, documents, zip files, Spreadsheets)
- Data can only be recovered by paying a ransom via “Bitcoins”
- Or, from a backup that has NOT been encrypted.

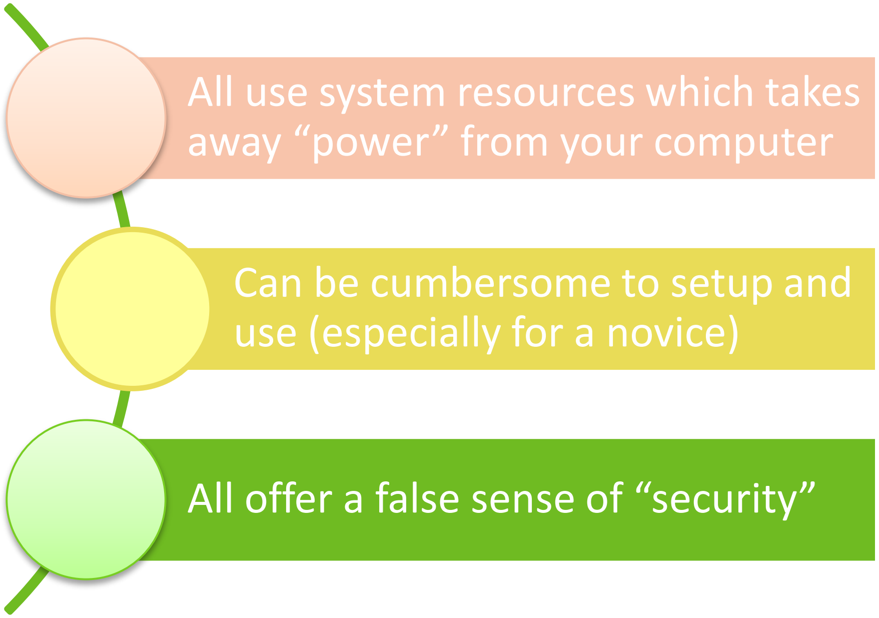
TELEPHONE SCAM: THEY SAY THEY WORK FOR:

Microsoft

Anyone who calls you, and says that they work for Microsoft or ANY company and that your PC is infected: HANG UP!

All Antivirus applications Stink!

Why?



All use system resources which takes away "power" from your computer

Can be cumbersome to setup and use (especially for a novice)

All offer a false sense of "security"

Let's see the competition!

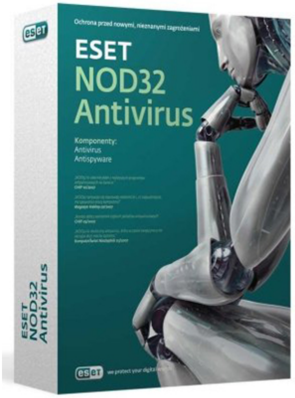
Let's Meet Our Contestants!

avast! antivirus

AVIRA AntiVir

McAfee® Proven Security™

symantec.™



eset
Ochrona przed nowymi, nieznanymi zagrożeniami
ESET NOD32 Antivirus
Komponenty: Antivirus Antispyware
ESET NOD32 Antivirus

Microsft Security Essentials

CLAMWIN FREE ANTIVIRUS open source security for your PC

AVG Anti-Virus System

Webroot® Spy Sweeper®

Norton Internet Security™

Which Applications are Free

AVG.
Anti-Virus
FREE EDITION

avast!
be free

CLAMWIN
FREE ANTIVIRUS
open source security for your PC

Microsoft
Security Essentials

Which Applications Stink the Least

THE PAID VERSIONS

ESET – LOW on resources!

Trend Micro – VERY GOOD, but expensive.

avast! – VERY GOOD, but HARD ON YOUR PC!

Which are the WORST ONES!

Which Applications Stink the Most

…and the Award goes to….

Why?
All use a considerable amount of computer resources.

Extremely cumbersome to setup and use

I often tell clients:
“Instead of using these products, you’re just better off getting the virus”

They are all more expensive than most

What to do when you get malware/virus/spyware

….because, by God you will no matter what you use.

No, it’s not Thundercats

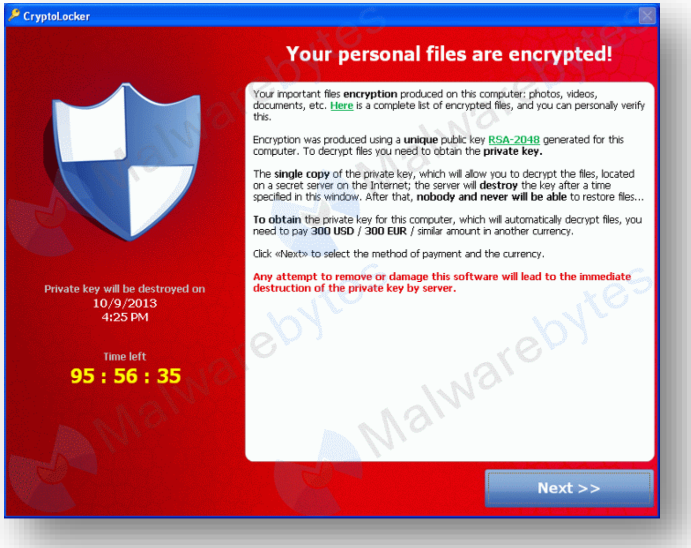
http://www.bleepingcomputer.com/combofix/how-to-use-combofix

Combofix

http://www.malwarebytes.org/

Malwarebytes

What to do when you get RANSOMWARE



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

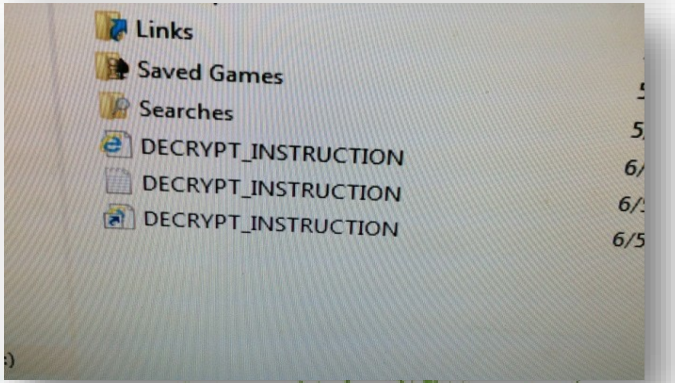
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35



Links
Saved Games
Searches
DECRYPT_INSTRUCTION
DECRYPT_INSTRUCTION
DECRYPT_INSTRUCTION

If you have This

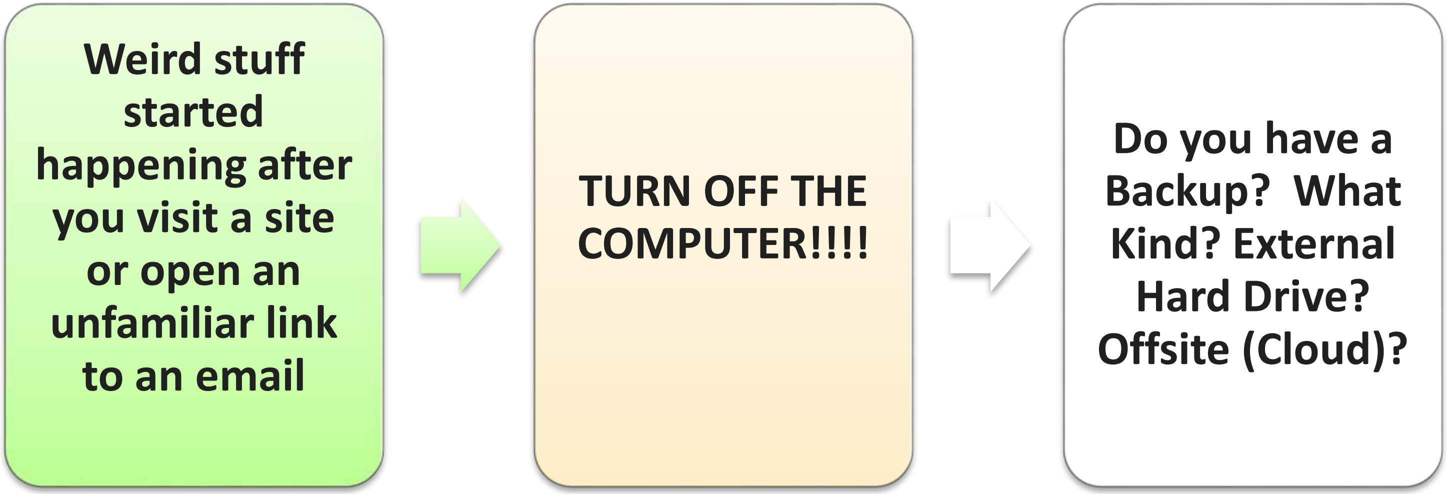
We still need to remove it with these

Hitman Pro

Emsisoft

If you “suspect” you have RANSOMWARE

Suspect “meaning”:



Weird stuff started happening after you visit a site or open an unfamiliar link to an email

TURN OFF THE COMPUTER!!!!

Do you have a Backup? What Kind? External Hard Drive? Offsite (Cloud)?

Steps to Removal

Download and Run **Combofix** in Safe Mode

Download and Run **Malwarebytes** QuickScan

Download and Run **HitManPro**

Download and Run **Emsisoft**

HOW TO LIMIT YOUR RISKS

- Website Blocking – Open DNS, ISA
- Update Windows
- Update Adobe Flash and Reader
- Use Script Blocker like “No Script” for Firefox
- Do not use Internet Explorer 6 or 9 (Windows XP/Vista). Best to use updated IE11, Firefox, Chrome, etc.

Cloud Backups

Find the right solution for you, and back up your data to the cloud.

CRASHPLAN™
Automatic Online Backup

mozy

CARBONITE™
ONLINE BACKUP