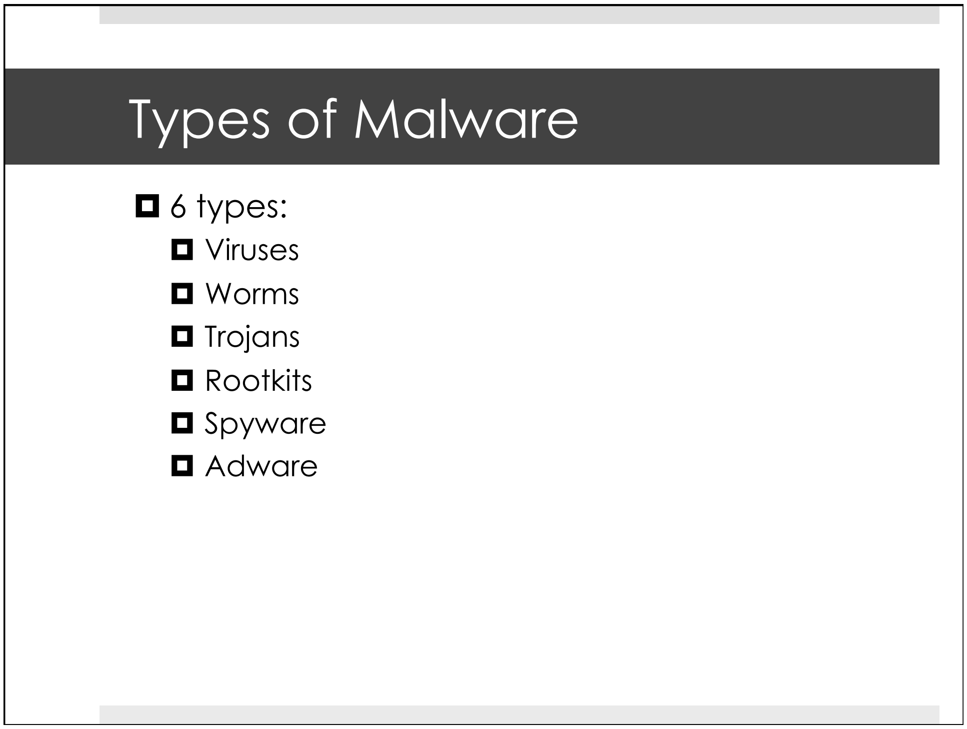
Malware

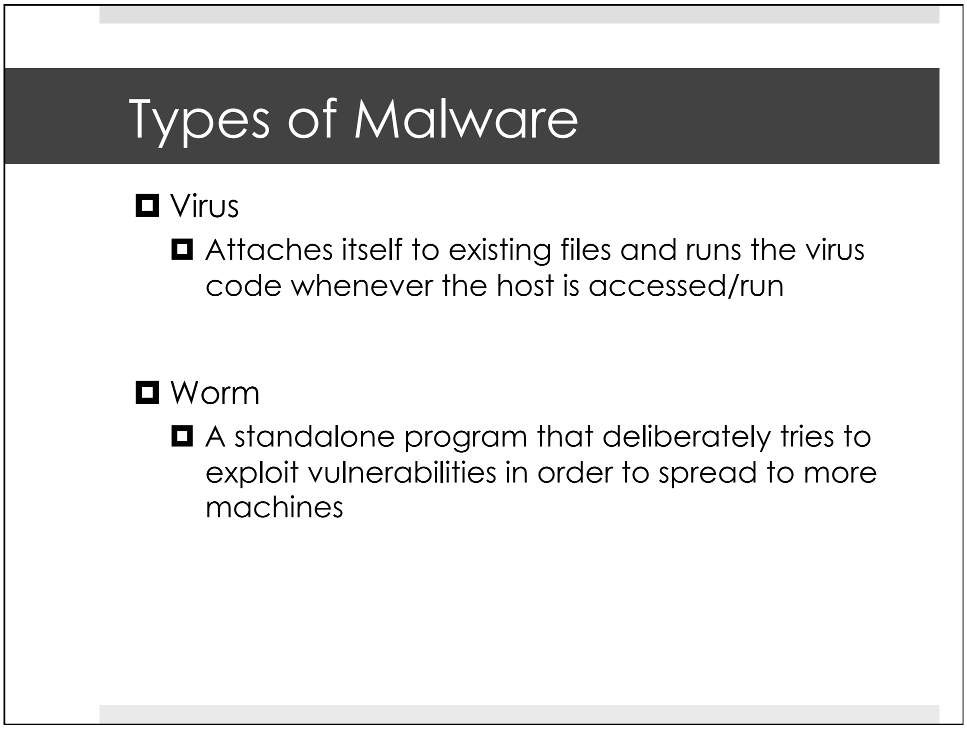
Malware Topics

- What is malware?
- What does it look like?
- How can you stop it?



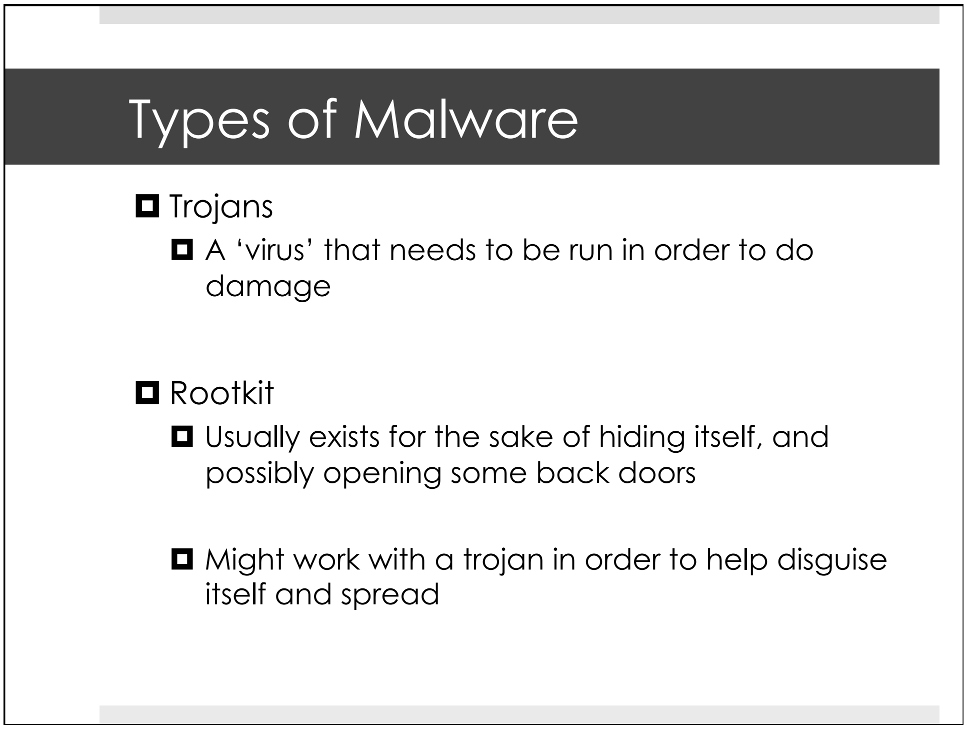
Types of Malware

- 6 types:
  - Viruses
  - Worms
  - Trojans
  - Rootkits
  - Spyware
  - Adware



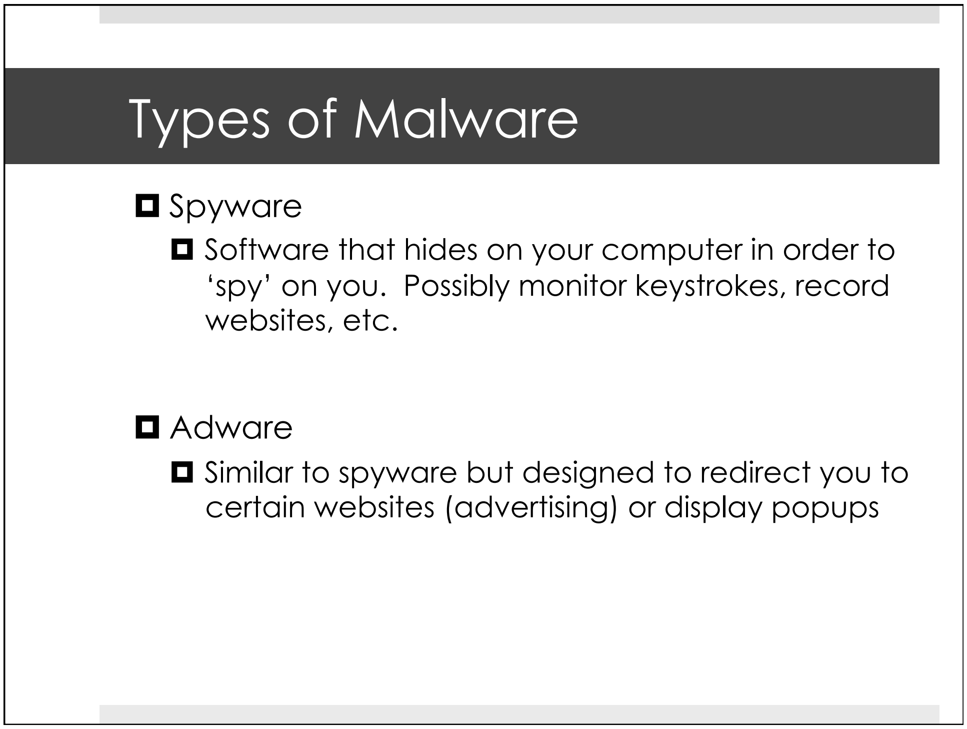
Types of Malware

- Virus
  - Attaches itself to existing files and runs the virus code whenever the host is accessed/run
- Worm
  - A standalone program that deliberately tries to exploit vulnerabilities in order to spread to more machines



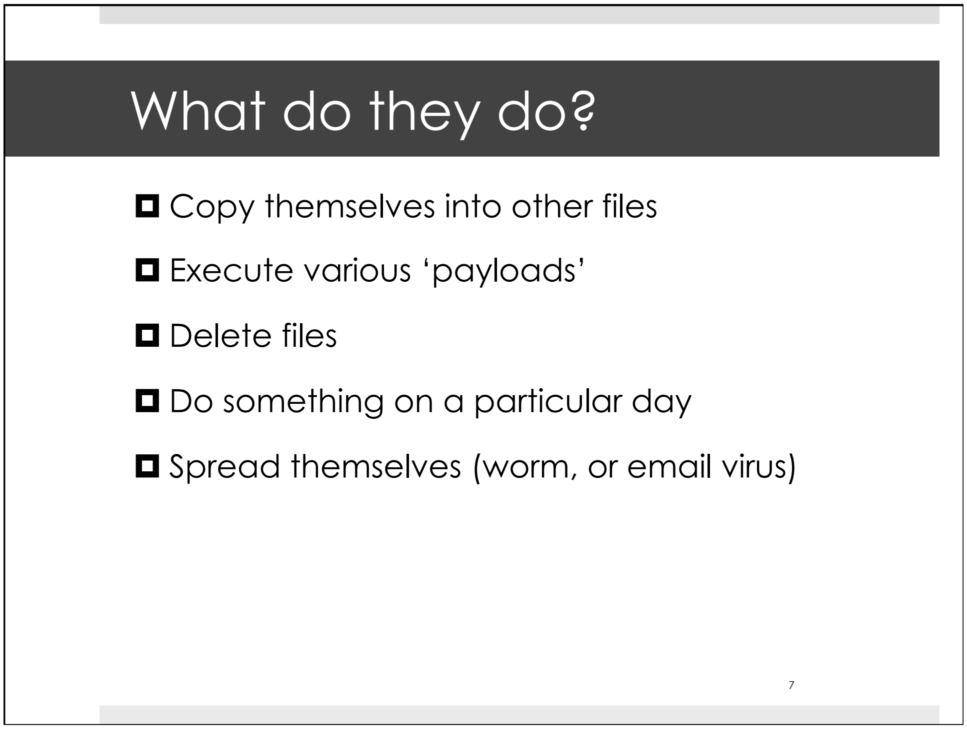
Types of Malware

- Trojans
  - A ‘virus’ that needs to be run in order to do damage
- Rootkit
  - Usually exists for the sake of hiding itself, and possibly opening some back doors
  - Might work with a trojan in order to help disguise itself and spread



Types of Malware

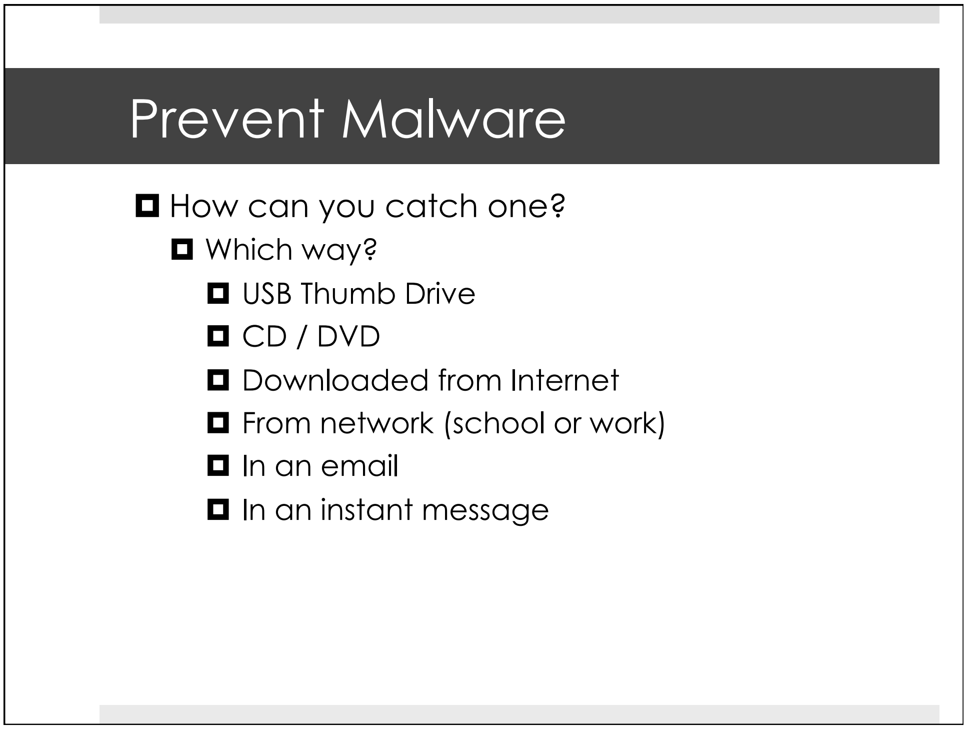
- Spyware
  - Software that hides on your computer in order to ‘spy’ on you. Possibly monitor keystrokes, record websites, etc.
- Adware
  - Similar to spyware but designed to redirect you to certain websites (advertising) or display popups



What do they do?

- Copy themselves into other files
- Execute various ‘payloads’
- Delete files
- Do something on a particular day
- Spread themselves (worm, or email virus)

7



Prevent Malware

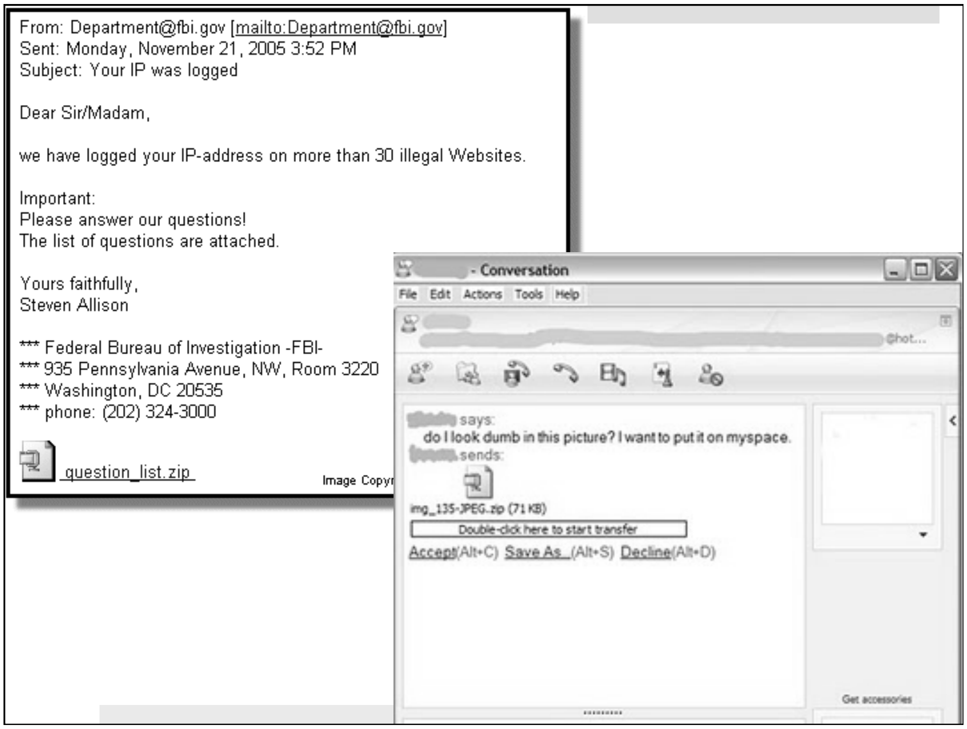
- How can you catch one?
  - Which way?
    - USB Thumb Drive
    - CD / DVD
    - Downloaded from Internet
    - From network (school or work)
    - In an email
    - In an instant message

Malware Examples

To: a_student@myschool.ca
FROM: your_pal@myschool.ca
SUBJECT LINE: Check it out!

Hi,
check the attached screensaver.. its really wonderfool..
i got it from freescreensavers.com

Attatchment: Screensavers.scr



From: Department@fbi.gov [mailto:Department@fbi.gov]
Sent: Monday, November 21, 2005 3:52 PM
Subject: Your IP was logged

Dear Sir/Madam,

we have logged your IP-address on more than 30 illegal Websites.

Important:
Please answer our questions!
The list of questions are attached.

Yours faithfully,
Steven Allison

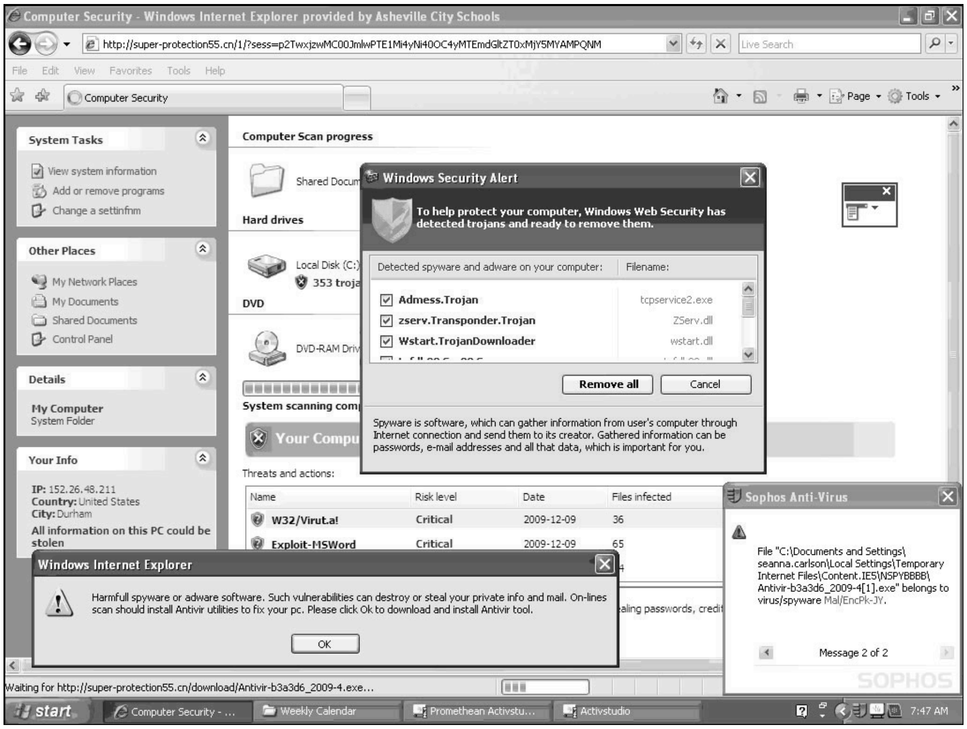
*** Federal Bureau of Investigation -FBI-
*** 935 Pennsylvania Avenue, NW, Room 3220
*** Washington, DC 20535
*** phone: (202) 324-3000

question_list.zip

Image Copyr

[redacted] - Conversation

[redacted] says:
do I look dumb in this picture? I want to put it on myspace.
[redacted] sends:
img_135-JPEG.zip (71 KB)



Windows Security Alert

To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
☑ Admess.Trojan	tcpservice2.exe
☑ zserv.Transponder.Trojan	ZServ.dll
☑ Wstart.TrojanDownloader	wstart.dll

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

IP: 152.26.48.211
Country: United States
City: Durham

All information on this PC could be stolen

Threats and actions:

Name	Risk level	Date	Files infected
W32/Virut.a!	Critical	2009-12-09	36
Exploit-MSWord	Critical	2009-12-09	65

Windows Internet Explorer

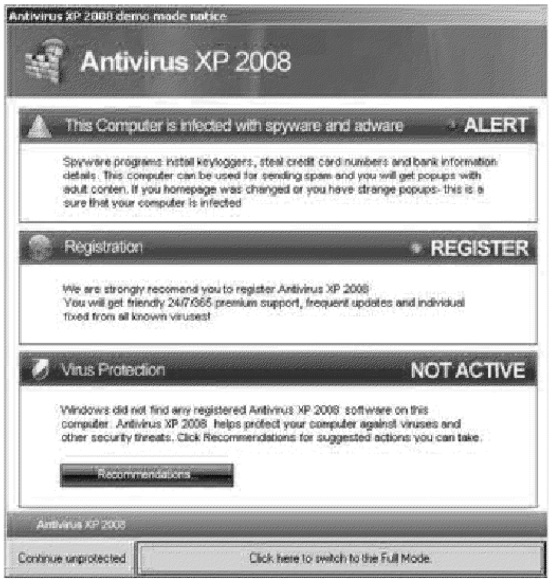
Harmfull spyware or adware software. Such vulnerabilities can destroy or steal your private info and mail. On-lines scan should install Antivir utilities to fix your pc. Please click Ok to download and install Antivir tool.

aling passwords, credit

Sophos Anti-Virus

File "C:\Documents and Settings\seanna.carlson\Local Settings\Temporary Internet Files\Content.IE5\NSPYBBBB\Antivir-b3a3d6_2009-4[1].exe" belongs to virus/spyware Mal/EncPk-JY.

Waiting for http://super-protection55.cn/download/Antivir-b3a3d6_2009-4.exe...


Antivirus XP 2008 demo mode notice
Antivirus XP 2008
Recommendations...
Antivirus XP 2008
Continue unprotected
Click here to switch to the Full Mode.

This Computer is infected with spyware and adware — ALERT

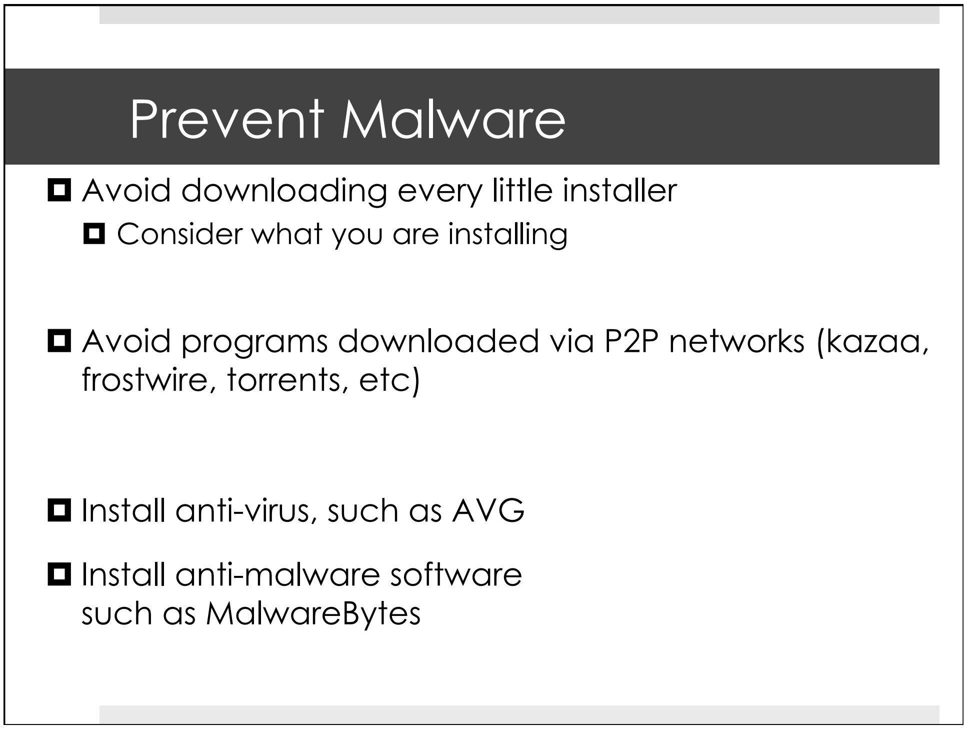
Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected

Registration — REGISTER

We are strongly recomend you to register Antivirus XP 2008
You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

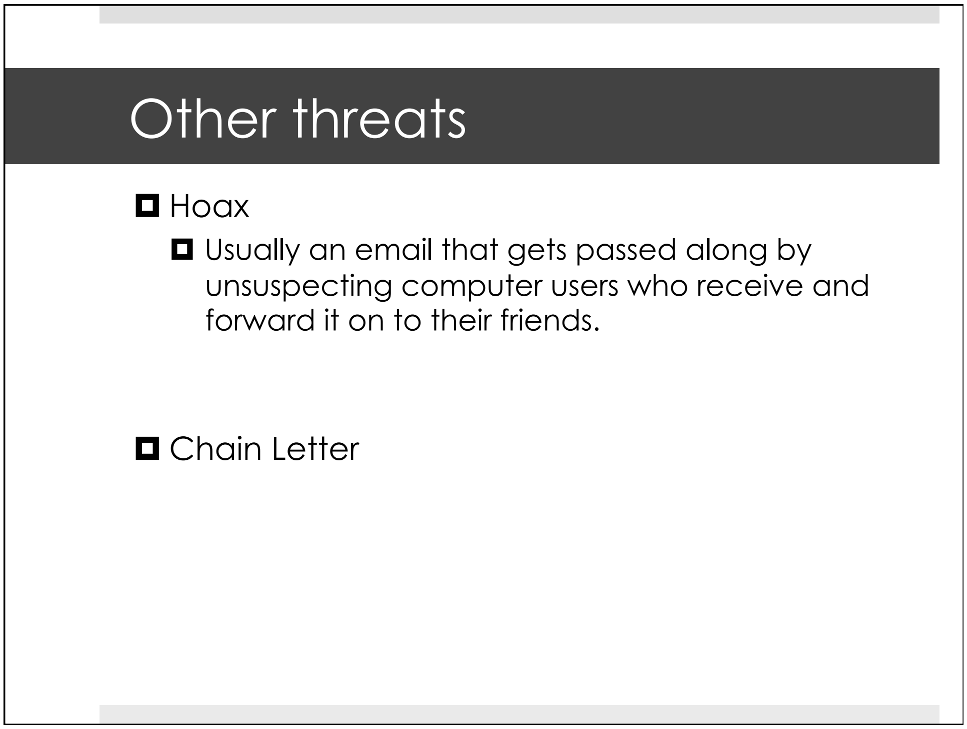
Virus Protection — NOT ACTIVE

Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.



Prevent Malware

- Avoid downloading every little installer
  - Consider what you are installing
- Avoid programs downloaded via P2P networks (kazaa, frostwire, torrents, etc)
- Install anti-virus, such as AVG
- Install anti-malware software such as MalwareBytes

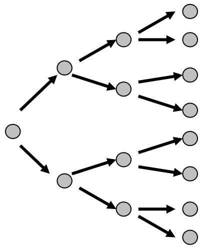


Other threats

- Hoax
  - Usually an email that gets passed along by unsuspecting computer users who receive and forward it on to their friends.
- Chain Letter

Hoaxes / Chain Letters

- Usually an email that gets passed along
- Spreads by email just like a virus
  - No code: it doesn’t replicate itself.
  - Gullible people email it around



Hoaxes & Chain Letters

- What does a hoax do?
  - Making you look foolish if you forward it
  - Clogs people’s email
  - Slows down your network and the Internet
  - Could ask you to do something that will damage your computer
- DO NOT forward on email even if it does sound like a real warning

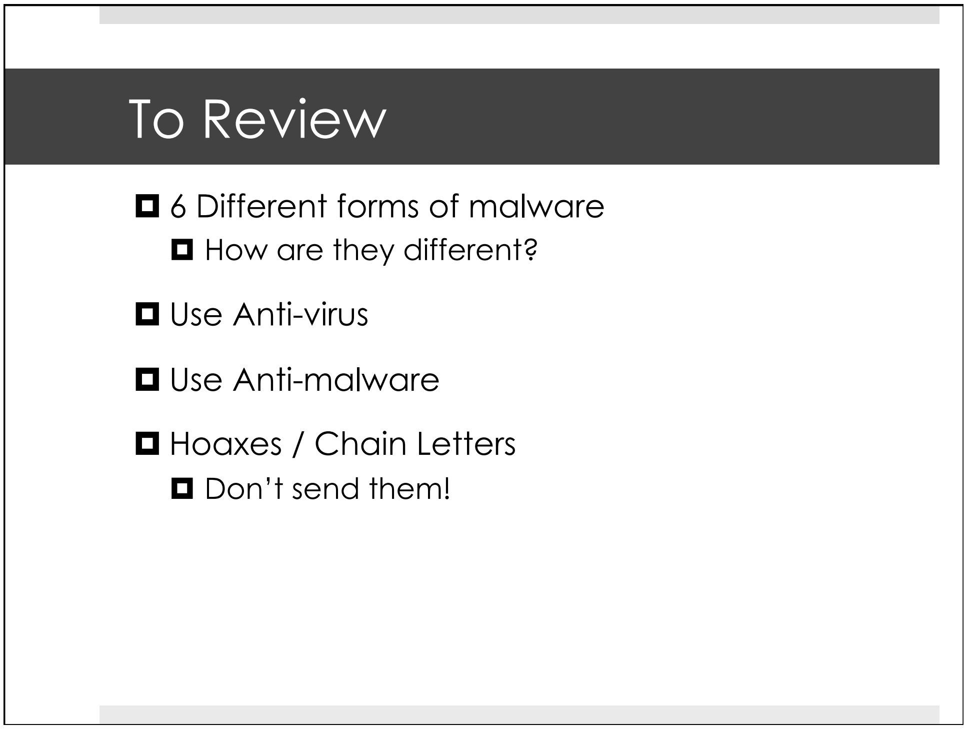
Example Hoax Email

On … Mars will look as large as the moon.

- Lots of technical detail
- All kinds of information
- Sensational
  - “Once in a 1000 years!”
  - “No one alive will see this again!”

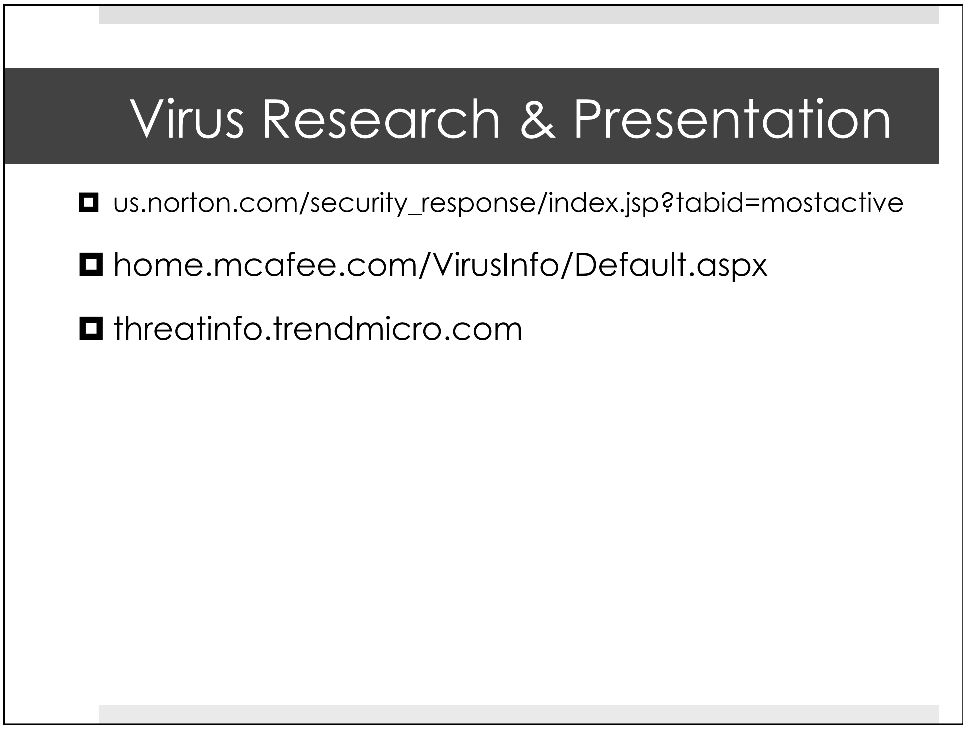
Worried?

- Check out snopes.com
- Check out hoaxbusters.org
- Contains info about
  - Hoax emails
  - Urban legends
  - Fake news reports
  - Chain Letters



To Review

- 6 Different forms of malware
  - How are they different?
- Use Anti-virus
- Use Anti-malware
- Hoaxes / Chain Letters
  - Don’t send them!



Virus Research & Presentation

- us.norton.com/security_response/index.jsp?tabid=mostactive
- home.mcafee.com/VirusInfo/Default.aspx
- threatinfo.trendmicro.com