

OLLI

Personal Computer Security

Daniel Venese

September 23, 2014

Security Measures

- Operating system updates (set for automatic update)
- Application program updates
- Anti-virus program or more inclusive suite (must keep signature file up to date), free version available
- Browser, hardening, plugins
- Virus removal tools available from Microsoft, major anti-virus vendors
- Off line virus removal tool available from Microsoft

Security Measures

- Spyware scanning and removal tools (Spybot, Malwarebyte)
- Userid/password practices, password safe
- Safe user behavior
- On-line security scanning tools
- Firewalls
- Backups
- More advanced tools

Terminology

- Malware: harmful program that compromises security (virus, worm, spyware, etc)
- Attack vector = payload + method of delivery
- Attack surface: programs, files, protocols, business partners, and network end points that can be attacked
- Microsoft definition of attack surface, SDL Practice #6: Attack Surface Analysis/Reduction
 - Reducing the opportunities for attackers to exploit a potential weak spot or vulnerability requires thoroughly analyzing overall attack surface and includes disabling or restricting access to system services, applying the principle of least privilege, and employing layered defenses wherever possible.

Security Precepts

- Security is never absolute (even isolated computer in Mission Impossible was compromised)
- Security posture can change at a moment's notice e.g., new vulnerability discovered
- Complexity and high skill level make it difficult to assess security posture and implement countermeasures
- Dangerous user behavior can thwart security measures

Security Vulnerabilities

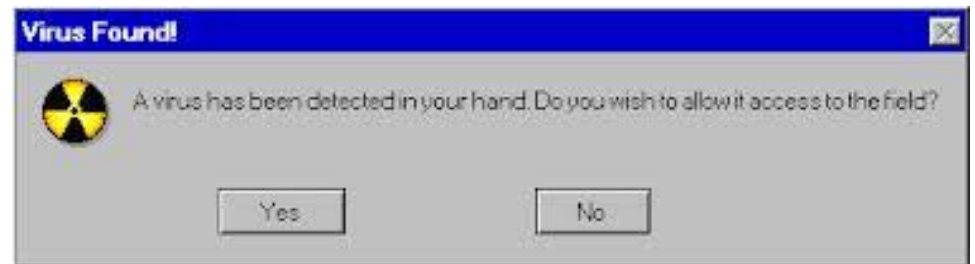
- Hackers have proven proficient at continuing to find new vulnerabilities
- Attacks can be launched against applications as well as operating systems; every application on your computer is a potential entry point
- Comprehensive approach needed, it only takes one weak spot to be compromised
- Security threat constantly evolves

Signs of Malware (virus) Infection

- Mouse/system frozen
- Computer works slowly
- Files missing or corrupted
- Computer crashes
- Disk drives disappear
- Pop-up ads, ransomware appear
- Browser hijack: home page redirected to porn or other undesirable site

Results of Computer Infection

- Computer becomes part of botnet
- Key logger installed to steal account information
- Personal information stolen for identity fraud
- Demand for credit card payment to remove spyware (ransomware)



Malware Toolkits

- Crimeware is growing more automated and effective, lowering the bar for criminals looking to cash in, says Symantec report.
- At least 61% of all online attacks today are launched via automated attack toolkits, says a new report from Symantec
- User friendly interfaces allow hackers to select type of attack to launch and target computers
- Toolkits are continually updated as vulnerabilities are patched

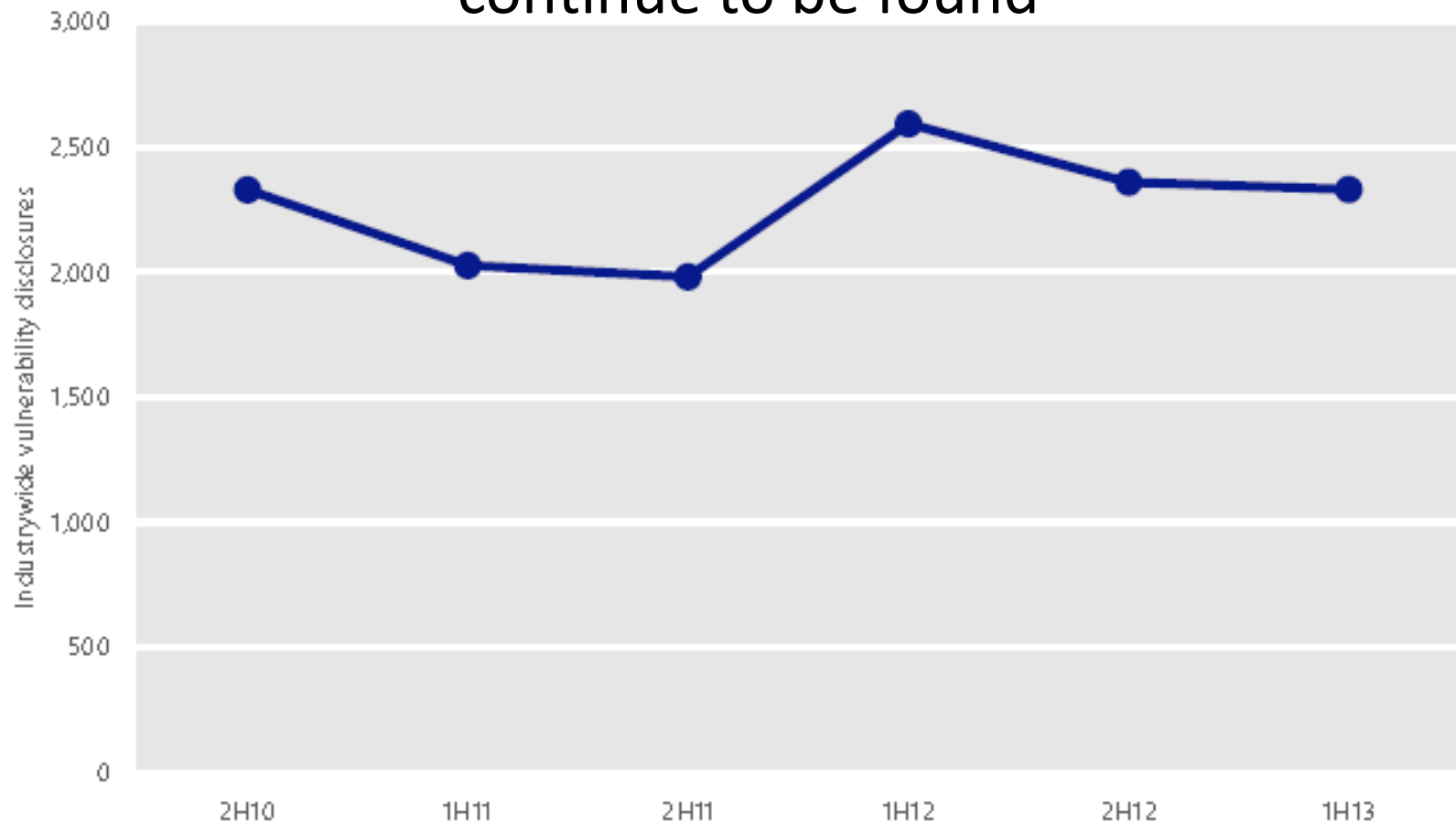
<http://www.informationweek.com/security/risk-management/malware-toolkits-generate-majority-of-online-attacks/d/d-id/1095509?>

Run Your Own Botnet

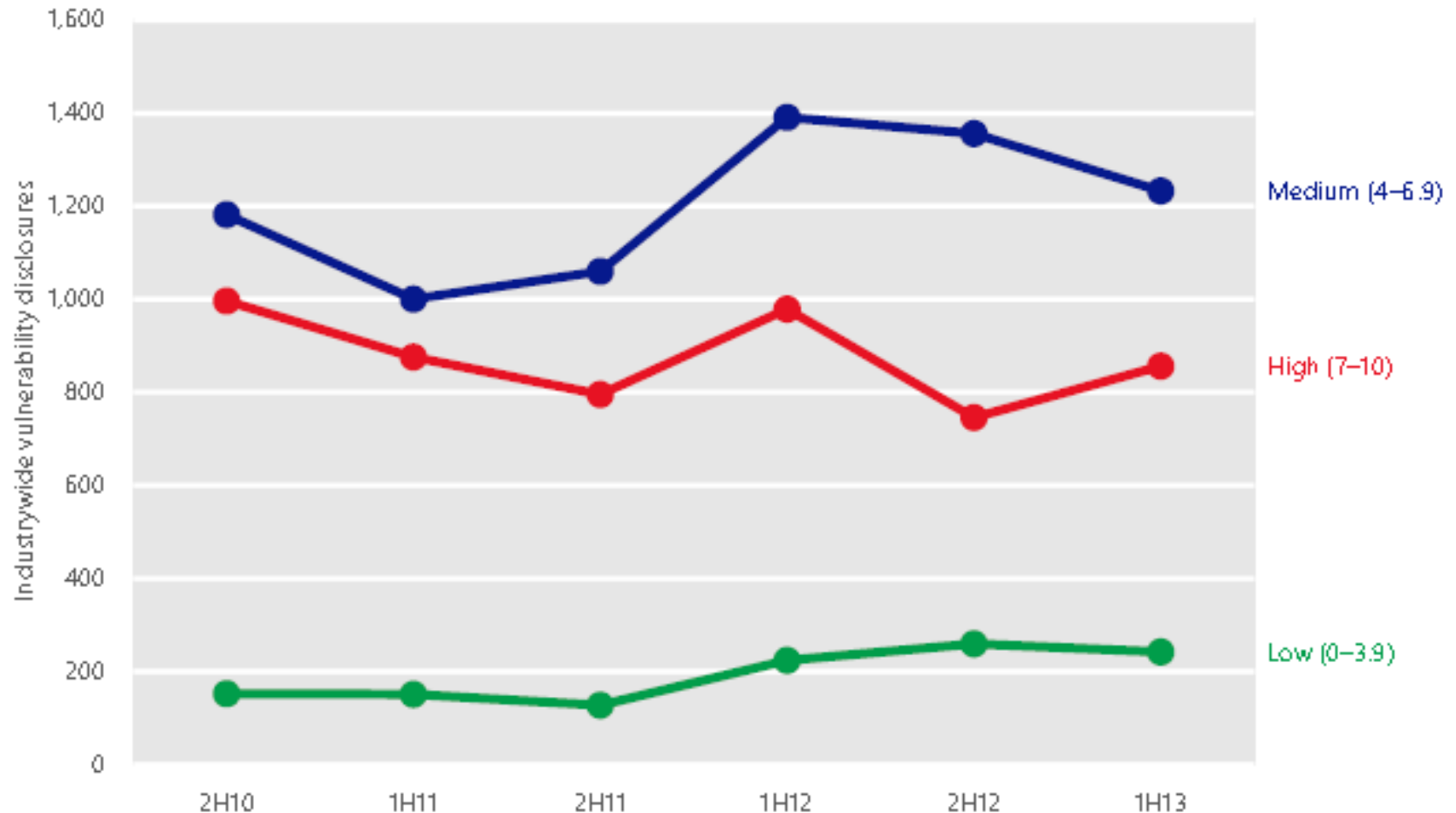
- Zeus is a toolkit to build and administer a botnet, primarily for stealing banking information
- A Control Panel application is used to maintain/update the botnet,
- A configurable Builder tool allows creation of executables that will be used to infect victim's computers
- Toolkit is a “commercial product” that is sold to many different users, and distributed freely to many more.
- The latest version of toolkit typically sells for about \$700 USD

Industrywide Vulnerability Disclosures

In spite of industry efforts vulnerabilities continue to be found

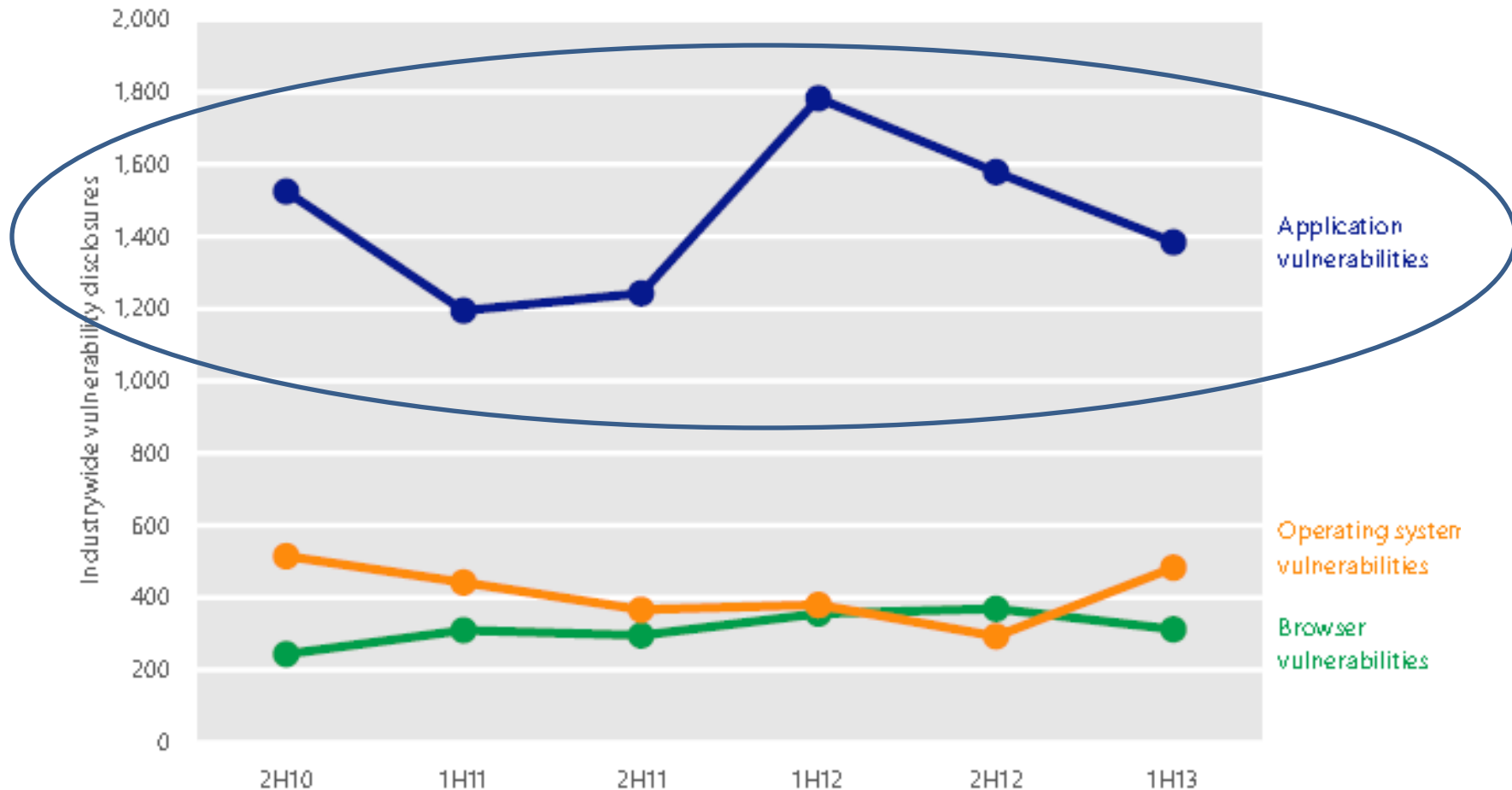


Industrywide Vulnerability Disclosures by Severity



Industrywide Operating System, Browser, & Application Vulnerabilities

Figure 11. Industrywide operating system, browser, and application vulnerabilities, 2H10–1H13



Common Attack Vectors

Attack Method	Malware Payload
Email	Malware file, link to malicious site, malware embedded in pictures, browser hijack, spam
Browse or link to malicious site	Malware, browser hijack
Open infected file	Malware



What is Spam

- Email spam is one of most common ways in which computers are infected
- Attempt to install malware on your computer
- Malware may do any or all of these
 - Send spam to every address in your contact list
 - Steal account information
 - Make your computer part of a botnet to infect other computers
 - Use your computer in a denial of service attack-to flood a computer with bogus traffic

Most Email is Spam

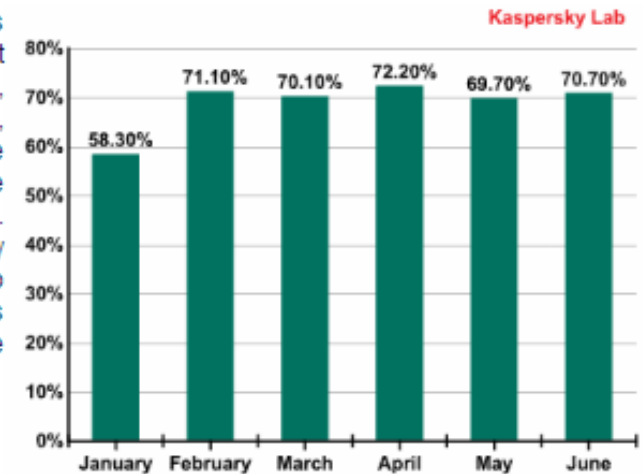
- A few low-cost servers can send out huge numbers of spam each day, hundreds of thousands
- Only a tiny response rate makes spam profitable

Spam Statistics Report Q2-2013

This Quarterly Spam Statistics Report, provides the latest analysis of spam trends, malicious attachments, phishing, and insights from the Kaspersky Lab intelligence team for the 2nd quarter 2013. This report provides not only key findings and trends but also spammer methods and tricks as well as spam by source globally.

Key Findings

In Q2 the percentage of spam in total email traffic increased by 4.2% from the first quarter of 2013 and came to 70.7%. The percentage of phishing emails in global mail traffic fell by 0.0016% and came to 0.0024%. Malicious attachments were detected in 2.3% of all emails — that's 1% less than in Q1 2013. These figures are among the results of Kaspersky Lab's email traffic analysis for Q2 2013.



The percentage of spam in email traffic

Source: Kaspersky Labs

Characteristics of Spam Messages

- May come from company you have a relationship with
- Offers a special deal, access to porn, or cheap prescription drugs
- Urges immediate action to prevent undesirable consequences, such as closing one of your accounts
- Offers big reward for helping to transfer large amount of money
- Impersonates a charity or political organization
- Email address is from someone you know

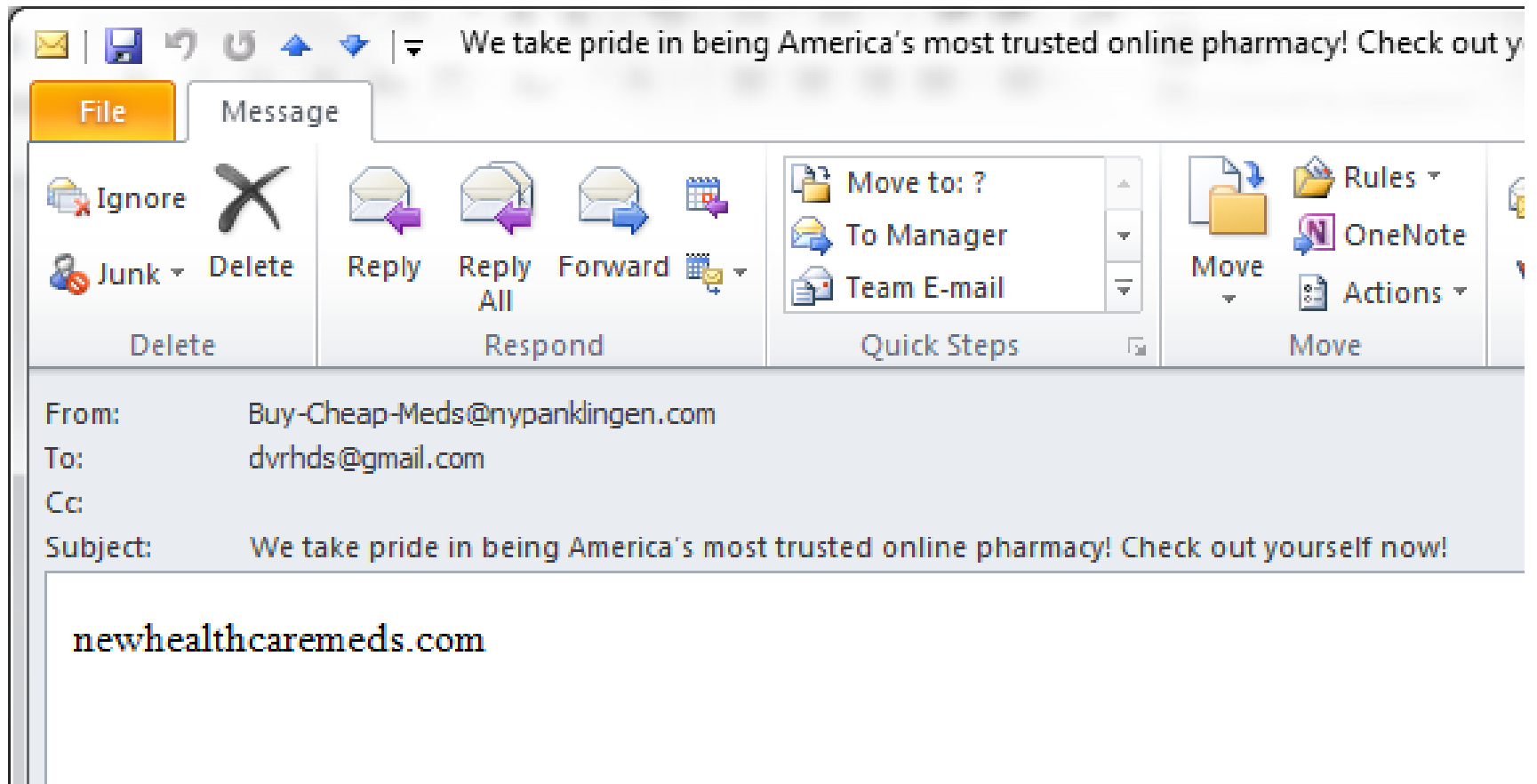
Lines of Defense Against Spam

- Most spam should be screened out by your ISP
- Email clients such as Microsoft Outlook have various capabilities to screen for email and place them in a junk mail folder
- Gmail and other email providers offer configurable filters to screen out spam
- Third party programs are available

How is Malware Installed from Email

- Open a message and click to download pictures, Word file, open PDF, etc.
- Many file types can contain executable code
- Click on a link embedded in a message and be directed to a malware site

Spam Example




America's Most Trusted Pharmacy is in Belarus

```
[Querying whois.ripe.net] [whois.ripe.net] %  
This is the RIPE Database query service. % The  
objects are in RPSL format. % % The RIPE  
Database is subject to Terms and Conditions. %  
See http://www.ripe.net/db/support/db-terms-conditions.pdf % Note: this output has  
been filtered. % To receive output for a  
database update, use the "-B" flag. %  
Information related to '91.149.173.0 -  
91.149.173.255' inetnum: 91.149.173.0 -  
91.149.173.255 org: ORG-MTIN1-RIPE  
netname: MTI-NET descr: Minsk Television  
Information Networks (CableTV, ISP) descr:  
23A Cnnynskaya str., Minsk 220100 Belarus  
country: BY admin-c: CHYU-RIPE tech-c: MAHE-  
RIPE status: ASSIGNED PA mnt-by: BYGIS-MNT  
mnt-domains: BYGIS-MNT source: RIPE #  
Filtered
```

How to Lookup IP Address


whatismyipaddress.com/ip-lookup

Suggested Sites Amazon.com - Onli... HP - See What's Hot HP Games Web Slice Gallery Bookmarks

 How you **connect** to the

MY IP IP LOOKUP SPEED TEST BLACKLIST CHECK TRACE EMAIL CHANGE IP HIDE

<http://whatismyipaddress.com/ip-lookup>

 IP Lookup

Lookup IP Address Location

If you can find out the IP address of an Internet user, you can get an idea what part of the country or world they're in by using our IP Lookup tool.

What to do: Enter the IP address you're curious about in the box below, then click "Look Up IP Address." Read the information below for an explanation.

71.255.254.129

On-Line File Scanner and URL Checker

[Statistics](#) [Documentation](#) [FAQ](#) [About](#) [English](#) [Join us](#)



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File

URL

Search

No file selected

Choose File

Maximum file size: 64MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

Microsoft OS Infection Rates

- “In the second half of 2012, XP's infection rate was 11.3 machines per 1,000 scanned by the company's security software,
- more than double the 4.5 per 1,000 for Windows 7 SP1 32-bit and
- Triple the 3.3 per 1,000 for Windows 7 SP1 64-bit.”
- NOTE: this does not include infections due to applications software such as Adobe Flash

<http://www.pcworld.com/article/2046548/windows-xps-retirement-could-spark-a-hacker-feeding-frenzy.html>

Windows XP - RIP

- End of life, support ending
- Higher probability of compromise
- Possible that hackers are stockpiling exploits for when support ends
- Use Windows 7/8

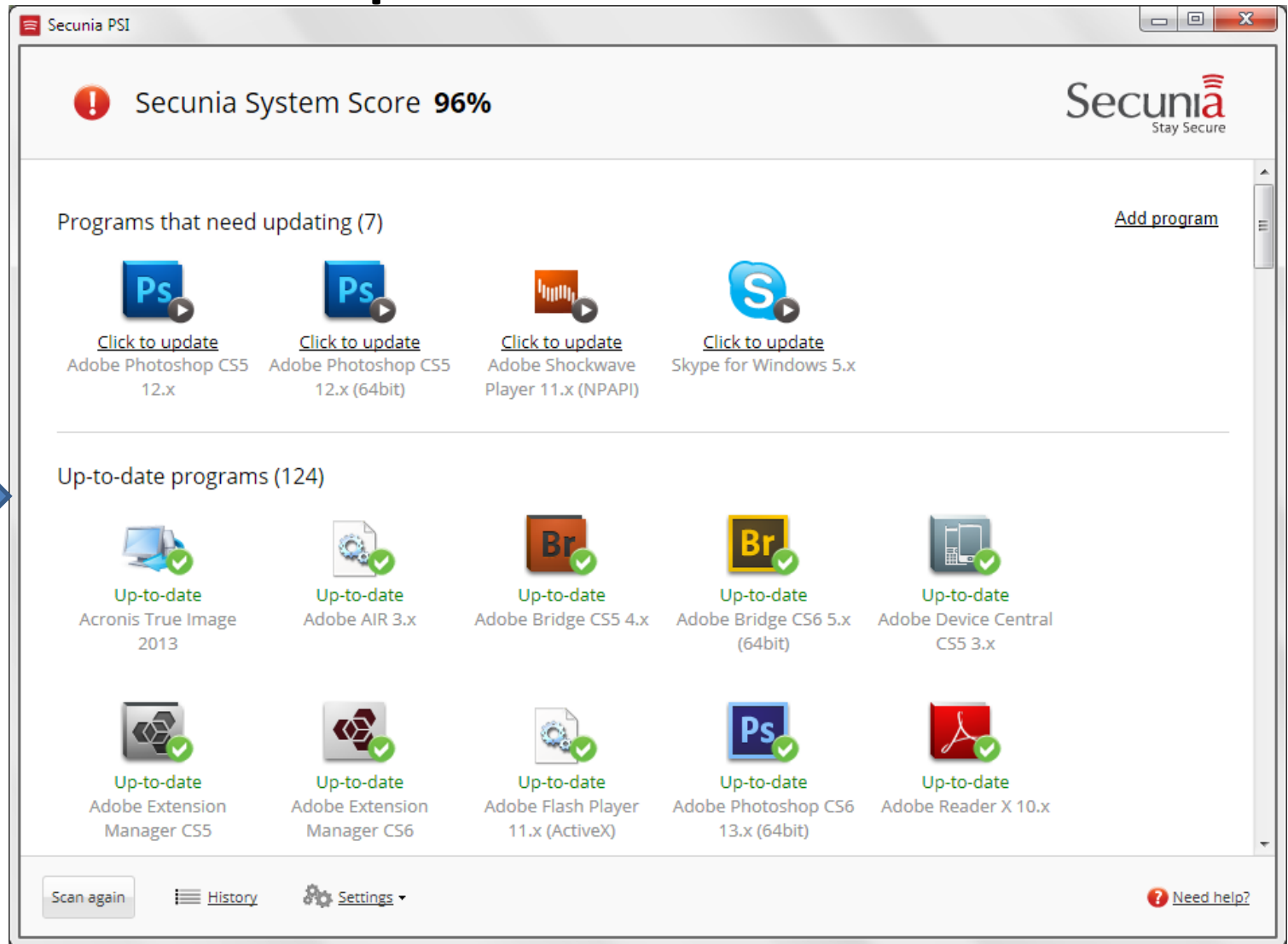
Free Microsoft Security Tools 1/2

- Microsoft Malicious Software Removal Tool
 - Runs once a month unless run manually
 - Removes malware after computer is infected
 - Updates and runs automatically
- Microsoft Security Essentials (part of Windows 8)
 - Targets malware and spyware
 - Must be manually installed on OS prior to Windows 8, automatically updates
 - Not compatible with third party anti-virus software e.g., Symantec or McAfee
 - Has mixed reviews as to effectiveness

Free Microsoft Security Tools 2/2

- Microsoft Safety Scanner removes malware and spyware
 - Works independently of other security tools to clean an infected system
 - Downloaded from Microsoft
- Windows Defender Offline
 - Microsoft's most powerful tool for consumers
 - Works outside of Windows on a bootable media such as a flash drive, can potentially clean an infected system that is inoperable
 - Must have working system to create bootable media or have created it in advance
 - Useful when computer will not boot normally

Free Update Scanner



124 programs

Finds applications where an update is available

Ninite Updater

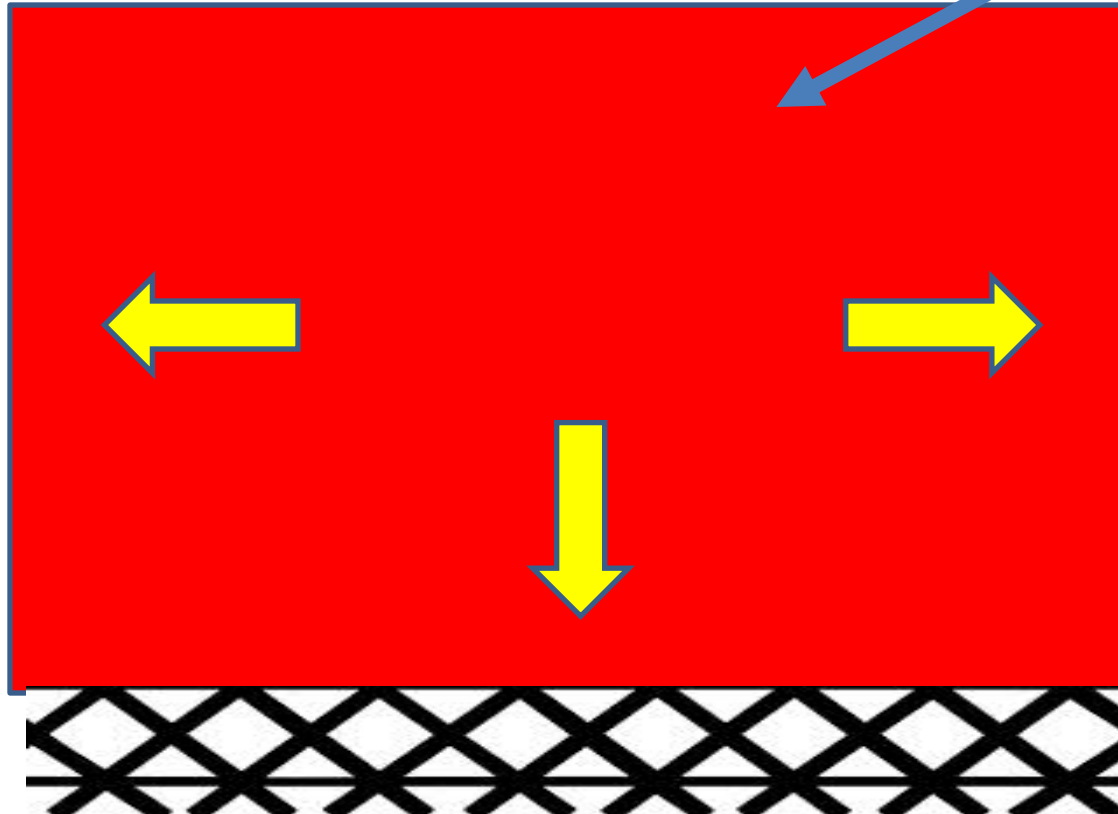
- Ninite Updater—from the makers of the awesome Ninite
- It has a sizeable database of apps, including all of the apps you can get for the Ninite installer, plus a few others that aren't on the list (like AutoHotkey).
- Cost \$10 per year

Enhanced Mitigation Experience Toolkit (EMET)

- Free Microsoft product can be downloaded from Microsoft website
- Enhances application security, estimated to cause 80-90% of exploits to fail
- Very powerful technology that reduces attack surface
- Protects against many vulnerabilities related to

EMET Concept

Vulnerable application



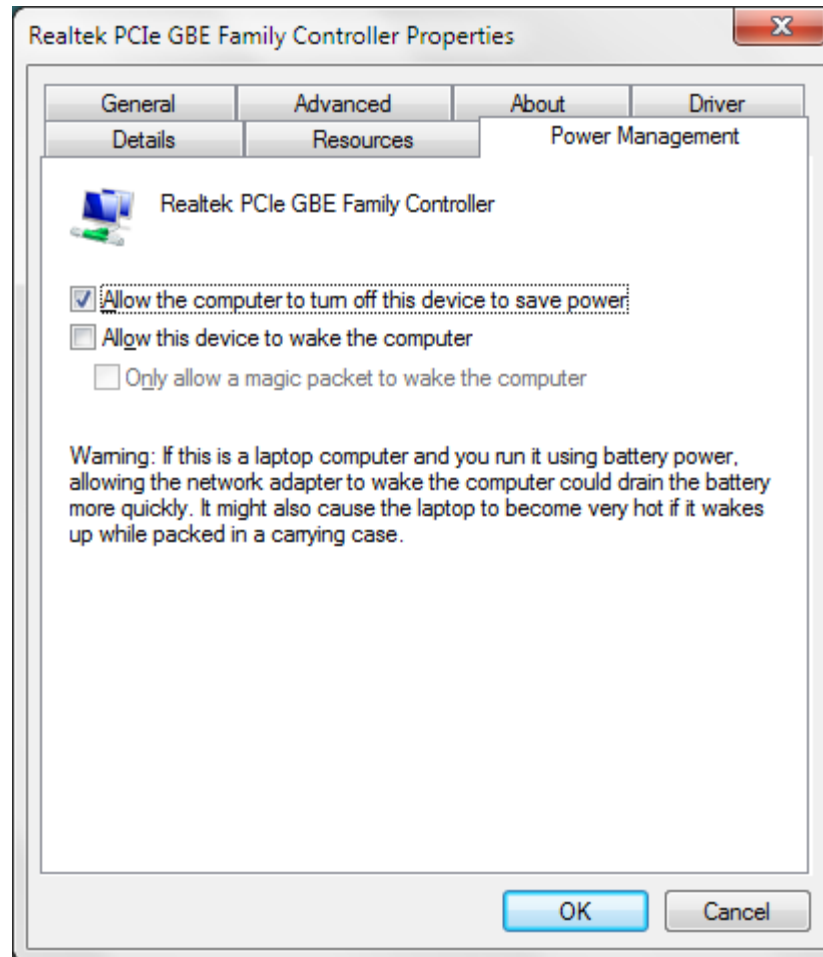
EMET Security Measures

Mitigation Techniques

EMET Security Mitigations	Included
Attack Surface Reduction (ASR) Mitigation	✓
Export Address Table Filtering (EAF+) Security Mitigation	✓
Data Execution Prevention (DEP) Security Mitigation	✓
Structured Execution Handling Overwrite Protection (SEHOP) Security Mitigation	✓
NullPage Security Mitigation	✓
Heapspray Allocation Security Mitigation	✓
Export Address Table Filtering (EAF) Security Mitigation	✓
Mandatory Address Space Layout Randomization (ASLR) Security Mitigation	✓
Bottom Up ASLR Security Mitigation	✓
Load Library Check – I	
Memory Protection C	
Caller Checks – Return	
Simulate Execution Flow – Return Oriented Programming (ROP) Security Mitigation*	✓
Stack Pivot – Return Oriented Programming (ROP) Security Mitigation	✓

Mandatory Address Space Layout Randomization (ASLR) Security Mitigation

Turn Off Allow Network Traffic To Wake Computer



Passwords

- Still most common means of authentication
- A password is a one factor means of authentication: something you know
- A multi-factor means of authentication includes multiple things you know like your mother's maiden name or something you have like an RSA token, or a token sent to your smartphone
- Passwords are subject to multiple types of attacks
- Construct your userid as a password, i.e., hard to guess

Password Vulnerabilities

- Use of easily guessed dictionary words, proper names, or common passwords (Pa\$\$word1)
- Use of short password that can be cracked using brute force (trying all combinations)
- Social network attacks
 - Glean password information from social media: dog's name, date of birth, etc.
- Exploit vulnerabilities in password reset or recovery procedure

Password Cracking Approaches

- Social networking: Facebook, LinkedIn, etc. reveal personal information used for password
- Brute force attack: try all combinations, answer found after searching half of all combinations
- Exploit use of proper names, syntactic tendencies, foreign words, commonly used passwords

Password Best Practices

- At minimum must have different passwords for sensitive sites (financial) and all others
- Passwords should be 12 characters and hard to guess, don't use phone number, birth date , or street address
- Use password program protected by strong password and encryption to store all passwords, e.g., ewallet or write down
- Userid ID should be viewed as another password; where allowed don't use your name
- Mother's maiden name and place of birth should be fictitious e.g., Olympus Queen, Isle of Doom

Password Pitfalls

- 1. Any part of your name
- 2. Your account name (this is a hanging offence)
- 3. Any part of the name of a member of your extended family (inc. pets) or, worse, a colleague
- 4. 17. Anything containing letters of the alphabet only
- 5. Name of operating system
- 6. Significant numbers (phone number, car license number)
- 7. Place names
- 8. Favorite or most-hated things

Password Pitfalls

- 9. Easy associations with favorites or most-hated things: for instance "Swan_Lake" is a bad password for a ballet freak
- 10. Any correctly spelled English word, especially one which is likely to be recognized by UNIX spell, application spell-checkers etc.
- 11. Any correctly spelled non-English word: exceptions may be acceptable in Urdu, any non-Mandarin dialect of Chinese, or Catalan, as long as they're not in languages you're *known* to speak
- 12. Song-titles, famous people, cartoon characters etc. Particularly avoid 'CharlieBrown', 'Snoopy', 'Kirk', 'Spock', 'McCoy', 'Garfield' and 'Doonesbury': well, you get the idea...

Password Pitfalls

- 13. Anything which is all upper case or lower case (unless the system is case insensitive!)
- 4 Anything with the first or last character uppercase and the rest lower case
- 15. Anything you've come across as a textbook example
- 16. Any significant numeric string, e.g. phone numbers, birthdates
- 17. Anagrams of any of the above, especially simple reversals etc.
- 18. Obvious variations such as appending or prepending a digit to one of the above or an anagram thereof

Most Popular Passwords of 2013

- | | |
|--------------------------------|----------------------------|
| 1. <i>password</i> (Unchanged) | 14. <i>sunshine</i> (Up 1) |
| 2. <i>123456</i> (Unchanged) | 15. <i>master</i> (Down 1) |
| 3. <i>12345678</i> (Unchanged) | 16. <i>123123</i> (Up 4) |
| 4. <i>abc123</i> (Up 1) | 17. <i>welcome</i> (New) |
| 5. <i>qwerty</i> (Down 1) | 18. <i>shadow</i> (Up 1) |
| 6. <i>monkey</i> (Unchanged) | 19. <i>ashley</i> (Down 3) |
| 7. <i>letmein</i> (Up 1) | 20. <i>football</i> (Up 5) |
| 8. <i>dragon</i> (Up 2) | 21. <i>jesus</i> (New) |
| 9. <i>111111</i> (Up 3) | 22. <i>michael</i> (Up 2) |
| 10. <i>baseball</i> (Up 1) | 23. <i>ninja</i> (New) |
| 11. <i>iloveyou</i> (Up 2) | 24. <i>mustang</i> (New) |
| 12. <i>trustno1</i> (Down 3) | 25. <i>password1</i> (New) |
| 13. <i>1234567</i> (Down 6) | |

Challenge of Multiple/Long Passwords

- Create from phrase: This is a way to generate long passwords that are easy to remember
- However it contains this distribution:
 - Consonants: t, w, t, g, l, p, t, t, r
 - Vowels: i, a, a, e,
- Distribution is unbalanced and exploitation of syntactic tendencies provides an avenue to break more quickly

eWallet Pseudo Password Generator

Random

\$@1#(=2Q!@5S

\$jIO2r&Y#508

(e(P#540M#-y

Mnemonic

Ua5hngaNhp-

ErwaDcchZ88=

(TUubDajXo96(

Pronounceable

SegeOwaud&!6

TuzBydvof-&\$

(Evdecselm5(0

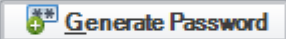
Generate Password

Select options below for the type of password you'd like to create and then click Generate Password.

Password Length:

Allowed Characters

☒ Lowercase Letters (a-z)
☒ Uppercase Letters (A-Z)
☒ Numbers (0-9)
☒ Punctuation ☐ None
☐ Mnemonic Sentence
☐ Pronounceable
☐ Dictionary ☐ Warped



Generated Password:

Memory Aid:

Anti-Virus Programs 1/2

- Anti-virus program with current signatures is essential
- These scan for malware using virus definitions and behavior heuristics
 - Definitions include signature files containing patterns of previously discovered malware
 - Heuristics attempt to identify types of actions that can compromise an operating system or application
- Malware found by an anti-virus program can be quarantined and deleted

Anti-Virus Programs 2/2

- Anti-virus programs are rated by their detection rate against various benchmarks
- Typical detection rates are in the 80-90% range
- Anti-virus program can flag a program as malicious that is not (called a false positive)
- Only one anti-virus can be installed at a time
- Freeware anti-virus software is available, AVG.com
- Reviews at CDNET, ZDNET, many other sites

tube.com/results?search_query=anti%20virus%20programs&sm=3

arks

virus programs



Filters

About 54,000 results

Did you mean: [antivirus programs](#)



Best Antivirus 2012/2013 - TOP 10 Antivirus 2012/2013 Review

by [TopTenAuthority](#) • 2 years ago • 229,146 views

Full Comparison Chart: <http://www.toptenauthority.com/Antivirus-Software> SAVE 30% off Bitdefender. Enter 30OFFTOPTEN during ...

HD



TOP 5 - Best Free AntiVirus 2013

by [Marc Meerbeek](#) • 1 year ago • 233,294 views

In this video I will show you the best free **antivirus** 2013. I will show the installer and interface for each top free **antivirus** More info: ...

HD



How to install AVG - Virus Removal- Free Antivirus Protection 2014

by [nickscomputerfix](#) • 9 months ago • 22,259 views

See how to install AVG 2014 **Virus** protection for FREE. Get outstanding basic protection for internet surfing and emailing. Get the ...

HD



Best Free Mac Anti-Virus App

by [Tekzilla](#) • 5 months ago • 4,745 views

Mike wrote in asking what if OS X had **anti-virus programs** available. Avast! Free Anti-Virus for Mac is our fav for free OS X ...

Spyware

- **Spyware** is software that aids in gathering information about a person or organization without their knowledge..., or that asserts control over a computer without the consumer's knowledge.
- Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information

Spyware Scanners

- Find and disable spyware, complement anti-virus program
- Typically, free and paid versions available
- Can interfere with anti-virus programs
- Only one spyware program can run at a time
- Most popular are Spybot and Malwarebytes

Spybot Scan Results

System Scan (Spybot - Search & Destroy 2.2)

Tasks Associated Tasks Online Help

System Scan

- Start a scan
- Pause scan
- Stop scan
- Fix selected
- Save scan log...
- Show previous logs
- Clean temporary files
- Help

Please Donate!

If you like free software and free support you can maintain this with your donation.

[Donate now](#)

[Hide](#)

Details

Select a threat in the results list to see details here.

Scan for malware [Show Info](#)

Description	Location	Threat Level	Type	Category	Rule#
Toolbar.Snap.do					
<input checked="" type="checkbox"/> Settings	HKCR\CLSID\{AE07101B-46D4-4A98-...	<div><div></div></div>	Registry Key	PUPSC	B8DD52AF
<input checked="" type="checkbox"/> Settings	HKCR\CLSID\{AE07101B-46D4-4A98-...	<div><div></div></div>	Registry Key	PUPSC	B8DD52AF
<input checked="" type="checkbox"/> User settings	HKUS\S-1-5-21-3053036278-33289432...	<div><div></div></div>	Registry Key	PUPSC	8A184072
<input checked="" type="checkbox"/> IE toolbar	HKLM\SOFTWARE\Microsoft\Internet...	<div><div></div></div>	Registry Value	PUPSC	2A1CCFF9
<input checked="" type="checkbox"/> IE toolbar	HKLM\SOFTWARE\Microsoft\Internet...	<div><div></div></div>	Registry Value	PUPSC	2A1CCFF9
Macromedia.FlashPlayer.Cookies					
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750
<input checked="" type="checkbox"/> Text file	C:\Users\dvenese\AppData\Roaming\...	<div><div></div></div>	File	Tracks	6AA61750

[Back to overview](#)

Scan finished.
72 results.

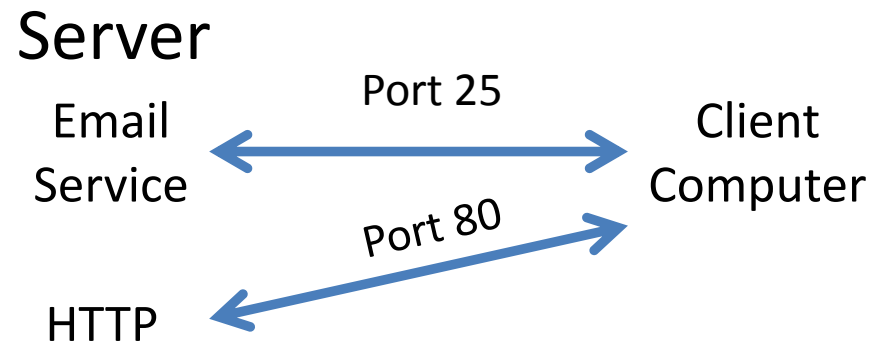
[Start a scan](#)

[Fix selected](#)

Scan finished. 72 results. Scan took 22:24 minutes.

TCP Ports

- Network services use an established logical TCP port to communicate with a computer
- Similar to a switchboard where two parties are connected



Port Scanning

- Malicious programs constantly scan Internet looking for ports vulnerable to attack
- Firewall programs lock down (X) unused ports and do not respond to scan requests

Inbound Rules						
Name	Group	Profile	Enabled	Action	Over	
✓ Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Private...	No	Allow	No	
✓ Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No	Allow	No	
✓ Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	No	Allow	No	
✓ Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Private...	No	Allow	No	
✓ Remote Assistance (DCOM-In)	Remote Assistance	Domain	Yes	Allow	No	
✓ Remote Assistance (PNRP-In)	Remote Assistance	Public	Yes	Allow	No	
✓ Remote Assistance (PNRP-In)	Remote Assistance	Domai...	Yes	Allow	No	
✓ Remote Assistance (RA Server TCP-In)	Remote Assistance	Domain	Yes	Allow	No	
✓ Remote Assistance (SSDP TCP-In)	Remote Assistance	Domai...	Yes	Allow	No	
✓ Remote Assistance (SSDP UDP-In)	Remote Assistance	Domai...	Yes	Allow	No	
✓ Remote Assistance (TCP-In)	Remote Assistance	Domai...	Yes	Allow	No	
✓ Remote Assistance (TCP-In)	Remote Assistance	Public	Yes	Allow	No	
✓ Remote Desktop - RemoteFX (UDP-In)	Remote Desktop - RemoteFX	All	No	Allow	No	
✓ Remote Event Log Management (NP-In)	Remote Event Log Manage...	Domain	No	Allow	No	
✓ Remote Event Log Management (NP-In)	Remote Event Log Manage...	Private...	No	Allow	No	
✓ Remote Event Log Management (RPC)	Remote Event Log Management	Domain	No	Allow	No	
✓ Remote Event Log Management (RPC)	Remote Event Log Manage...	Private...	No	Allow	No	
✓ Remote Event Log Management (RPC-EP...	Remote Event Log Manage...	Domain	No	Allow	No	
✓ Remote Event Log Management (RPC-EP...	Remote Event Log Manage...	Private...	No	Allow	No	

Example of default firewall rules

UPnP Exposure

- “UPnP is a protocol designed to automatically configure networking equipment without user intervention
- Vulnerable products include webcams, printers, security cameras, media servers, smart TVs and routers
- ... scans show over 23 million devices vulnerable to a remote code execution flaw”

<http://nakedsecurity.sophos.com/2013/02/05/upnp-flaws-turn-millions-of-firewalls-into-doorstops/>

Port Scanner

- Gibson Research Corporation (GRC) has been providing a free online tool to scan your router for open ports for over ten years. This tool is called Shields Up. The UPnP Exposure test will check to see if your router is open to a new router exploit that gives hackers the ability to access and control your router.



Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Universal Plug n'Play (UPnP) Internet Exposure Test

This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address (**71.255.254.129**) in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were **never** designed to be exposed to the public Internet, and **any** Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.

Your equipment at IP:

71.255.254.129

Is now being queried:



THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!

(That's good news!)

Server Port Test

The screenshot displays the 'Server Port Test' tool on the website www.whatsmyip.org/port-scanner/server/. The browser's address bar and tabs are visible at the top. The tool's interface includes a sidebar with 'Networking Tools' and 'Text Related Tools'. The main area shows a progress bar at 100% and a 'Re-Scan' button. Below this is a table with three columns: Application, Port, and Status. All scanned ports are marked as 'Timed-Out'.

Application	Port	Status
FTP	21	Timed-Out
SSH	22	Timed-Out
Telnet	23	Timed-Out
Mail [SMTP]	25	Timed-Out
DNS	53	Timed-Out
Web Server [HTTP]	80	Timed-Out
Mail [POP]	110	Timed-Out
netbios	137	Timed-Out
netbios	138	Timed-Out
netbios	139	Timed-Out
Mail [IMAP]	143	Timed-Out
Web Server [HTTPS]	443	Timed-Out

<http://www.whatsmyip.org/port-scanner/>

Application Port Test

WhatsMyIP.org | Application Port Test - Google Chrome

www.whatsmyip.org/port-scanner/apps/

Apps Suggested Sites Amazon.com - Onli... HP - See What's Hot HP Games Web Slice Gallery Bookmarks

Application Port Test

Home / Port Scanners / Application Ports

Like 482 Tweet 36 +1 143

Progress: 100% [Re-Scan](#)

Application	Port	Status
TCP/IP Printer Sharing	515	Timed-Out
TCP/IP Printer Sharing	631	Timed-Out
Apple Remote Desktop	3282	Timed-Out
Windows Remote Desktop	3389	Timed-Out
AOL Instant Messenger [AIM]	5190	Timed-Out
Yahoo Instant Messenger	5050	Timed-Out
Yahoo IM File Transfer	4443	Timed-Out
MSN Messenger	1863	Timed-Out
MSN Messenger File Transfer	6891	Timed-Out
MSN Messenger App Sharing	1503	Timed-Out
PC Anywhere	5631	Timed-Out
PC Anywhere	5632	Timed-Out
VNC	5900	Timed-Out

Networking Tools

- More Info About You
- Port Scanners
- Traceroute
- HTTP Compression
- Ping
- WHOIS & DNS
- Website Ranking
- IP Location
- HTTP Headers

Text Related Tools

- Short URL Machine
- HTML Characters
- String to Timestamp
- Hash Generator
- Text Case Changer

WhatsMyIP.org Ap....htm

WhatsMyIP.org Ser....htm

choosing_your_pass....pdf

Problematic-Unlove....pdf

EsetWP-DodgeCyber....pdf

Show all downloads...

Peer to Peer Port Test

WhatsMyIP.org | P2P Port Test - Google Chrome

www.whatsmyip.org/port-scanner/p2p/

Apps Suggested Sites Amazon.com - Onli... HP - See What's Hot HP Games Web Slice Gallery Bookmarks

P2P Port Test

Home / Port Scanners / P2P Ports

Like 482 Tweet 36 +1 143

Progress: 100% Re-Scan

Application	Port	Status
USENET	119	Timed-Out
Direct Connect	375	Timed-Out
Direct Connect	425	Timed-Out
Kazza, FastTrack	1214	Timed-Out
DC++	412	Timed-Out
DC++	1412	Timed-Out
DC++	2412	Timed-Out
eDonkey	4661	Timed-Out
eDonkey	4662	Timed-Out
eDonkey	4665	Timed-Out
Hotline Server	5500	Timed-Out
Gnutella, LimeWire, Acquisition	6346	Timed-Out
BitTorrent	6881	Timed-Out

Networking Tools

- More Info About You
- Port Scanners
- Traceroute
- HTTP Compression
- Ping
- WHOIS & DNS
- Website Ranking
- IP Location
- HTTP Headers

Text Related Tools

- Short URL Machine
- HTML Characters
- String to Timestamp
- Hash Generator
- Text Case Changer

WhatsMyIP.org Ap....htm

WhatsMyIP.org Ser....htm

choosing_your_pass....pdf

Problematic-Unlove....pdf

EsetWP-DodgeCyber....pdf

Show all downloads...

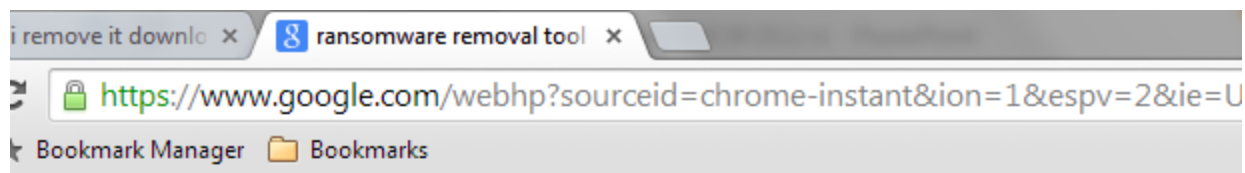
How to Harden Your Browser

- Browser plugins
- Browser settings

Browser Strategy

- One of the main avenues for infection
- Use of plugins can restrict functionality on many websites, cookies or Javascript may be required
- Many plugins have overlapping functionality
- Recommendation is to use a locked down Chrome as default browser and IE when compatibility problems encountered
- Beware request to install plugins when web surfing
- Use a non-administrative account when browsing
- Install latest product version
- Check site reputation at webutation.com. Beware if no information available

Web of Trust



Ransomware Infection. Many of these websites are focused on promote and ...

FBI Moneypak Ransomware - from Wiki-Security, a source ...

www.wiki-security.com/wiki/Parasite/FBIMoneypakRansomware/

Learn how to detect and remove FBI Moneypak Ransomware on your PC. ... future spyware attacks, we recommend you buy SpyHunter's spyware removal tool, ...

How to Remove Cryptorbit Ransomware (Removal Solved ...

www.malwareexperts.com/ransomware

Feb 5, 2014 - Learn how to remove Cryptorbit Ransomware from a Windows Vista, 7, ... to disarm this self-preservation tool that Cryptorbit Ransomware has.

Remove Ransomware Virus.

Ad www.spywareremove.com/

How to Remove Ransomware Malware. Ransomware Removal Instructions.
Remove Mysearchdial Virus - Remove Ukash Virus. - Remove Redirect Virus

Best 10 Virus Removers

Ad www.top10antivirussoftware.com/Removal

Compare Top 10 Security Software. Protect Your PC Against Viruses Now

Removal Of Ransomware

Ad www.wow.com/Removal+Of+Ransomware

Search for Removal Of Ransomware Look Up Quick Results Now!

Dangerous site

- Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

- Administrator

Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

Why is a standard account recommended?

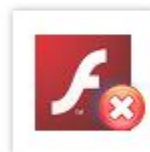
Check your browser.

Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.

[Install Plugin](#)[Scan without installing plugin](#)

Check your browser and system security

Click the "Install Plugin" button to enable fast, safe scanning.



Find vulnerabilities at the click of a button

Scan and view all security issues in an easy-to-understand detailed list.

[Fix It](#)

Take charge of any issues found

Follow recommended steps to resolve each vulnerability found.

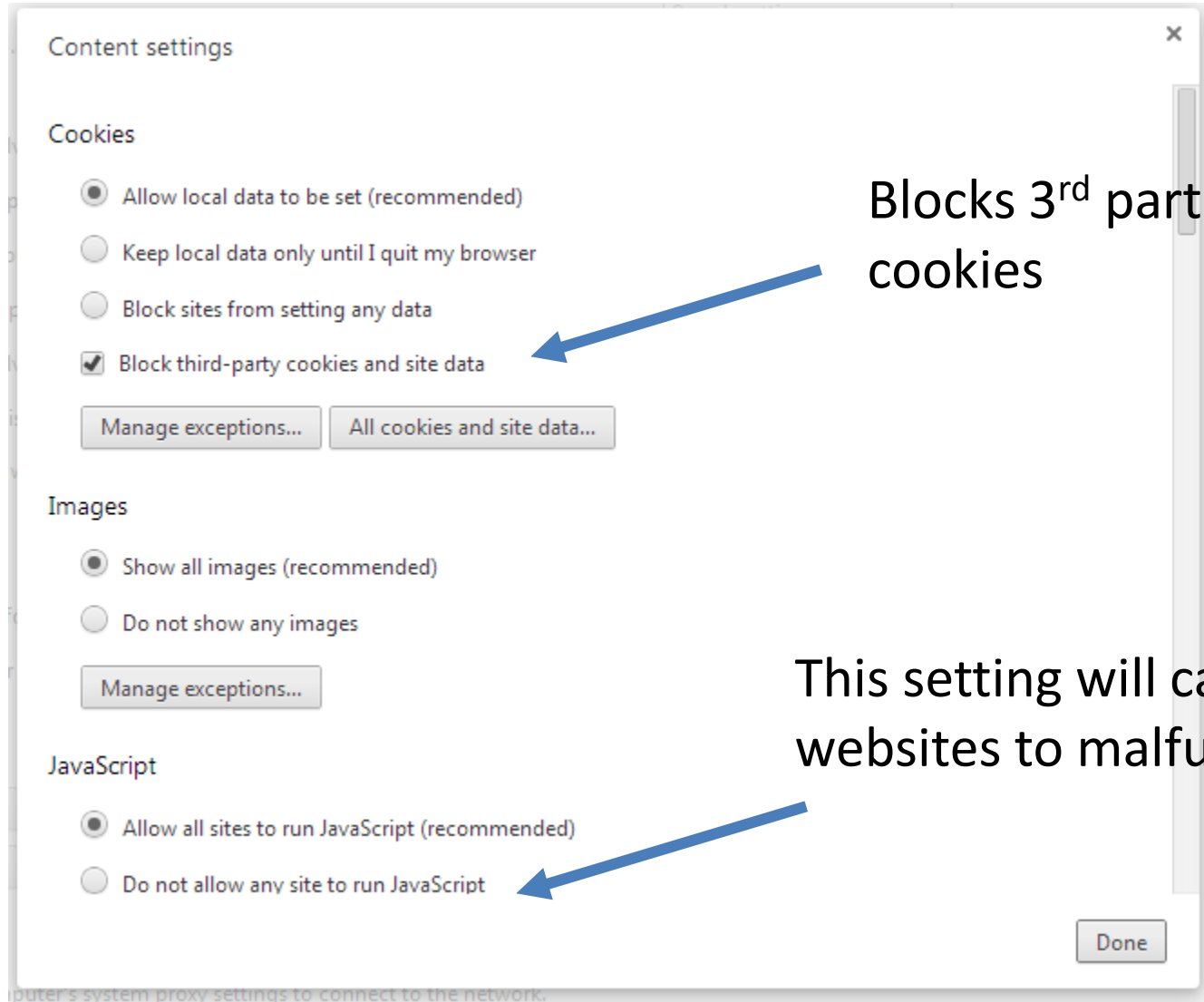
Browser Plug-ins for Security/Privacy

- Plug-in, a program that works as extension to a browser such as Chrome, Internet Explorer, or Firefox
 - Recommended Chrome Plug-ins:
 - **Ghostery** summarizes ad networks and tracking scripts on any given site
 - **KB SSL Enforcer** ensures a secure connection (SSL) is used when available
 - **AdBlock** Plus blocks pop-up ads
 - **Web of Trust** provides site safety rating
 - **(Optional) ScriptSafe** prevents javascript from running without permission

Chrome Browser Settings

- Modify Adobe flash player settings to make sure that third-party flash cookies are disabled
- Remove Java plugin if installed
- For privacy concerns use an anonymous browser such as startpage
- Set option for do not track (voluntary request of limited value)

Chrome Browser Settings



Resources

- Sites of major anti-virus vendors
(many offer free virus removal tools, security guides)
 - Norton, McAfee, F-Secure, Kaspersky
- us-cert.gov/, current security threats, critical updates
- Internet IP lookup
 - www.geobytes.com/IpLocator.htm
 - www.whatismyip.com/ip-address-lookup/

Reviews/Downloads of Security Software

- CNET.com, large repository (contains free software that often includes potentially unwanted software (PUPs) e.g., browser hijacker: conduit.com
- Check reputation of free programs before installing
- pcmag.com, software reviews, downloads
- sourceforge.net:, wide array of open source geared to computer professionals, server environments

sourceforge.net/directory/security-utilities/os:windows/freshness:recently-updated/

Manager [Bookmarks](#)

[Home](#) / [Browse](#) / [Security & Utilities](#)

Advanced

Filters

OS: **Windows** x

Freshness: **Recently updated** x

Security & Utilities

Sort By: **Most Popular**

[Archiving](#)

[Security](#)

[File Transfer Protocol \(FTP\)](#)

[Power \(UPS\)](#)

[Terminals](#)

[Log Analysis](#)

[Log Rotation](#)

[File Management](#)

Showing page 1 of 52.



FileZilla

The free FTP solution
553,323 weekly downloads



Anti-Spam SMTP Proxy Server

The Anti-Spam SMTP Proxy (ASSP) Server project aims to create an o...
290,672 weekly downloads



Scrollout F1 email gateway

Secure email servers easy
152,168 weekly downloads



KeePass Password Safe

KeePass - A free open source password manager.
106,269 weekly downloads



ophcrack

Ophcrack is a Windows password cracker based on a time-memory t...
69,371 weekly downloads



WinMerge

Windows visual diff and merge for files and directories
38,678 weekly downloads



Staff Picks



[FileZilla](#)



[GroundWork Monitor Comr](#)



[Hydrogen](#)



[iText®, a JAVA PDF library](#)



[iTextSharp, a .NET PDF lib](#)



[JSToolNpp](#)



[Little cms color engine](#)



[OGRE \(O-O Graphics Rend](#)



[Apache OpenOffice](#)



[Pandora FMS: Flexible Mo](#)



[Pinguy OS](#)



[PostBooks ERP, accountir](#)



[TigerVNC](#)

How to Find Utilities, Security Guides, Security help

- Google and youtube are your friends
 - “anti virus reviews”
 - “browser hardening”
 - “malware removal guide”
 - “free anti virus software”
 - “spyware removal”
 - “best password practices”

Guides for Malware Removal

- How to Know If Your Computer Is Infected
- Best Computer Security Sites
- Clean 64-bit machine
- Elitekiller
- Select Real Security
- Majorgeeks other
- Bleepingcomputer
- Geeks to Go
- Deletemalware
- Remove-Malware.com
- overclock.net
- MakeUseOf
- Where malware hides?
- How to remove a virus when your computer won't work
- How to Remove a Rootkit from a Windows System
- Kaspersky

Malware removal tools can damage systems

Ransomware Removal

- Kaspersky Windows
Unlocker Banner Removal
- Fsecure labs
global/removal-instructions
- Bitdefender
- Symantec
- Norton
- Try windows restore to roll-back before ransomware installed

https://www.google.com/search?q=guidance+on+malware+detection+and+removal&rlz

gested Sites Amazon.com - Onli... HP - See What's Hot HP Games Web Slice Gallery Bookm

About 16,200,000 results (0.45 seconds)

Microsoft resources and guidance for removal of malware a...

support.microsoft.com/kb/2671662 Microsoft Corporation

Microsoft resources and **guidance** for **removal** of **malware** and viruses. Print ... The **scan** is free and will **detect and remove** many of the issues that customers ...

Free Malware Removal Tool | Anti-Malware Scan Software ...

www.microsoft.com/.../pc.../malware-removal.asp... Microsoft Corporation

The Malicious Software **Removal** Tool is used for **malware removal**. Stay up-to-date with anti-**malware** software to protect your Windows computer and **remove malware**. ...

Get password **guidance**. Create stronger passwords · Help protect your ...

Download Malicious Software ... - Malware families cleaned by ... - Win32/Simda

Spyware Removal Guide - Gizmo's Tech Support Alert

https://www.techsupportalert.com/content/spyware-removal-guide.htm

Oct 26, 2013 - This **malware removal guide** provides **guidance** on how to **remove** ... you attempt to **remove malware** from your computer, but also **scan** the disk ...

[PDF] MALWARE REMOVAL GUIDE Malware Detection and ...

www.inf.ed.ac.uk/.../MalwareRem... United States Department of Education

MALWARE REMOVAL GUIDE. Malware Detection and Removal on Windows. There are a number of free tools that can help with this. None of them are perfect, ...

Rootkit and malware detection and removal guide

www.computerweekly.com/.../Rootkit-and-malware-d... Computer Weekly

are_re....pdf

Free Virus Removalhtm

Chinese hacker crac....htm

YouTube




pc security for windows 7



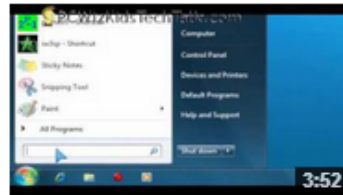
- What to Watch
- My Channel
- My Subscriptions
- Social
- History
- Watch Later

SUBSCRIPTIONS

-  Drawing - Topic 15
- Browse channels
- Manage subscriptions

Filters

About 304,000 results



Windows 7 - Security Features

by **PCWizKids Tech Talk** • 4 years ago • 27,965 views

Whats New with **Windows 7's security** features? Well let me tell you that you still need an AntiVirus software installed but thats ...

OFFICIAL HD



How to Improve PC Security with Windows 7 Action Center For Dummies

by **fordummies** • 3 years ago • 5,626 views

Use Windows 7 Action Center to improve **PC security**. Windows 7 Action Center flags any PC problems it notices and provides ...



Microsoft Security Essentials -Best Free AntiVirus For Windows XP/Vista/7/8 [Tutorial]

by **shirazistudios** • 7 months ago • 4,870 views

This is a beginners tutorial on how to install and use Microsoft **Security Essentials**, the free anti-virus program from Microsoft.

HD



Learn Windows 7 - Microsoft Security Essentials

by **mahalodotcom** • 3 years ago • 9,575 views

In this video, Mahalo's **Windows** expert Sean Hewitt discusses Microsoft **Security Essentials**. Installing Microsoft **Security** ...

HD

Browser Hardening Guides

- cert.org/historical/tech_tips/securing-web-browser-index.cfm
- insanitybit.com/2012/06/02/the-definitive-guide-for-securing-chrome/
- techsupportalert.com/content/how-harden-your-browser-against-malware-and-privacy-concerns.htm

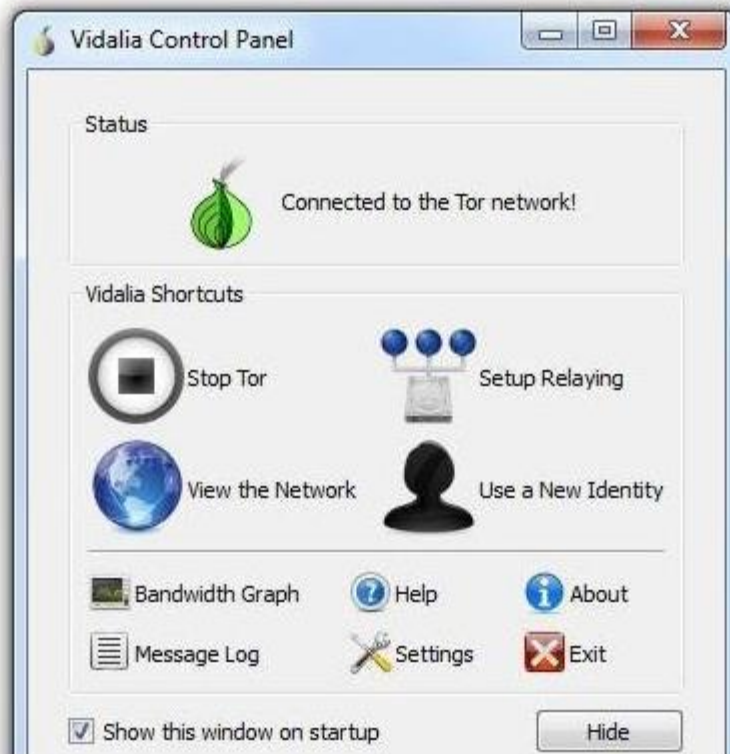
Anonymous Browsing

DOWNLOADS

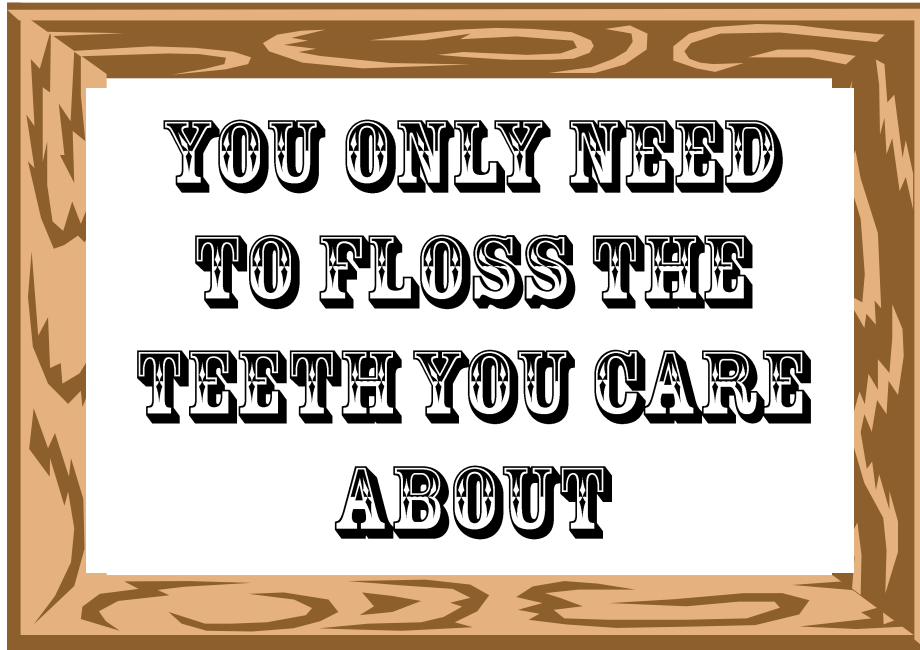
Tor Browser Bundle

★ REVIEW

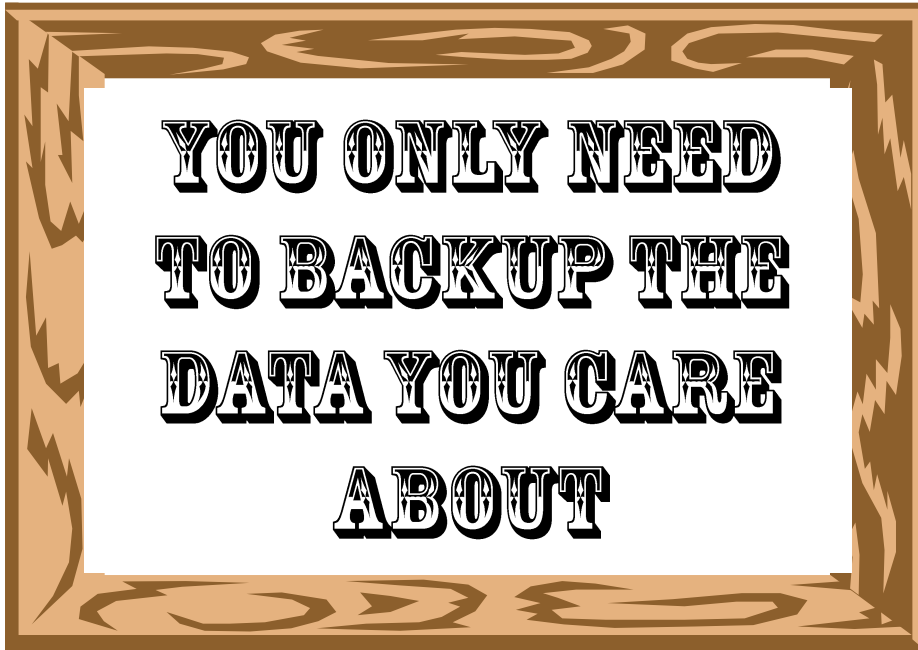
≡ PRODUCT SPECS



Sign in my Dentist's Office



My Version



A backup is your best protection
against file loss or corruption

How to Backup

- Local media: CD/DVD, external/internal hard drive, paper
- Another computer
- Cloud service
- Network or directly connected device

What to Backup

- Emails
- All or selected files, videos, music, photos
- Settings, such as bookmarks
- Image of entire disk, includes installed programs

Backup Strategy

- On set schedule e.g., daily, weekly
- File synchronization
- One or multiple data copies
- Off-site storage
- Restoration procedure

Don't let this be you

Recommended Backup Strategy

- Use external disk drives, 1TB available for \$80
- One drive contains a disk image of computer hard drive
 - Allows for easy restore
- Two external disk drives that contain copies of all files of value
- Consider storing a file backup at another location