

*Greensboro Computer Center for Seniors*



[www.greensboroshepnet.org](http://www.greensboroshepnet.org)

# *Security II*

*Your Computer and the Internet*

Here are the things we should be aware of...

- Viruses
- Spyware / Malware
- Other 'things'

# *Viruses*

There are three categories of viruses:

- Instant Viruses
- Trojans
- Worms

## *General precautions about viruses...*

- Be suspicious of email attachments from unknown sources.
- If someone gives you a flash drive – scan it first!
- If someone gives you a CD – scan it first!

*A good and up-to-date antivirus program will stop it all.*

# *Spyware and Malware*

# What are some of the symptoms?

- Lots and lots of popups on the screen.
- Browser redirects to unwanted websites.
- Unable to get to some sites.
- Many times a Window asking for \$ to fix problem.
- Unable to start Antivirus or Malware.
- System gets really slow.

# How do I get these things?

- “Social Engineering”
- Downloading ‘free’ programs
- If it looks too good to be true...it is!

## *What is social engineering?*

Online criminals can use sophisticated technology to try to gain access to your computer, or they can use something simpler and more insidious: social engineering.

The purpose of social engineering is usually to secretly install spyware or other malicious software or to trick you into handing over your passwords or other sensitive financial or personal information.

Some online criminals find it easier to exploit human nature than to exploit holes in the software.

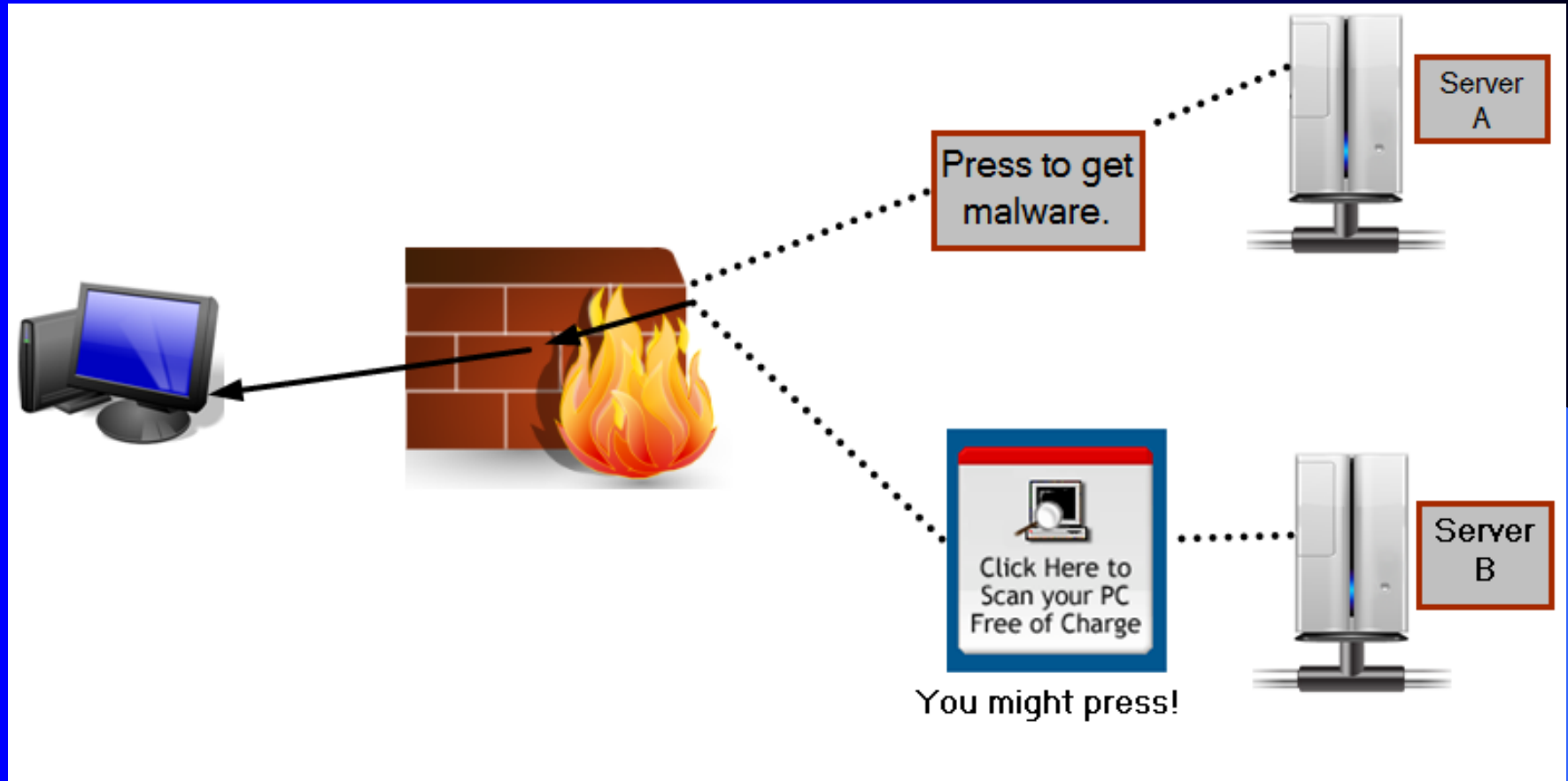
# What does a 'firewall' do?



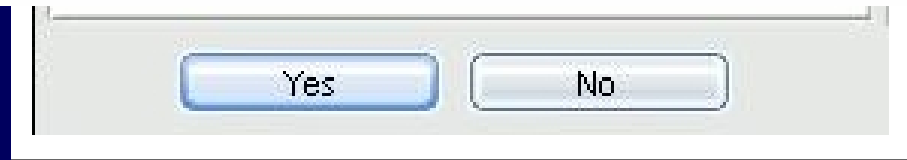
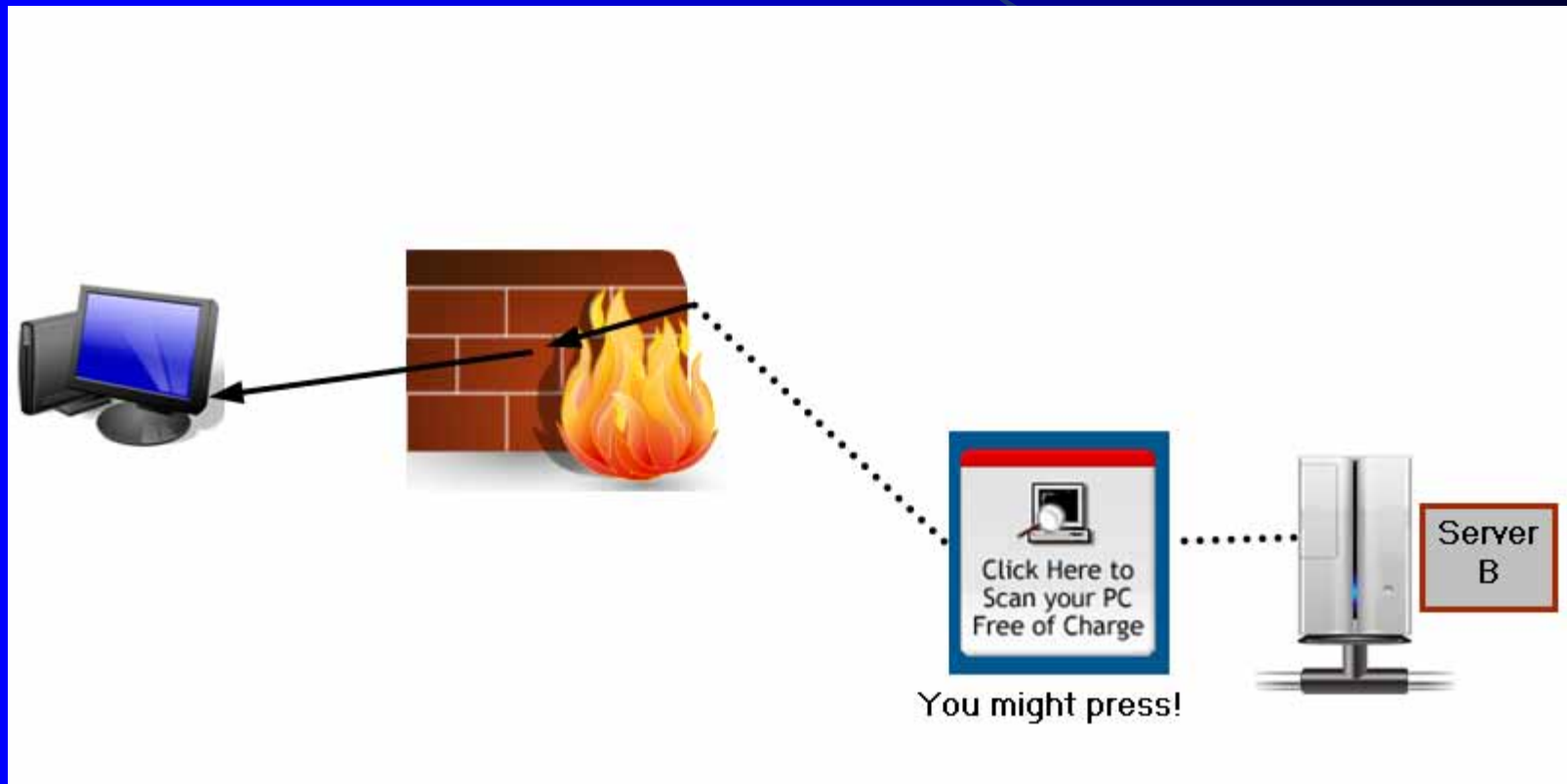
You tell the firewall that if a, b, or c come calling, let them in.

What if d and f come calling? Well...the firewall checks permissions and d and f are not on the list. Entry is *Refused*.

# Example of “Social Engineering”



# “More” of “How do I get these things?”




-  My Computer
-  My Network Places
-  Internet Explorer
-  Privacy center

Support Help

## Privacy center

Simple one-click solution to protect your PC

 Intel(R) Celeron(R) 2.00GHz  
Windows SP (Service Pack 1)

**Database update error**

The database is out of date. Some components are not working correctly. Your security is under threat. Update your software immediately!

[Open update manager](#)

**Security threat!**

The components providing security have reported a critically low level of system protection. Make sure all the components are working correctly.

[Show](#)

**License error!**

The Center for License Control has detected outdated or unsupported software licenses. View the system reports now.


[Open license manager](#)

[Fix all](#)

[www.microsoft.com/privacy](http://www.microsoft.com/privacy)

**Main page > Registry doctor**

**20 dangerous files and (or) privacy violations found**      Security: **0%**

 This component watches the status of the system registry. Outdated signatures slow down system operation and can cause instability or crashing. Besides, many types of spyware use the registry to store their data. Regular cleanups of the registry will provide for stability, security and high operation speed of your computer.

Objects for scanning	Detected errors
Choose registry items to scan	View errors that were deleted
<input checked="" type="checkbox"/> Application paths      1 errors	<input checked="" type="checkbox"/> HKCR CLSID>{42071714-76d4-11d1-8b24-00a0c9068ff3}()
<input checked="" type="checkbox"/> CLSID      1 errors	<input checked="" type="checkbox"/> HKLM SOFTWARE\Security
<input checked="" type="checkbox"/> Help paths      0 errors	<input checked="" type="checkbox"/> HKLM SOFTWARE\Windows 3.1 Migration Status
<input checked="" type="checkbox"/> File extensions      0 errors	<input checked="" type="checkbox"/> HKCU SOFTWARE\Policies
<input checked="" type="checkbox"/> Software settings      4 errors	<input checked="" type="checkbox"/> HKCU SOFTWARE\Classes

**Performing scan**

**Problems detected: 6**

Current registry entry: \\HKCU\SOFTWARE\Classes





# Antivirus XP 2008



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 content. If your homepage was changed or you have strange popups- this is a sure that your computer is infected



Registration

**REGISTER**

We are strongly recommend 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.

Recommendations

Antivirus XP 2008

Continue unprotected

Click here to switch to the Full Mode

Security Center

System Scan

Privacy

Settings

Update

## System info



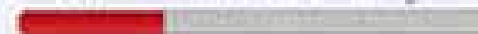
Computer name: FORENSICS

Operating system: Windows XP Professional

Default browser: Windows® Internet Explorer

Protection level: **Low**

Low Medium High



To protect your PC, please register your version of ANG Antivirus, enable automatic updates, and turn privacy features on.

Last scan: 01.03.2009 08:40:34

Total scans: 1

Last Scan Results: **14 threats have been found**

Registration e-mail: **Unregistered**

Registration code: **Unregistered**

ANG AntiVirus 09

**Get full real-time protection Now!**



Update Now

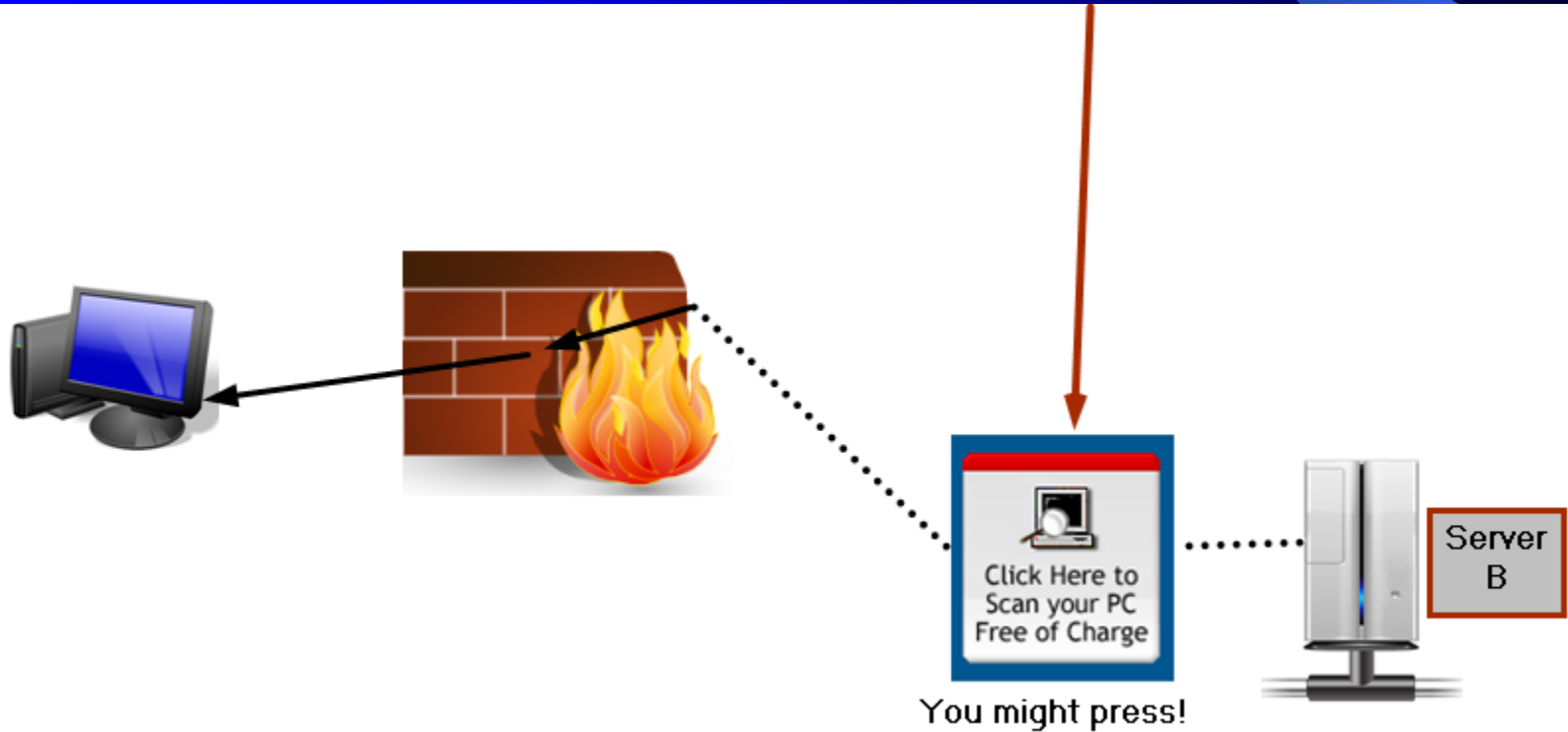
Download the latest protection to help keep your PC safe



Scan Now

Check your computer for viruses and other threats

Learn how to ensure complete system protection with [Windows Security](#).



# What are they trying to do?

- Install malware that steals your data.
- Social engineering to steal personal info.
- Pop-ups with false or misleading info.
- Prevent updates to legitimate security and malware programs.
- Slow down your computer.
- Corrupt files.

Why are they doing this?

Money!



## Crypt programmer

### Рады приветствовать вас на нашем сайте

Приглашаем в нашу команду крипто-программистов **в том числе и программистов без опыта работы** в этой области.

Мы предлагаем:

- Базовую зарплату от 2000\$ в месяц, с увеличением зарплаты в зависимости от качества и оперативности вашей работы.
- Выплаты производятся еженедельно.
- Долгосрочное сотрудничество (с многими программистами мы сотрудничаем уже более двух лет).
- Адекватность.

Пожалуйста, пишите ваши предложения только если вы понимаете о чём идёт речь. Спасибо.

The Russian text in the above ad translates to:

“We invite you to join our team of crypto-programmers, including programmers with no experience in this field.

We offer:

- \* Base salary from \$2,000 per month, with an increase in salary, depending on the quality and timeliness of your work.
- \* Payments are made weekly.
- \* Long-term cooperation (with many programmers, we have been in business for more than two years).

Please fill in your application only if you understand what is at stake. Thank you.”

Other ads, like the one below, seek qualified candidates for similar jobs with a promise of as much as \$5,000 per month for creating custom crypters and providing customer support.

от <b>5000\$</b> в месяц	<b>ТРЕБУЮТСЯ КРИПТОРЫ</b> с постоянной поддержкой
--------------------------	--

# What can you do to help prevent them?

- Good antivirus program – up to date.
- Good pro-active spyware/malware program – up to date.

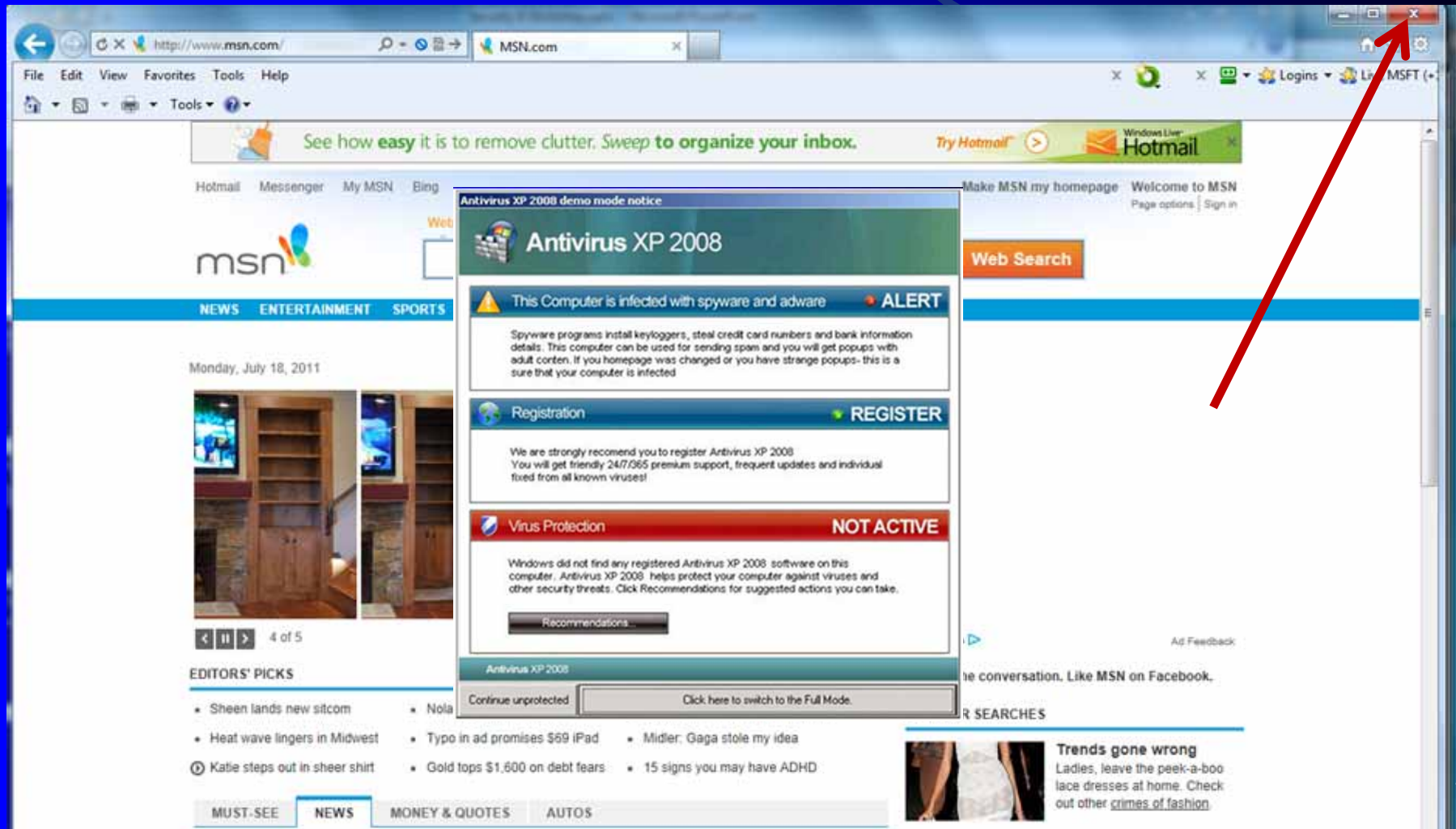
Plus...a few other tips.

# Staying safe online...

1. Don't Panic.
2. Stay up-to-date.
3. Never install software unless you are sure it is safe.
4. Be smart with passwords.

# 1. Don't panic.

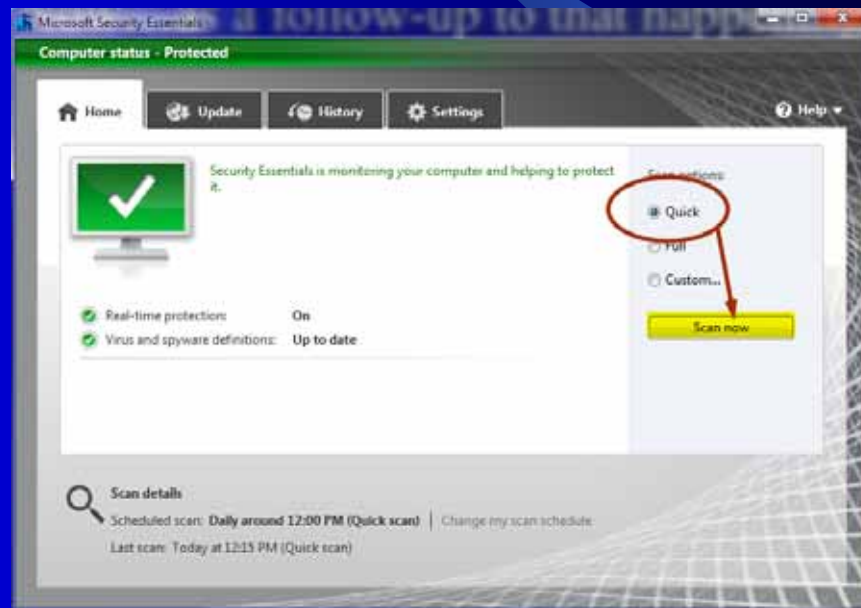
If you see a suspicious window, shut down the Internet Explorer.



# Now...as a follow-up to that happening

You might want to do a Quick Scan with:

- Malwarebytes or whatever program you are using
- Antivirus



*Don't run 3 or 4 spyware programs and a couple of Registry Cleaners. The two steps above are sufficient.*

## 2. Stay up-to-date...

- Set Windows Updates to Automatic.
  - Control Panel
  - System and Security



Windows Update

Turn automatic updating on or off

## Other things to keep updated:

- Adobe Reader
- Adobe Flash
- Quick Time or Real Player
- Java

If you get a notice that something needs updating – go to their website and download the new version.

3. Never install any software unless you're certain it's safe.

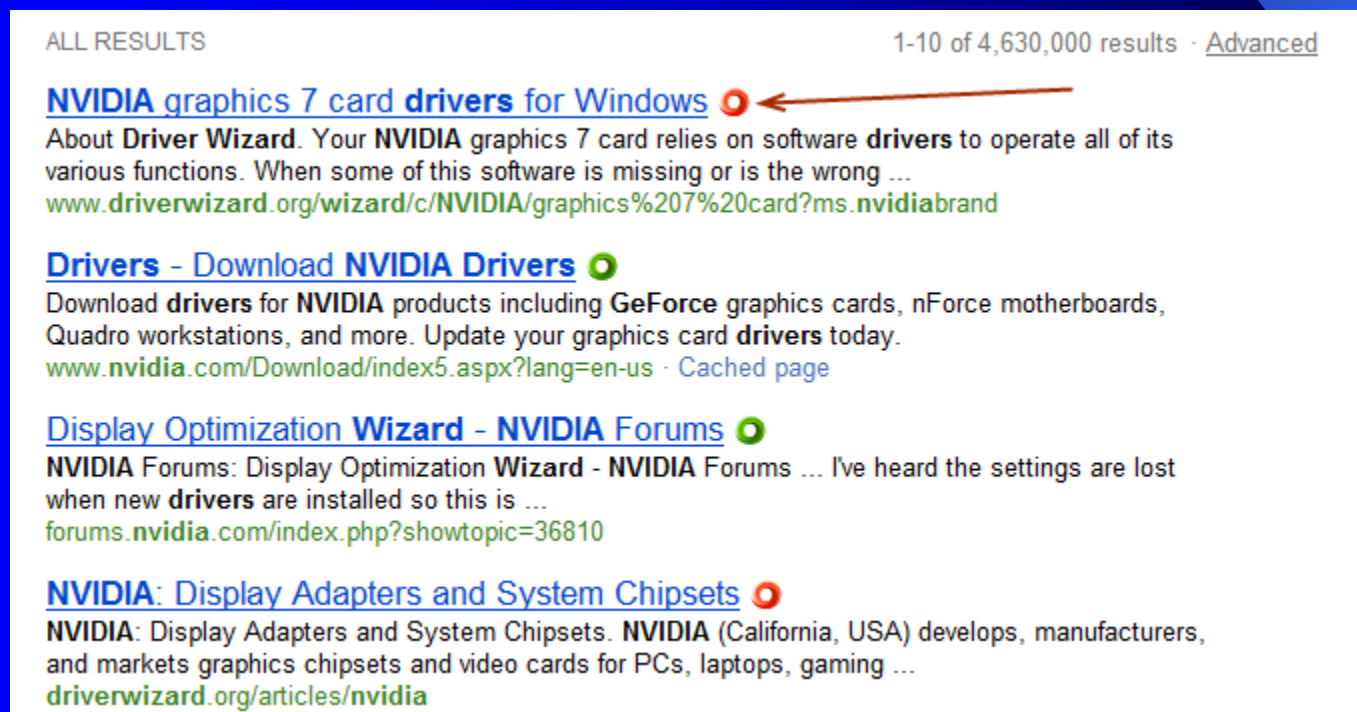
If you have any doubts\* about a software program, you should not install it. Period.

\* Google – “Is the Acme Greeting Card program safe?”


# Let me give you an example of this rule for staying safe online:

A certain unnamed person thought it was time to check and see if he needed to update his drivers for his video card.


He searched NVIDIA drivers and got this:




ALL RESULTS 1-10 of 4,630,000 results · [Advanced](#)

**[NVIDIA graphics 7 card drivers for Windows](#)**  ←


About **Driver Wizard**. Your **NVIDIA** graphics 7 card relies on software **drivers** to operate all of its various functions. When some of this software is missing or is the wrong ...  
[www.driverwizard.org/wizard/c/NVIDIA/graphics%20%20card?ms.nvidia-brand](http://www.driverwizard.org/wizard/c/NVIDIA/graphics%20%20card?ms.nvidia-brand)

**[Drivers - Download NVIDIA Drivers](#)** 

Download **drivers** for **NVIDIA** products including **GeForce** graphics cards, **nForce** motherboards, **Quadro** workstations, and more. Update your graphics card **drivers** today.  
[www.nvidia.com/Download/index5.aspx?lang=en-us](http://www.nvidia.com/Download/index5.aspx?lang=en-us) · [Cached page](#)

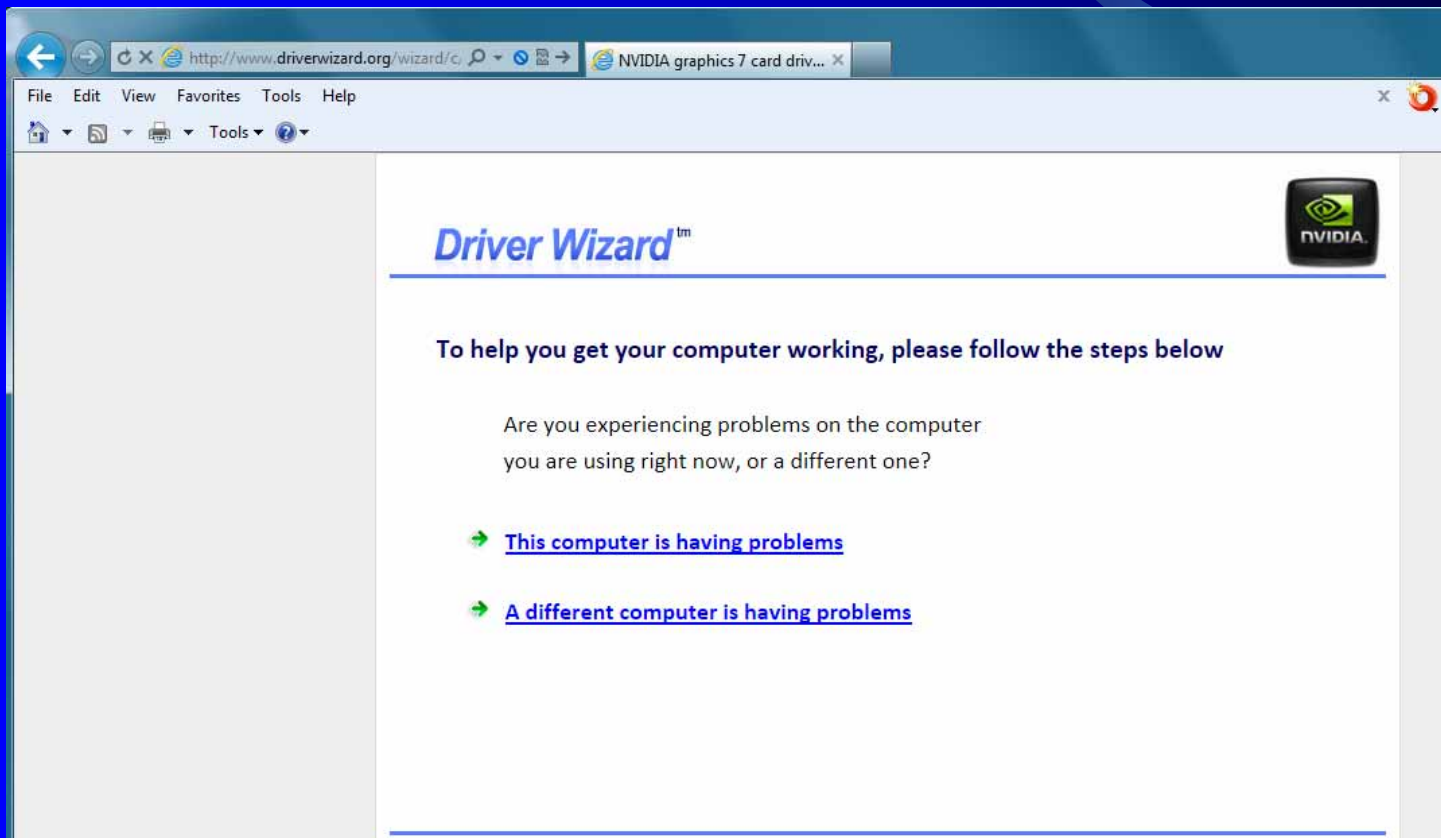
**[Display Optimization Wizard - NVIDIA Forums](#)** 

**NVIDIA** Forums: Display Optimization **Wizard** - **NVIDIA** Forums ... I've heard the settings are lost when new **drivers** are installed so this is ...  
[forums.nvidia.com/index.php?showtopic=36810](http://forums.nvidia.com/index.php?showtopic=36810)

**[NVIDIA: Display Adapters and System Chipsets](#)** 

**NVIDIA**: Display Adapters and System Chipsets. **NVIDIA** (California, USA) develops, manufactures, and markets graphics chipsets and video cards for PCs, laptops, gaming ...  
[driverwizard.org/articles/nvidia](http://driverwizard.org/articles/nvidia)

He got this window:



...still not notice the red circle.


Driver Wizard™

The software for your NVIDIA graphics 7 card needs to be updated before it will work properly

- Download the device auto-updater
- The updater utility will automatically locate and install the correct update.

Click on **Start Download** below and choose **Run** as shown in the image.

[Start Download](#)



Driver Wizard™

Download starting...

Installation will start automatically if you selected **Run**.

Note: If not then locate the Driver\_Wizard.exe installer (likely on your desktop) and double-click it to install using the default installation options.

Once the installation is complete, click on the **Scan** button inside the utility and follow the steps to finish updating your device.

Make sure your problem is solved!

Enter your first name and email address below and we'll follow up with you right away to ensure your NVIDIA graphics 7 card is working properly. We'll also occasionally send you recommendations on tools and downloads to make your computer life trouble-free. We will **not** be sharing your email information with a third party!

First name:

Email:

[Continue >](#)

Setup - Driver Wizard

**Welcome to the Driver Wizard Setup Wizard**

This will install Driver Wizard on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



[Next >](#) [Cancel](#)

Setup - Driver Wizard

**License Agreement**

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

bugs. The PUBLISHER gives no other express or implicit warranty under the LICENCE.

**PARTIAL NON VALIDITY**  
If any one of the clauses or provisions in the LICENCE is ruled null and void or not written, the remaining provisions shall nonetheless remain valid.

**APPLICABLE LAW**  
The LICENCE is subject to French law, excluding rules on the conflict of laws.

? Avanquest Software and its licensors all rights reserved

I accept the agreement

I do not accept the agreement

[< Back](#) [Next >](#) [Cancel](#)

At this point, he decides to check...

He goes to Google and types:

“Is driver wizard a safe program?”

## Is driver wizard a safe program?

About 652,000 results (0.34 seconds)

▶ [driver wizard Complaints - cancellation](#)   

[www.complaintsboard.com/complaints/driver-wizard-c311357.html](http://www.complaintsboard.com/complaints/driver-wizard-c311357.html) - Cached

Feb 16, 2010 – Some one should do something about Driver Wizard and Safe-cart ripping people off! ... All of that for purchasing the Driver Wizard program. ...

[driver wizard free download](#)   

[en.softonic.com/s/driver-wizard](http://en.softonic.com/s/driver-wizard) - Cached

May 5, 2011 – Free download **driver wizard** - DriverMax 5.91: Export and reinstall your PC drivers easily, and much more ... Free software. Safe downloads. Search Softonic. Search: ... **driver wizard** Search Results (10 programs) ...

[Driver Wizard - User' REVIEW, Scam or Safe?](#)   

[www.registrycleanercompare.com/driver-wizard/](http://www.registrycleanercompare.com/driver-wizard/) - Cached

Driver Wizard Review Here. And **Driver Wizard is not recommended for you.** ... probably the most strong Driver Up-date Software program I actually examined. ...

[Safe Software - Wikipedia, the free encyclopedia](#)   

[en.wikipedia.org/wiki/Safe\\_Software](http://en.wikipedia.org/wiki/Safe_Software) - Cached

Safe Software Inc. provides software and consulting services focused on managing the exchange of both spatial (geographic) and non-spatial data between GIS ...

## 4. Be smart with passwords...

*Repeat after me:*

Never use the same password in multiple places, and be especially vigilant with passwords for e-mail accounts.

“Why...you might ask?”

In the past 3 months, Facebook, Sony, Gawker, Plentyoffish, etc. etc.. were hacked and the Usernames and Passwords were published.

That would be a total of 3,500,000 Usernames and Passwords that were compromised.

I know you would not do this:

But just for fun, suppose that your Username and Password were the same for:

- Google
- Bellsouth
- Schwab
- Wells Fargo
- Need I say more??

# Krebs on Security

In-depth security news and investigation



This man is a real techie and I subscribe to his news letter. His philosophy can be summed up as:

*Krebs's 3 Basic Rules for Online Safety*

1. *“If you didn’t go looking for it, don’t install it!”*
2. *“If you installed it, update it.”*
3. *“If you no longer need it, remove it.”*

# What I believe to be mandatory products for your computer security.

- A good Antivirus program.
- A good spyware/malware blocking program.

# Antivirus Programs

***These are good and free.***

AVG

[www.free.grisoft.com](http://www.free.grisoft.com)

MICROSOFT SECURITY ESSENTIALS

[www.microsoft.com/security\\_essentials/](http://www.microsoft.com/security_essentials/)

AVAST

[www.avast.com](http://www.avast.com)

## My personal choice is Microsoft Security Essentials.

- It is free.
- It is very highly rated among antiviruses.
- It automatically updates.
- There is no “Pro” version to upgrade to for \$\$\$.

# Spyware/Malware Programs

***These are good and free.***

AD-AWARE

[www.lavasoft.com/products/ad\\_aware\\_free.php](http://www.lavasoft.com/products/ad_aware_free.php)

MALWAREBYTES

[www.malwarebytes.org](http://www.malwarebytes.org)

SPYBOT

[www.safer-networking.org/en/download/](http://www.safer-networking.org/en/download/)

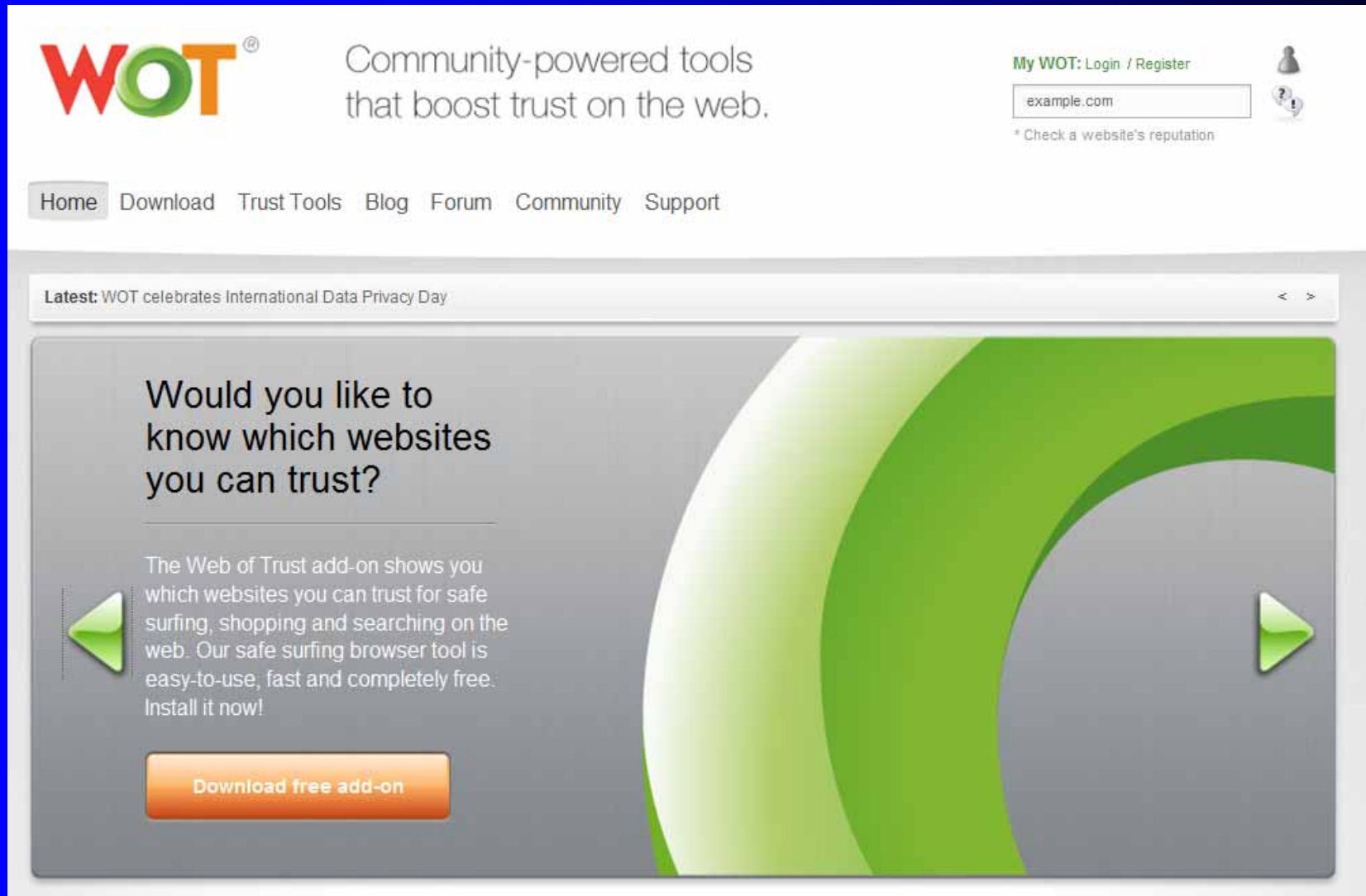
## My personal choice is Malwarebytes.

- It is ~~free~~. I paid \$25 for a lifetime purchase.
- It is very highly rated among malware programs.
- It automatically updates.

\*\* All of the free malware programs, including Malwarebytes, are essentially ‘after the fact’. If you get malware, you must run the program to remove the problem.

The \$25 version runs all the time and stops the installation of malware programs. It is pro-active.

# Another [free] great tool!



The screenshot shows the WOT website homepage. At the top left is the WOT logo, followed by the tagline "Community-powered tools that boost trust on the web." To the right, there is a "My WOT: Login / Register" link, a search input field containing "example.com", and a small help icon. Below the header is a navigation menu with links for Home, Download, Trust Tools, Blog, Forum, Community, and Support. A "Latest" news section features a slide titled "WOT celebrates International Data Privacy Day". The main content area contains a promotional message: "Would you like to know which websites you can trust?" followed by a description of the Web of Trust add-on and a "Download free add-on" button.

**WOT**<sup>®</sup> Community-powered tools that boost trust on the web.

My WOT: Login / Register  
example.com  
\* Check a website's reputation

Home Download Trust Tools Blog Forum Community Support

Latest: WOT celebrates International Data Privacy Day

Would you like to know which websites you can trust?

The Web of Trust add-on shows you which websites you can trust for safe surfing, shopping and searching on the web. Our safe surfing browser tool is easy-to-use, fast and completely free. Install it now!

Download free add-on

[www.mywot.com/en/download](http://www.mywot.com/en/download)

Free Music Downloads - Download Free MP3 Music - Best Limewire Alternative! - Windows Internet Explorer

http://www.bearshare.com/ free music downloads

WOT Warning: This site has a poor reputation.

# WARNING!

This site has a poor reputation.  
bearshare.com

[View rating details and comments](#)

	<b>Trustworthiness</b>	Poor
	<b>Vendor reliability</b>	Poor
	<b>Privacy</b>	Poor
	<b>Child safety</b>	Very poor

[This site is safe - I want to rate it](#) [Ignore warning and go to the site](#)

**WOT**  
WEB OF TRUST

Malwarebytes' Anti-Malware  
Successfully blocked access to a potentially malicious website: 207.232.22.52  
Type: outgoing  
Port: 51186  
Process: iexplore.exe

Done Internet

*This is not rocket science  
...it is called being alert.*

The weakest point in your computer system is  
usually located in front of the monitor!

*Hey!*

*Let's be careful out there...*

?

Questions

?

*Greensboro Computer Center for Seniors*



[www.greensboroshepnet.org](http://www.greensboroshepnet.org)