



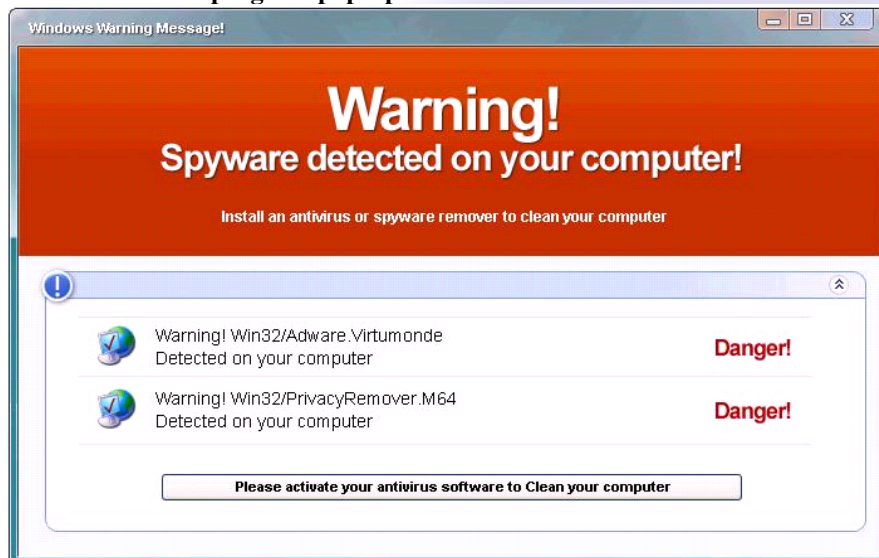
## Malware Prevention Guide 6-22-2010

The frequency and severity of malicious software infections has increased dramatically during the past few months. In addition, the clean-up process of an infected system has become more time consuming and in certain cases almost impossible (short of a full wipe and re-build) depending on the infection.

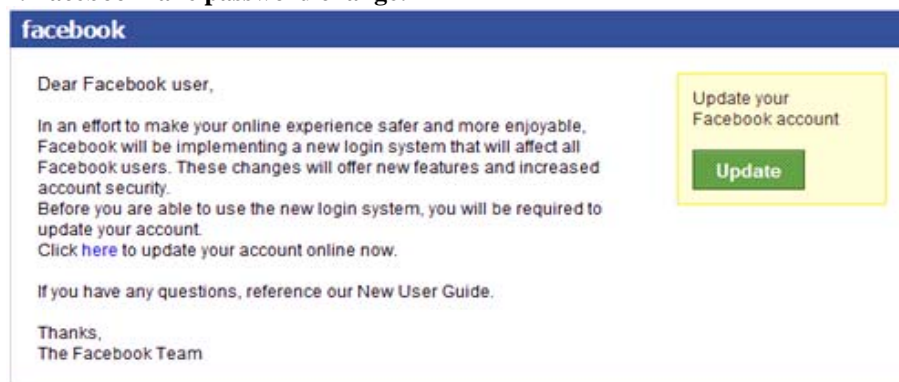
Types of Infections include those that take advantage of PCs that are not fully updated (patched) with critical security updates or with expired, or not up to date antivirus programs. E-mails that ask you to change login and password information for popular services such as Twitter, Facebook, PayPal, E-Bay, etc. Forged e-mail messages that make them look like someone you know sent you a message for a meeting or a chain-letter or joke. Those may contain links that if you click them will infect your PC. Pop-ups from fake antivirus advertisements that tell you your PC is infected. Here are some examples and please *do expect variations*. All these messages fall under the term “**phishing**” (i.e. fishing for your information)

The following are some common ways of infection. The second Section contains guidelines to mitigate these issues.

### 1. Fake Antivirus program pop-ups



### 2. Facebook fake password change:



### 3. Fake banking password change:

Subject: Verify your E-mail with Citibank

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:

[https://web.da-us.citibank.com/signin/citifi/scripts/email\\_verify.jsp](https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp)

### 4. Paypal fake account change request

#### Please Update Your Account

Dear valued **PayPal** member:

It has come to our attention that your **PayPal** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online services.

However, failure to update your records will result in account suspension. Please update your records on or before **Jan 30, 2008**.

Once you have updated your account records, your **PayPal** session will not be interrupted and will continue as normal.

To update your **PayPal** records click on the following link:  
<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>



## 5. Fake UPS e-mail (similar messages apply for other postal services)



## 6. Fake meeting confirmation requests

Hello,

Please don't forget about our conference meeting on Friday. And remember to RSVP for the Meetup group.

**Make sure to review our schedule for the entire day here:**

<http://www.conference-schedules.391325.com/planning/meeting/>

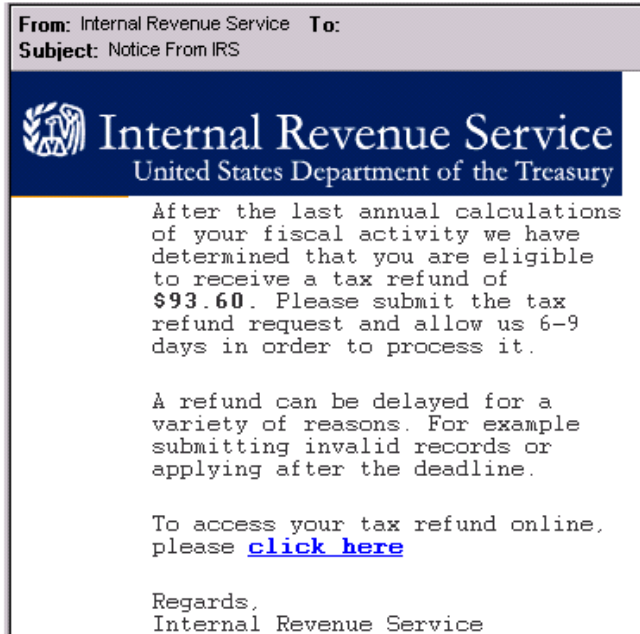
I'll provide you with a complete spending report before Thursday.

Thank you,

## 7. Fake News Bulletins or Fake News E-mails when real major real events occur (such as Haiti, World Cup, etc. ). Also fake donation messages for big disaster and other events.



## 8. Fake government and other official e-mail messages.



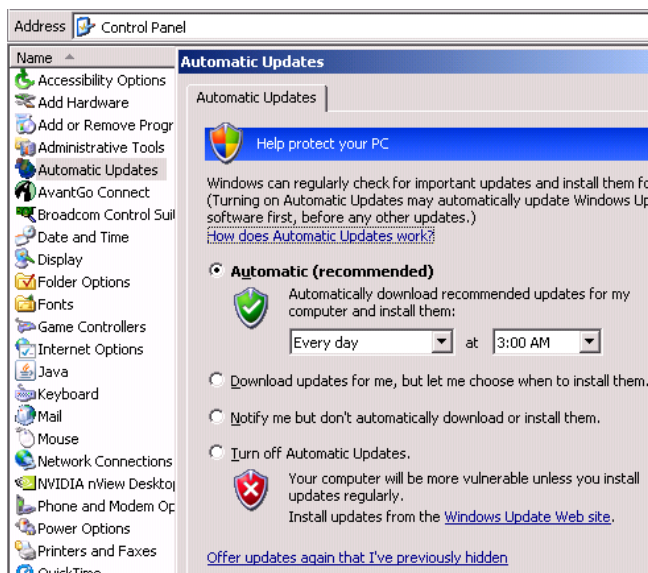
## 9. Other fake messages

There are many other fake e-mails, such as: Fake Microsoft e-mails prompting you to install a security update. Fake notifications that your e-mail settings have changed and you need to click a link to update them. Fake notifications that there are some updates that will be installed as part of a maintenance schedule and you need to click on a link to apply them.

### Steps to take to prevent infection:

#### Windows Updates:

Keep Windows up to date by going to **Start>Control Panel> Automatic Updates** and selecting to automatically receive and install updates on your PC. **If you set for evening updates be sure to leave the PC on.**



### Browser updates and Search Engines:

Keep the internet browsers that you use (Internet Explorer, Firefox, Opera, Google Chrome, Safari) up to date. If an update notification is received, get it directly from the **maker of that program** and not from any other third-party source to ensure that the program you are installing has not been tampered with. For example, Internet Explorer can be downloaded from <http://www.microsoft.com/ie>

Be very leery of search results displayed on the very top as **sponsored links** or any ads on the right or left side of the search results. Reading the preview text can be helpful in determining if a link is just an ad or if it looks like a valid result. If you misspell a website or a search item and a search engine opens do not use it. Completely close your browser window and re-open it and type the address again. May incorrectly spelled websites are bought by unscrupulous individuals and they masquerade as search engines.

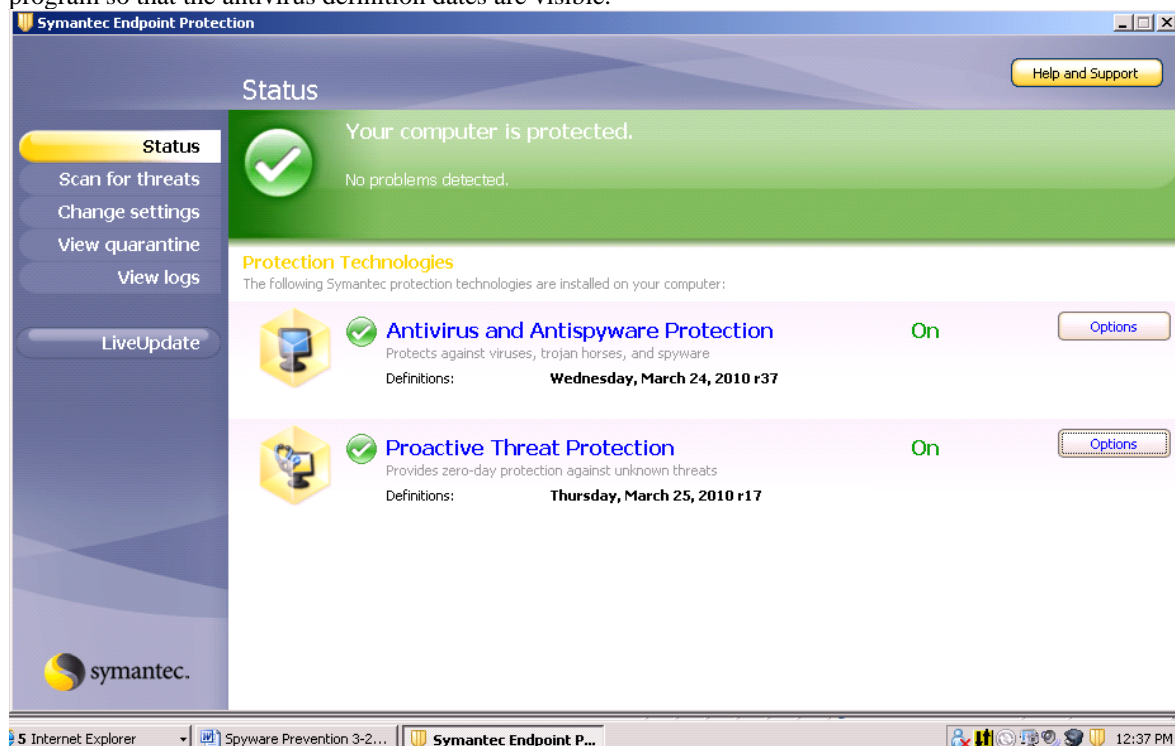
Do not save any passwords for banking or other websites. It is strongly suggested that you open a new browser window to do your banking, and close it after you are done. Also, clear you cookies and browsing history after you are done with your session. Newer browsers also come with **Private mode** that does not store any cookies or settings for the current session you are in and can be very useful.

### Antivirus updates:

Know the name of the antivirus program that is installed on your PC (eg: Norton Antivirus, Norton Internet Security, McAfee, Kaspersky, ESET, Microsoft Security Essentials) and what the tray icon and notifications look like, so you do not fall for those fake antivirus notification pop-ups.

Make sure your antivirus program is up to date with an updated subscription and up to date antivirus definitions. Also make sure that no component of it is disabled.

Periodically double click on the antivirus icon that is on the system tray and verify that the antivirus program is up to date. In this example the Antivirus program is Symantec Endpoint Protection. Note the yellow shield with no warning signs on the tray icon itself. Double clicking on the shield brings up the program so that the antivirus definition dates are visible.

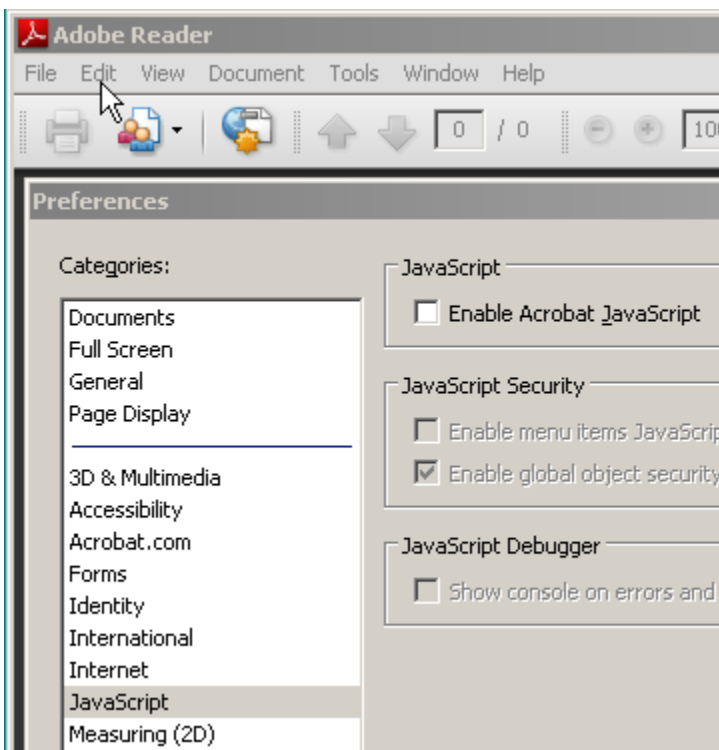


**Popular software such as Adobe Reader and Flash which are targets of attacks:**

There has been an increase in the amount of security flaws that have been discovered in popular business software such as Adobe Acrobat Reader (used to open **PDF** Files) and Adobe Flash (used for delivering online video content and for animations in websites and web advertisements). We strongly recommend keeping those programs up to date by going to [www.adobe.com](http://www.adobe.com) and clicking on the links shown below.



Once you install Adobe Acrobat Reader, run it, and click on **Edit>Preferences**. **Uncheck** the Enable Acrobat JavaScript as show below and click **OK**. This will dramatically reduce any security vulnerabilities that have been exploited with malformed PDF files.



If another website you are visiting states that you are using an old version of Adobe Flash or Adobe Reader do not try to update it from the website you are visiting. Just go to [www.adobe.com](http://www.adobe.com) and update it from there to ensure the installation program is legitimate and not a virus.

**Java updates:**

More recently, there have been fake Java updates. Java is a programming language used in many websites. If a website requests a java update please do not perform it from that website. Instead, go to [www.java.com](http://www.java.com) and get the update from there to ensure the installation program is legitimate.



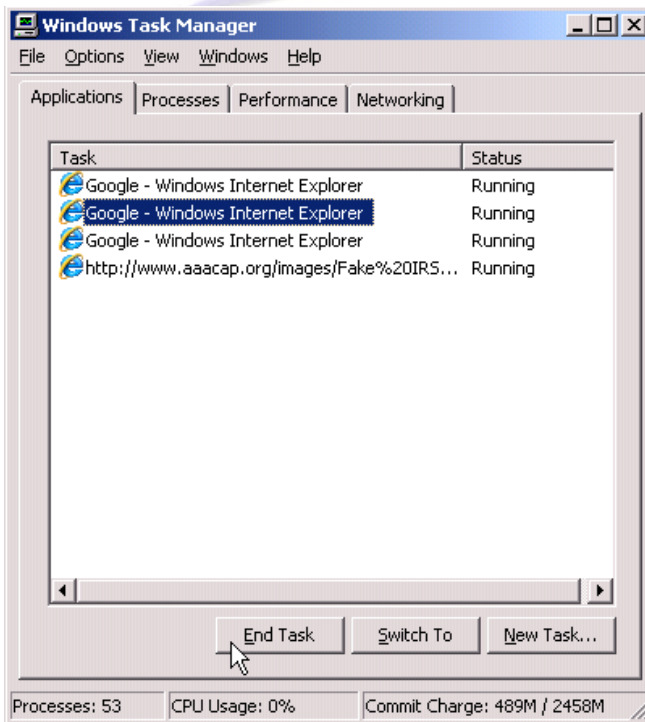
### E-mail Handling:

Always treat e-mail messages you were not expecting with a healthy dose of suspicion even if the sender appears to be someone you know. Their e-mail address may have been forged. If you communicate often with trusted sources, you start to get a feel for how they write, what their e-mail signatures on the bottom look like and you can use these clues as comparison when you see an unexpected message.

**All the fake e-mail messages you get, should be deleted without clicking on any of the links they contain.**

Twitter, E-bay, MySpace, PayPal or your bank, normally never send you a message asking you to change your password or enter a credit card number for verification. If you see any of those messages, just delete them and do not click on any of the links.

Even websites that are considered reputable may contain pop-up ads for fake antispyware and antivirus programs as was previously shown. If you see one of those pop-ups, do not panic. **Do NOT** try to click on **Cancel** or on the **X** button to close it. It is better to press the keys **CTRL+ALT+DEL** on your keyboard, select **Task Manager** select **End Task** out of all the browser sessions you have open as shown below. That way you do not have to worry about clicking anywhere on the pop-up because you cannot really trust that say, the cancel button will cancel the install.



### Social Networks and Messenger software:

If you have to use Facebook, or MySpace, avoid installing any MySpace messengers or any other add-ins that come with the software. Try to limit joining too many wacky Facebook groups or installing additional Facebook applications such as games and gift giving applications. They pose a privacy and security risk. Review your privacy settings and tighten them up to where, say, only friends can view your posts, pictures etc. The default settings allow full view from everyone. That may be beneficial for ad-targeted campaigns that Facebook relies on to get their money, but it is detrimental to your privacy.



If you have to use messaging software such as MSN messenger, AOL instant Messenger or Yahoo Messenger, please keep them up to date, by going to the respective vendor pages and getting the updates and do not accept any incoming files transmitted via messenger since they pose a security risk as well.

If your business uses online meeting software such as GoToMeeting or Cisco Meeting Place, GroupSite, Microsoft LiveMeeting know what it is and what invitation requests look like so that you can tell whether e-mail messages with meeting requests are legitimate or fake. When in doubt create a **new e-mail message** asking the sender if they did sent a meeting request to you or a quick call will allow you to verify identity. In any event, a couple of minutes spent verifying messages can prevent hours of clean-up of infected PCs and downtime.

**Program installation procedures:**

When you install programs select the custom installation. This in many cases allows you more control of what gets installed in your PC. Many times some legitimate utilities install additional toolbars such as msn, google, etc. Those slow down your browser. By selecting **Custom installation** (also called Expert or Advanced installation) that allows you to uncheck any additional toolbars that would have been installed had you chosen the Typical or Quick setup.

**General and password Guidelines:**

Never provide access to any computers or server rooms or any sensitive facilities without first verifying identity and intent.

Never give out passwords to anyone you are not certain of over the phone.

Do not share network passwords with co-workers and if you have to write them down, please keep them in a safe place. (Hint: Below the keyboard is not a safe place.) If you have to write them down, try and not write down the whole phrase. Try a partial or three or four initial letters. That way it may help you get jumpstarted on remembering the password, but if it falls into the wrong hands it will make it harder to guess. This of course assumes that you are using strong passwords. Strong passwords are at least 10 characters long, contain numbers and letters and symbols. Do not use your name, birthday, driver's license, passport number, or similar information.

Ultimately, manipulating people so that they can divulge information (what is termed as “social engineering” ) is nothing new and will always occur with ever increasing sophistication. We hope that the information and recommended practices provided will aid you in identifying these attempts and in having a safer experience on-line.

Please be sure to check periodically for updates to this guide.

