i.t.solutions
uahuntsville

PREVENTING FAKE ANTIVIRUS INFECTIONS

AUDIENCE

This document is for UAHuntsville faculty, staff, and students.

FAKE ANTI-VIRUS ALERTS

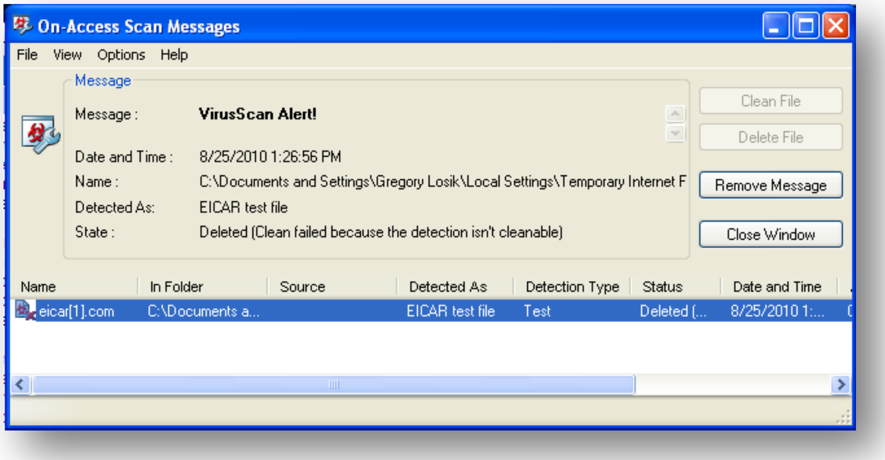
Displaying fake virus warnings in order to get users to click a button is one of today's most prevalent virus threats. The warning tricks the user into clicking a pop up message that will supposedly clean a virus that is already on the user's computer. Clicking on these alerts actually causes a real virus to install.

It is important to **never** click anything on these messages. Even clicking the red **"X"** button, in the upper right corner of the windows could cause a virus to install. Some of these rogue pieces of software might prompt for payment to remove the "infection." The FBI estimates that users have been scammed of over $150 million by paying for these fake anti-virus scams.

KNOW YOUR OWN LEGITIMATE ANTIVIRUS SOFTWARE

Legitimate anti-virus alerts will be displayed by an installed anti-virus software. Before clicking on anything, read what it says in the pop-up title bar. If the title and icon match a program that you know and have already installed then it is more likely to be safe.

Get familiar with the virus alert for your system's virus software. UAHuntsville provides McAfee VirusScan for free to computers accessing the network—contact TAG for a free download. If you have McAfee installed, you can expect a message that looks similar to this.



Message : VirusScan Alert!

Date and Time : 8/25/2010 1:26:56 PM
Name : C:\Documents and Settings\Gregory Losik\Local Settings\Temporary Internet F
Detected As: EICAR test file
State : Deleted (Clean failed because the detection isn't cleanable)

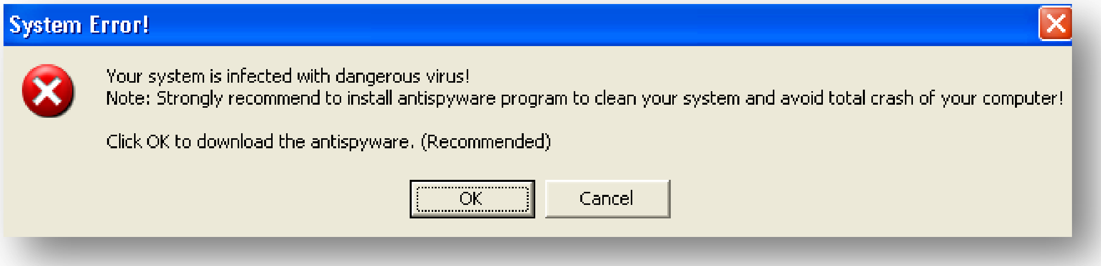
Name	In Folder	Source	Detected As	Detection Type	Status	Date and Time
eicar[1].com	C:\Documents a...		EICAR test file	Test	Deleted (...	8/25/2010 1:...

Use the following steps if you are using an antivirus package other than McAfee, or want to get a better idea of what the warning looks like on your computer so you won't be fooled by the fakes.

1. Go to http://www.eicar.org/anti_virus_test_file.htm.
2. In the **Download area using the standard protocol http,** click on the eicar.com link. A download of a harmless file used for testing antivirus will begin.
3. Your virus scanning software should display a legitimate antivirus warning, indicating that your antivirus software is working.
4. If you also receive a download Security Warning before downloading, click Cancel.

KNOW HOW TO IDENTIFY FAKE ANTIVIRUS SOFTWARE

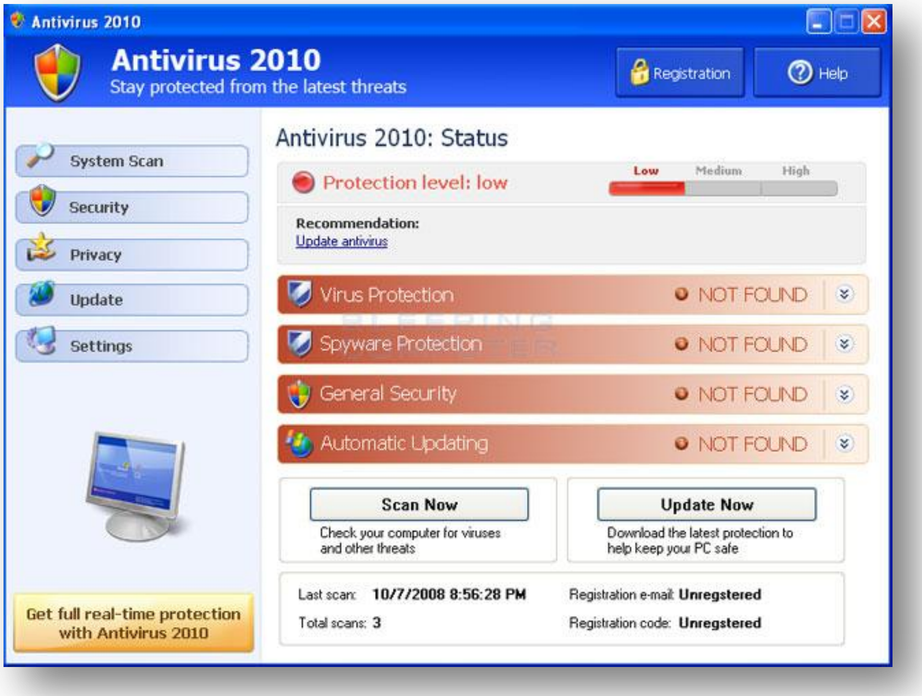
The following images represent some of the common fake anti-virus rouge software alerts.



System Error!

Your system is infected with dangerous virus!
Note: Strongly recommend to install antispyware program to clean your system and avoid total crash of your computer!

Click OK to download the antispyware. (Recommended)



Antivirus 2010

Antivirus 2010
Stay protected from the latest threats

Antivirus 2010: Status

Protection level: low

Recommendation:
Update antivirus

Virus Protection — NOT FOUND
Spyware Protection — NOT FOUND
General Security — NOT FOUND
Automatic Updating — NOT FOUND

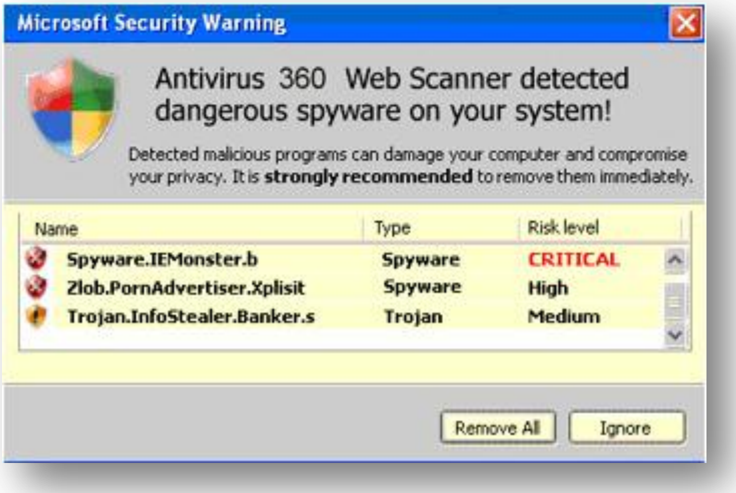
Scan Now — Check your computer for viruses and other threats

Update Now — Download the latest protection to help keep your PC safe

Last scan: 10/7/2008 8:56:28 PM
Total scans: 3

Registration e-mail: Unregstered
Registration code: Unregstered

Get full real-time protection with Antivirus 2010



Microsoft Security Warning

Antivirus 360 Web Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

KNOW YOUR RISKS

Fake antivirus software can be very dangerous. Here are some of the things the fake antivirus software can do.

- Steal your identity
- Send spam messages from your e-mail address
- Corrupt or destroy your documents
- Allow other, stronger infections into your computer
- Crash your computer
- Slow your computer to a crawl
- Wreak havoc on the network, causing larger computer issues
- Infect other computers
- Create a fake Windows "blue screen of death"

PROTECTING YOURSELF

Take the following precautions to protect yourself.

- Always install an Anti-Virus software package.
- Check that your Anti-Virus software is updating daily.
- Use Mozilla Firefox with the extensions No-Script, Ad-Block and WOT (Web of Trust) installed or Google Chrome which has a sandbox feature, for general off campus Internet browsing. Only use Microsoft Internet Explorer for campus authenticated applications. Upgrade Internet Explorer to version 8.0 for better phishing protection.
- Avoid questionable websites.
- Avoid using file sharing programs to download games, music, movies, TV shows, etc. A large majority of the files shared on this network are infected.
- Don’t click advertisements on the Internet.
- Don’t give anyone your password

- Don’t open or respond to SPAM.
- Read all warnings very carefully.
- Never click OK or cancel to warnings like this.

STEPS TO PERFORM IF YOU GET A POP-UP

Use the following steps to prevent a fake Anti-virus infection.

Note: If you are uncomfortable in performing the tasks below, contact the TAG Help Desk at 824-3333 for assistance.

- Do not click anywhere inside the Fake Alert window.
- Press Ctrl-Alt-Delete (i.e., all three keys at once)
- A window will pop up. Select Task Manager.
- The Task Manager will display. Make sure the Applications tab is selected.
- Look for Internet Explorer (or whatever web browser you are using).
- Click on it.
- Click End Task.
- Select each additional instance of your web browser and click on End Task until they have all been ended.
- Close the Task Manager.
- Save any applications you may have open.
- Reboot your computer and see if the pop-up disappears.
- Perform a full anti-virus scan of your system.
- Contact the TAG helpdesk at ext 3333 for any other assistance.