What to do if your PC is infected by malware

Even the best anti-malware software can't give complete protection, so here's what to do if something slips past its defences.

New security holes are discovered in Windows and web browsers all the time, and it's possible for hackers to exploit them before anyone can issue a fix.

New malware can also slip under the radar of anti-malware software and while malware database updates are usually quick to arrive, there's often a **small window of opportunity** when internet nasties can sneak in undetected.

So how can you tell when your PC is infected by malware and, more importantly, what can you do about it?

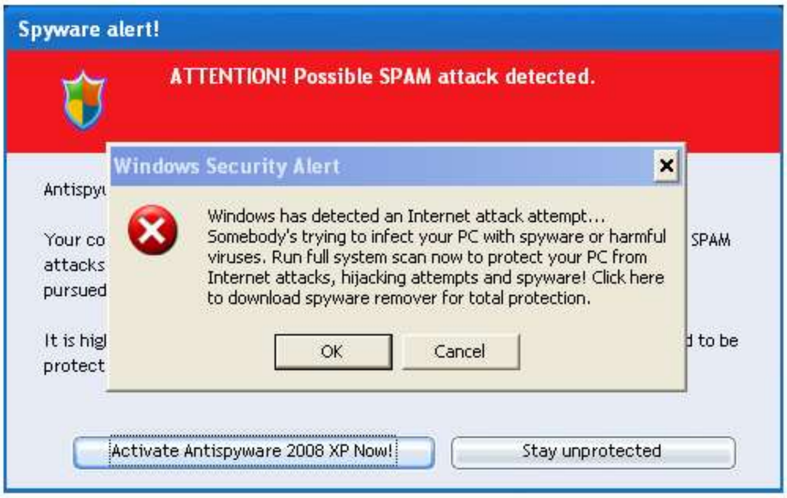
Know your anti-malware software

If you're lucky, you'll have plenty of warning when your PC picks up a malware infection — your anti-malware software will display an alert.

Just make sure you're familiar with the look and feel of your malware software. Some sneaky malware can display very convincing fake 'alerts' that try to fool you into installing yet more dangerous software in the guise of getting rid of it.

Watch your web browser

Malware can also hijack your web browser. If you find your homepage (the page that opens when you open a new browser tab) has changed, pop-up windows containing ads keep appearing or web pages that look like anti-malware appliations open by themselves, malware is almost certainly the culprit.



Spyware alert!

ATTENTION! Possible SPAM attack detected.

Antispyu

Your co
attacks
pursued

SPAM

It is hig
protect

d to be

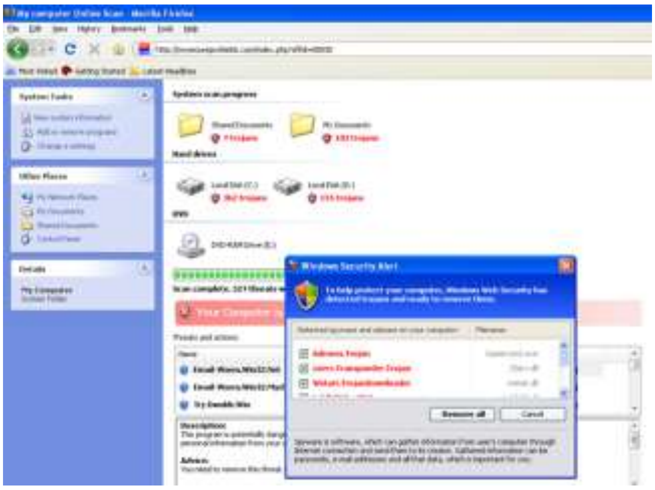
Windows Security Alert

Windows has detected an Internet attack attempt... Somebody's trying to infect your PC with spyware or harmful viruses. Run full system scan now to protect your PC from Internet attacks, hijacking attempts and spyware! Click here to download spyware remover for total protection.

Look for other signs of infection

The worst case scenario is that are no visual clues to a malware infection. But if your PC suddenly starts to run far slower than usual, or crashes for no apparent reason, there may be cause to worry.

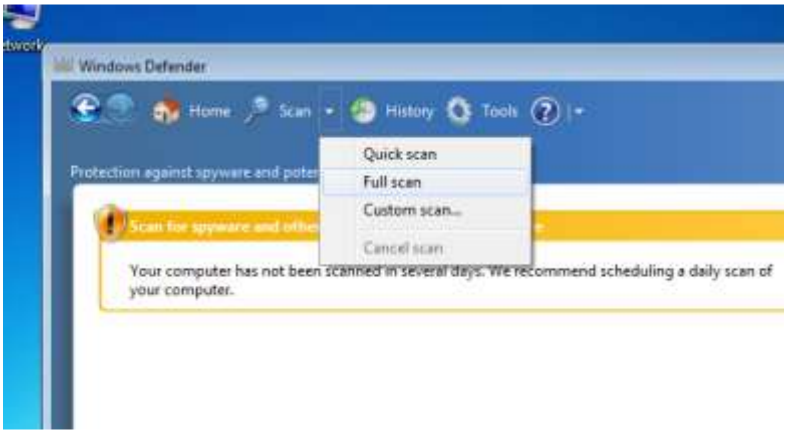
Ignoring these kinds of subtle warning signs is how ‘botnets’ get so big. These vast collections of malware-infected computers are controlled remotely by hackers and used for cyber attacks — all without their owners’ knowledge.



What to do if you’re infected

Step 1: Run a malware scan

The first thing you should do when you suspect your PC might have a malware infection is launch your anti-malware application and update its malware database. If you are BT customer this may be NetProtect.



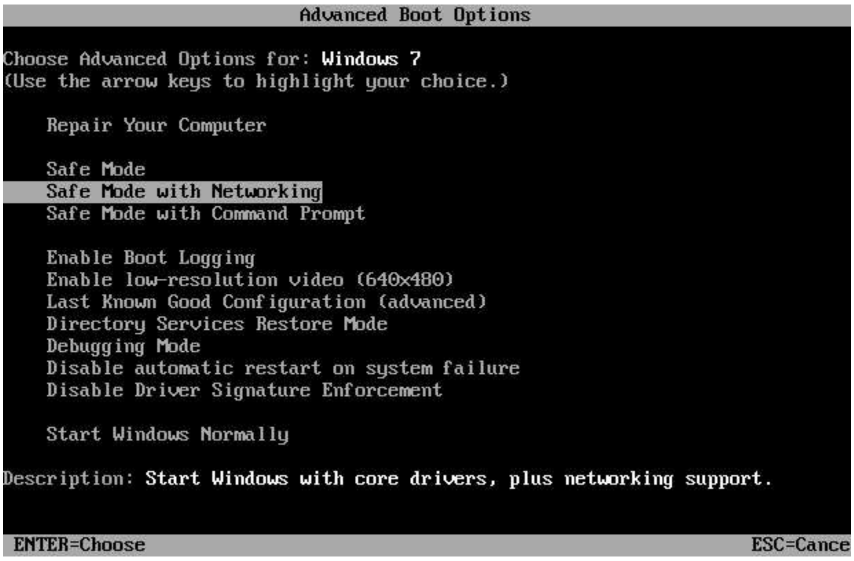
Your computer has not been scanned in several days. We recommend scheduling a daily scan of your computer.

Then perform a full system scan — you may have to select this option manually, since some software defaults to a less thorough ‘quick’ scan.

Since malware has already slipped past your anti-malware software, this step may not be much use, but it’s worth a try.

Step 2: Restart Windows in Safe Mode

If a malware scan finds nothing, or if malware stops you from using them (it can be very devious), restart Windows from the Start menu. As soon as the screen goes black as Windows restarts, press the **F8** key on the keyboard repeatedly until you see a black**‘Advanced boot options’** screen — you may need to try this a few times to



```
                         Advanced Boot Options

Choose Advanced Options for: Windows 7
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Start Windows with core drivers, plus networking support.

 ENTER=Choose                                                   ESC=Cance
```

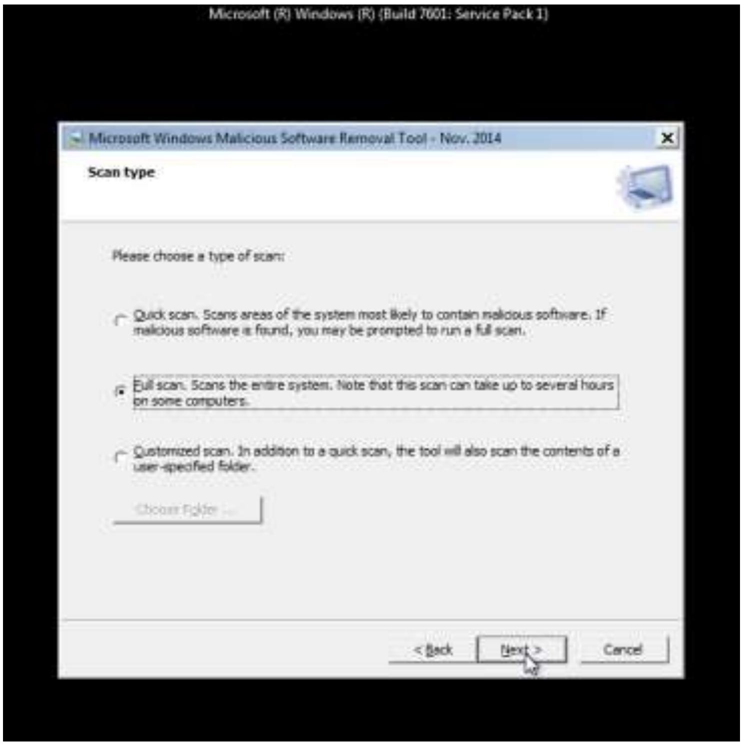
activate it before Windows loads normally. Use the keyboard arrow keys to select the **'Safe mode with networking'** option and press **Return**.
If malware prevents you from restarting Windows, just switch your PC off and an again, then try activating Safe Mode.

Safe Mode is a stripped-down version of Windows that disables many of its advanced features, so don't be surprised if it looks very different to how Windows normally looks. Safe Mode also disables many of the programs that start automatically with Windows — which may include malware. And that's just what we want.

Step 3: Run the Microsoft Malicious Software Removal tool

If your own anti-malware software doesn't detect anything, use Microsoft's free Malicious Software Removal Tool, which is available to download **here.** Disconnect your PC from the internet when the download is complete, but before you run the tool — this can disable some malware features, making it easier to detect and remove. Just unplug your PC's network cable or switch of its Wi-fi to do this.

When the Malicious Software Removal Tool runs, select the **'Full scan'** option when prompted and wait until it completes.


Microsoft (R) Windows (R) (Build 7601: Service Pack 1)

Microsoft Windows Malicious Software Removal Tool - Nov. 2014

Scan type

Please choose a type of scan:

○ Quick scan. Scans areas of the system most likely to contain malicious software. If malicious software is found, you may be prompted to run a full scan.

● Full scan. Scans the entire system. Note that this scan can take up to several hours on some computers.

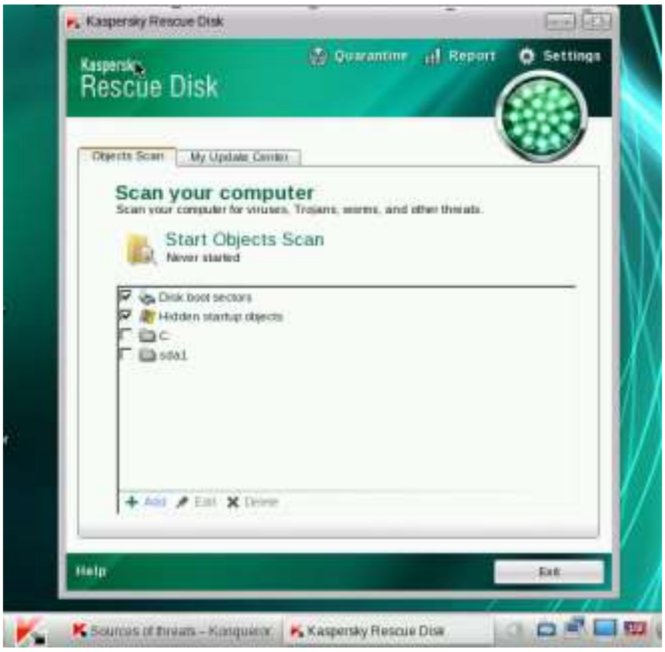
○ Customized scan. In addition to a quick scan, the tool will also scan the contents of a user-specified folder.

Step 4: Boot from an anti-malware rescue CD

If you get this far without any success, the next step is to boot your PC using a dedicated anti-malware CD. This bypasses Windows completely— and any malware with it — which makes it much easier to detect and clean an infection.

The only catch is that you'll need to download and create the CD using another, uninfected, PC. Doing it on your own PC risks creating an infected CD, which won't get you very far.

Ask someone you know to download the Kaspersky Rescue Disk 10



Scan your computer

Scan your computer for viruses, Trojans, worms, and other threats.

Start Objects Scan

Never started

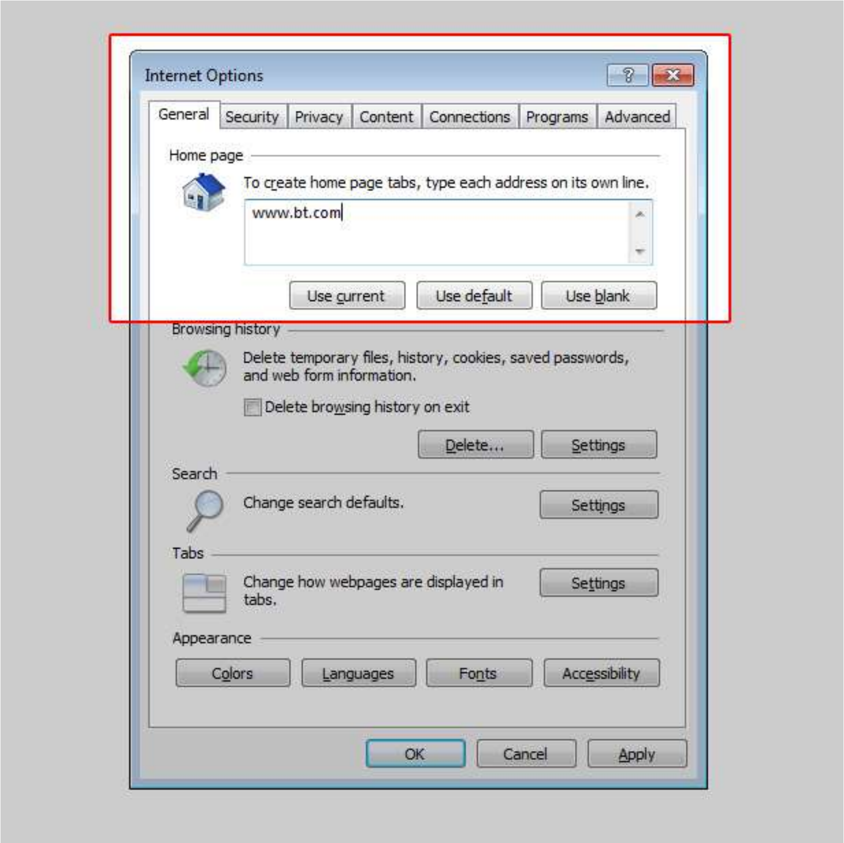
☑ Disk boot sectors
☑ Hidden startup objects
□ C:
□ sda1

fromhttp://support.kaspersky.co.uk/viruses/rescuedisk#downloads and then burn it to a CD. Use the CD to boot your PC and follow the on-screen instructions to scan for — and hopefully remove — any malware.

Step 5: Perform some final checks

If you have successfully detected and removed a malware infection, your work is not yet done. You'll also need to check your web browser and restore any hijacked web pages — look in its **'Options'** to see what the current home page is set to. You should also consider upgrading your anti-malware software to something more effective.

Since malware can also intercept just about everything you do on your PC, you should also change the account passwords for your email and online services, particularly those for financial institutions. Keep an eye on your back accounts, too, just in case a hacker has gained access.



To create home page tabs, type each address on its own line.

www.bt.com

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Change search defaults.

Change how webpages are displayed in tabs.

]

Step 6: If all else fails…

If none of these steps successfully removes a malware infection, you've been unlucky enough to catch something that's all but incurable.

In this case, the only option is to the drastic step of reformatting your PC's hard drive and reinstalling Windows. You'll then need to restore your applications and files from your **most recent backup**, if you have one. Otherwise, you'll need to copy your files onto another drive and dig out your software install discs.

In either case, make sure you install and update some anti-malware software as soon as Windows is reinstalled — and before you install anything else.