

Here you will find the latest information and recommendations on how to protect yourself from the latest Internet risks.

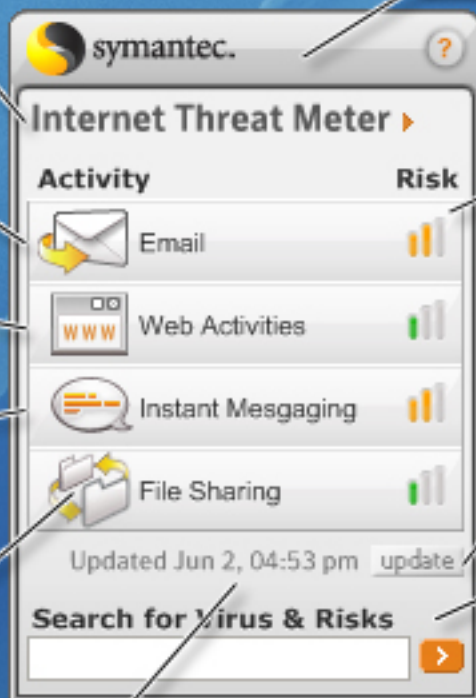
Right-click on the widget to adjust your preferences - such as how you want to be alerted when threat levels increase.

Sending and receiving Email is one of the most popular online activities - as well as the preferred method for spreading "malware" and many kinds of online fraud.

Web Activities include all the common tasks associated with using a Web browser, such as surfing the Internet.

Instant Messaging refers to the use of applications that enable live chat online.

File Sharing refers to the use of "peer-to-peer" applications to share audio and video files.



Risk levels represent the current risk associated with a given activity. Think of them as a kind of weather report that you can use to make informed decisions about how you work and play online.

Manually update the threat information from the Symantec website.

Search Symantec's website for the latest information on viruses and other online risks.

More Symantec Web resources.

Indicates when the Meter was last updated.

The screenshot shows the Symantec Internet Threat Meter interface. At the top, the Symantec logo and a help icon are visible. Below the title bar, the text "Internet Threat Meter" is displayed with a right-pointing arrow. The main area is divided into two columns: "Activity" and "Risk". Under "Activity", there are four categories: "Email" (with an envelope icon), "Web" (with a WWW icon), "Instant" (with a speech bubble icon), and "File" (with a folder icon). Each category has a corresponding risk level indicator. The "Email" category is highlighted in yellow, and a tooltip is displayed over it. The tooltip contains the text: "Medium Risk: Use Extra Caution" followed by a detailed warning: "A recent attack is reported to send a malicious Word document attachment via email. The Word document installs malware. The malicious email is disguised to appear as if it's from a trusted source. Don't open unexpected email that contains Word documents." At the bottom of the window, there is a "Search for" field and a "Updated J" label.

Email

Medium Risk: Use Extra Caution

A recent attack is reported to send a malicious Word document attachment via email. The Word document installs malware. The malicious email is disguised to appear as if it's from a trusted source. Don't open unexpected email that contains Word documents.