

Date: August 10, 2009  
To: All DHS employees  
From: Kyle Miller, DHS Information Security Officer  
Subject: Potentially malicious Web advertisements

The occurrence of virus attacks on DHS computers has been rising rapidly. The bad-guys are finding new tricky ways of delivering their nasty payloads on unsuspecting computer users. The Information Security Office's (ISO) forensics staff, working with the statewide Enterprise Security Office team, has isolated many of the recent attacks to "advertisements" embedded in websites. Most are passive; in that they include a picture and/or text that link to the advertiser's web site.

As a result, DHS has taken steps to warn you about these types of advertisements and block the potential execution of malicious code.

### What you will see

Depending on how a specific web page is designed, the warning may pop up in a separate browser window, or it take the place of the embedded ad. If it appears in place of the ad (or inline), it looks like the picture below. In many cases, the warning will appear cut off. If you see this warning, it is okay to continue browsing the page; the warning effectively disables the advertisement.

The screenshot shows a web browser interface with a navigation bar at the top containing "What's New? - Mobile Mail - Options" and search buttons for "Search Mail" and "Search the Web". Below the navigation bar, a red-bordered box highlights a security warning that has replaced a banner advertisement. The warning text reads: "ADVERTISEMENT WARNING! DHS monitoring. Any use of this site at DHS may be inappropriate for a valid reason. Questions about Web use go to the Information Security Office. SECURITY See DHS policy: Acceptable Use of Information Systems". Below the warning, a table displays technical details: "User/Machine: DEFAULT", "IP: 170.104.57.39", "Category: Banner/Web Ads", and "Blocked URL: http://ad.yieldmanager.com/st?\_PVID=AAAJbN&ad\_type=iframe&ad\_size=28&cb=1249677424105711&zip=&ycq=...&b\_redirect=http://us.ard.yahoo.com/...". To the left of the warning, a text block under "Entertainment" and "Sports" categories contains a link "Airspeed systems failed on US planes" with a mouse cursor over it, and several lines of text starting with "a dozen recent flights by U.S. ...".

Example of the security warning displayed in place of a potentially harmful banner ad.

What's New? - Mobile Mail - Options

Search Mail Search the Web

ADVERTISEMENT  
**WARNING! DHS monitoring.**

**Any use of this site at DHS may be inappropriate for a valid reason. Questions about Web use go to the Information Security Office.**

**SECURITY**

See DHS policy: Acceptable Use of Information Systems

<b>User/Machine:</b>	DEFAULT
<b>IP:</b>	170.104.57.39
<b>Category:</b>	Banner/Web Ads
<b>Blocked URL:</b>	http://ad.yieldmanager.com/st?_PVID=AAAJbN&ad_type=iframe&ad_size=28&cb=1249677424105711&zip=&ycq=...&b_redirect=http://us.ard.yahoo.com/...

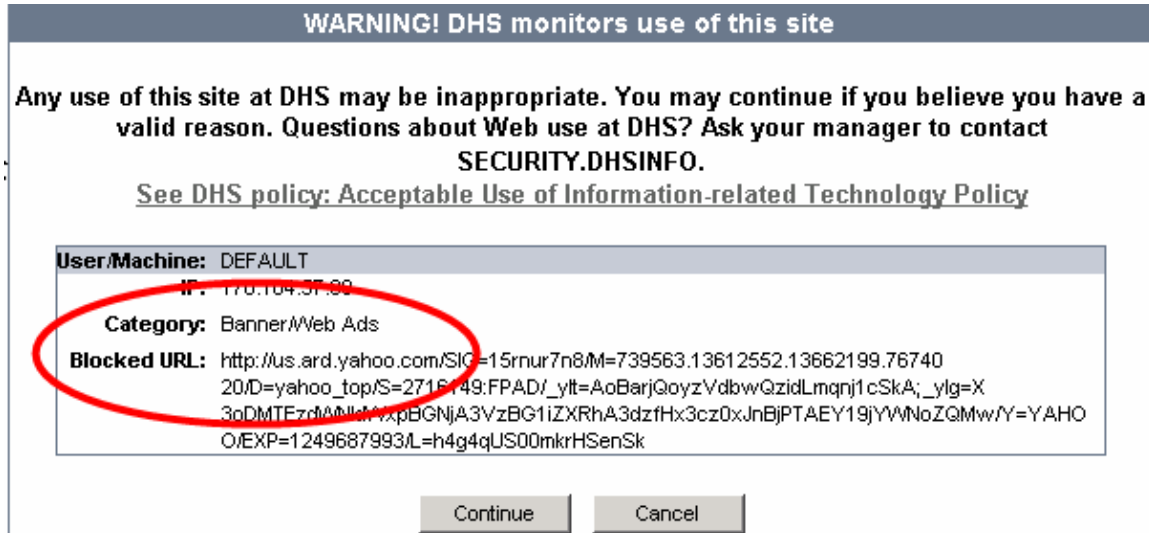
Entertainment Sports

[Airspeed systems failed on US planes](#)

a dozen recent flights by U.S. ...  
ctioning equipment made it impossible  
v how fast they were flying, federal  
e discovered. A similar breakdown is  
ir France crash into the Atlantic that

w to militants (AP)  
signing early (AP)  
out of state residence (AP)

If you get a pop up warning in a separate window, it provides clues to help you determine the risk. Note the example below. The **Category** item clearly indicates that the link is an advertisement and it shows the address (URL) of the blocked page. If the **Blocked URL** does not match the site you are browsing, it could be malicious.



### Practice safe browsing

We cannot identify every situation where a warning may appear, nor can we determine what a legitimate business use is for you. You are not prevented from viewing the contents of the page and may continue by clicking the Continue button.

*Please exercise caution when clicking on advertisements and other embedded content not related to the web site you are visiting.*