

# Fake browser warnings dupe users into downloading 'scareware'

**Scammers are spoofing the anti-malware warnings of popular browsers to dupe Windows users into downloading fake security software, according to Symantec.**

**By Gregg Keizer**

October 05, 2010 — [Computerworld](#) — Scammers are spoofing the anti-malware warnings of popular browsers to dupe Windows users into downloading fake security software, Symantec said Monday.

Several malicious Web sites are displaying phony versions of the alerts that Google's Chrome and Mozilla's Firefox present when users encounter pages suspected of hosting attack code, said Symantec researcher Parveen Vashishtha in a post to the [firm's blog](#) .

Rather than simply warn users that the page they're about to visit may be dangerous -- as do the legitimate alerts -- the sham versions also include a prominent message that suggests downloading a browser security update.

In reality, no browser offers its users security updates from its anti-malware warning screen.

Anyone who accepts the update actually downloads bogus software, often called "scareware" because it bombards users with endless fictitious infection warnings until people pay \$40 to \$50 to buy the useless program.

Even the cautious can be nailed by these sites. Users who refuse the mock updates are assaulted by a multi-exploit toolkit that includes attack code for 10 different vulnerabilities in Windows, Adobe Reader, Internet Explorer and Java. Windows PCs that have been kept up-to-date with bug patches will be immune from the exploit kit, however.

"Malware authors are employing innovative social engineering tricks to fool users -- it's as simple as that," said Vashishtha.

The strategy that Symantec pointed out isn't new. A month ago, [Microsoft](#) 's malware protection center warned that fake antivirus scammers were putting up bogus alerts in Internet Explorer, Firefox and Chrome.

"The similarity between the fake warning pages [and the real things] is so accurate that it can trick even highly trained eyes," Microsoft said in [early September](#) .

It's no surprise that scareware dealers are constantly looking for new ways to con users into downloading their good-for-nothing software: It's a serious business.

According to the FBI, rogue security makers have made [at least \\$150 million](#) by duping the public.

Little wonder, then, that the fake security software industry is huge. During the 12 months from July 1, 2008, to June 30, 2009, more than 250 different phony programs tried to get on more than 43 million machines worldwide, Symantec said in a report issued last October.

Gregg Keizer covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at [@gkeizer](#) or subscribe to [Gregg's RSS feed](#) . His e-mail address is [gkeizer@computerworld.com](mailto:gkeizer@computerworld.com) .