

united states

global sites

products

purchase

service &amp; support

security response

downloads

about symantec

search

feedback

## Don't Be Denied

Denial of service (DoS) attacks are becoming more widespread as many computer users are enjoying high speed, "always-on" connections to the Internet. During a denial of service attack, a huge number of server requests are sent to a server or router. When these requests are sent, the server or router replies to the computer that sent the original request. Hackers staging DoS attacks may send the request with a forged "reply to" address so that the reply cannot be delivered. By default, the server or router waits a specified length of time before trying to send out the reply again, but by this time another request has been sent with another forged "reply to" address. Soon the server or router is so overwhelmed with requests that it cannot reply to any.

When hackers organize DoS attacks, they may recruit outside forces to do their dirty work. They can use a program that will install the attack program on hundreds or thousands of machines via the Internet or a virus, like a Trojan horse. On command from the hacker, these computers attack the target site. The thousands of computers working together to take down another server can flood an individual site with gigabytes of requests. Proliferation of the DoS attack has been seen recently when such attacks took down sites like Yahoo! and Microsoft.

### Don't Lend a Hand to Hackers

You don't have to become part of a DoS attack launched on someone else. Here are a few steps to make sure your Mac doesn't unwittingly contribute to the undermining of another server.

- **Build a wall.** Your Mac is susceptible to attack any time you're connected to the Internet. A firewall protects your computer when it's online by monitoring traffic traveling to and from your computer and scanning for suspicious activity. Intrusion detection software constantly monitors your Mac for attacks. Together, these powerful tools protect against DoS attacks. [Norton™ Personal Firewall for Macintosh®](#) monitors all Internet connections to and from your Mac, logging and alerting you to attempted intrusions that could signal a hacker or participation in a DoS attack.
- **Don't share.** Allowing File Sharing on your Mac can make it easier for intruders to gain access to your computer. Unless you're using it for a specific reason, it's best to disable File Sharing. Open up your File Sharing control panel and disable File Sharing. Next, open your Web Sharing control panel and disable Web Sharing.
- **Keep an eye out.** If you see the light on your cable or DSL modem blink continuously or remain lit, then your Mac may be helping to attack someone. The light will blink on and off when you are sending or receiving information. If it stays lit, that means packets of data so numerous are passing through your modem that it is at full capacity. Someone might have tricked you into launching a stream of authentication requests at a distant server.
- **Give it a rest.** It's a good idea to shut down your Mac or at least disconnect your Internet connection if you are not using your computer. If you leave it connected while you are out, you may miss warning signs of an intruder or hack attack. If you don't have a firewall, don't make your computer more susceptible to hackers than it already is -- disconnect it when you're not using it.

Protecting your computer with a firewall and intrusion detection software is the best way to make sure your Mac doesn't become part of a DoS attack on someone else's system. Protect your Mac with Norton Personal Firewall today and you won't lend a helping hand to hackers.

[Tell a friend about this article.](#)

[Return to the Symantec Macintosh Security Site](#)