

# Cisco Systems "10 Basic Cyber Security Tips for Small Businesses"

*Cisco Systems' Network Security Experts Contribute to White House & Congressional Efforts to Understand and Address Internet Security*

The recent series of denial of service (hacker) attacks against high profile Web sites focused the nation's attention on the issue of Internet security. To address public concerns and improve their own understanding of the issues involved, government leaders convened a series of meetings and hearings to learn more. Every time the topic turned to network security, our nation's leaders turned to Cisco Systems.

On March 9, 2000, Roger Farnsworth of Cisco testified before the Senate Committee on Small Business on the security challenges and solutions facing small businesses online. Included as part of Roger Farnsworth testimony are the Cisco Top 10 Basic Security Tips for Small Businesses. Those tips are listed below. Roger Farnsworth's complete testimony as well as the testimonies from additional Cisco security representatives at the other recent government hearings can be found at [www.cisco.com/go/gov](http://www.cisco.com/go/gov) under the NetNews section.

## Cisco Systems "10 Basic Cyber Security Tips for Small Businesses"

1. Encourage or require employees to choose strong passwords. Hacker programs available on the Internet contain tens of thousands of common passwords, which can be used to break into unsecured computer systems. A password should have a minimum of 8 characters. They should be non-dictionary words. They should combine upper and lower case characters. You can even mix in a symbol, like a \$. An ideal password might be something like 2B3#N3\$.
2. Require new passwords every 90 days. By the time a hacker gets your password, it will already be outdated.
3. Make sure your virus protection subscription is current. Most businesses purchase virus protection programs from companies like Norton or McAfee. These companies regularly offer patches and updates to their programs to respond to new threats. Companies should regularly check for defense improvements and be sure their subscription to virus protection updates remains current.
4. Educate employees about attachments. Just because it's in the "in-box" doesn't mean it's been cleared through any security mechanism. Attachments, particularly executables (with .exe at the end) can be dangerous, dropping off a little software code called a "Trojan Horse" that corrupts your system or allows it to be infiltrated at a later time. Employees should be educated about security basics, including the need to avoid opening attachments from unknown sources.
5. Install a total solution. If you're securing your own system (instead of relying upon an ISP or Web host), don't just throw a firewall at a network and call it secure. Firewalls do a great job of securing a perimeter, but no one device will do the trick. Complete solutions should include firewalling, intrusion detection and policy management.
6. Assess your security posture regularly. Don't secure and run. Hackers are constantly updating their technology. Small and medium businesses need to know how they stack up against the most current types of attack. If you're relying on a Web host or ISP, be sure to choose a vendor who is security savvy. Compare their offerings to those of other companies.

7. When an employee leaves a company, remove the employee's network access immediately. When asked to evaluate the internal security posture of networks, the Cisco Security Consulting team finds vulnerabilities in almost every network tested. Just as you ask departing employees to turn in their keys to the front door, you should take away their key to the network when they leave. Disgruntled employees are the greatest threat to any systems' security.
8. If you allow people to work at home, provide a secure, centrally managed server for remote traffic. Telecommuting increases worker satisfaction and productivity. But it also presents a security challenge. It makes little sense to spend \$10,000 on a security system for your Web site while you allow people to dial-in to your network unabated.
9. Update your Web server software regularly. Stay on top of security updates and patches. These are often available for free over the Web. Make sure you're always running the latest versions of software to stay ahead of hackers, who are certainly working to stay ahead of you.
10. Don't run any unnecessary network services. If your employees don't need Web access, don't provide it. If you don't need services such as NFS, Finger, Echo or some of the other programs that are routinely provided with software suites, make sure they're turned off. Often, a variety of services are provided by default in a program. Exploitation of these services is one of the most common hacks seen by Cisco customers.



**Corporate Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
<http://www.cisco.com>  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 526-4100

**European Headquarters**  
 Cisco Systems Europe s.a.r.l.  
 Parc Evolic, Batiment L1/L2  
 16 Avenue du Quebec  
 Villebon, BP 706  
 91961 Courtaboeuf Cedex  
 France  
<http://www-europe.cisco.com>  
 Tel: 33 1 69 18 61 00  
 Fax: 33 1 69 28 83 26

**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
<http://www.cisco.com>  
 Tel: 408 526-7660  
 Fax: 408 527-0883

**Asia Headquarters**  
 Nihon Cisco Systems K.K.  
 Fuji Building, 9th Floor  
 3-2-3 Marunouchi  
 Chiyoda-ku, Tokyo 100  
 Japan  
<http://www.cisco.com>  
 Tel: 81 3 5219 6250  
 Fax: 81 3 5219 6001

**Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at <http://www.cisco.com/offices>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
 Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia  
 Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore  
 Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela