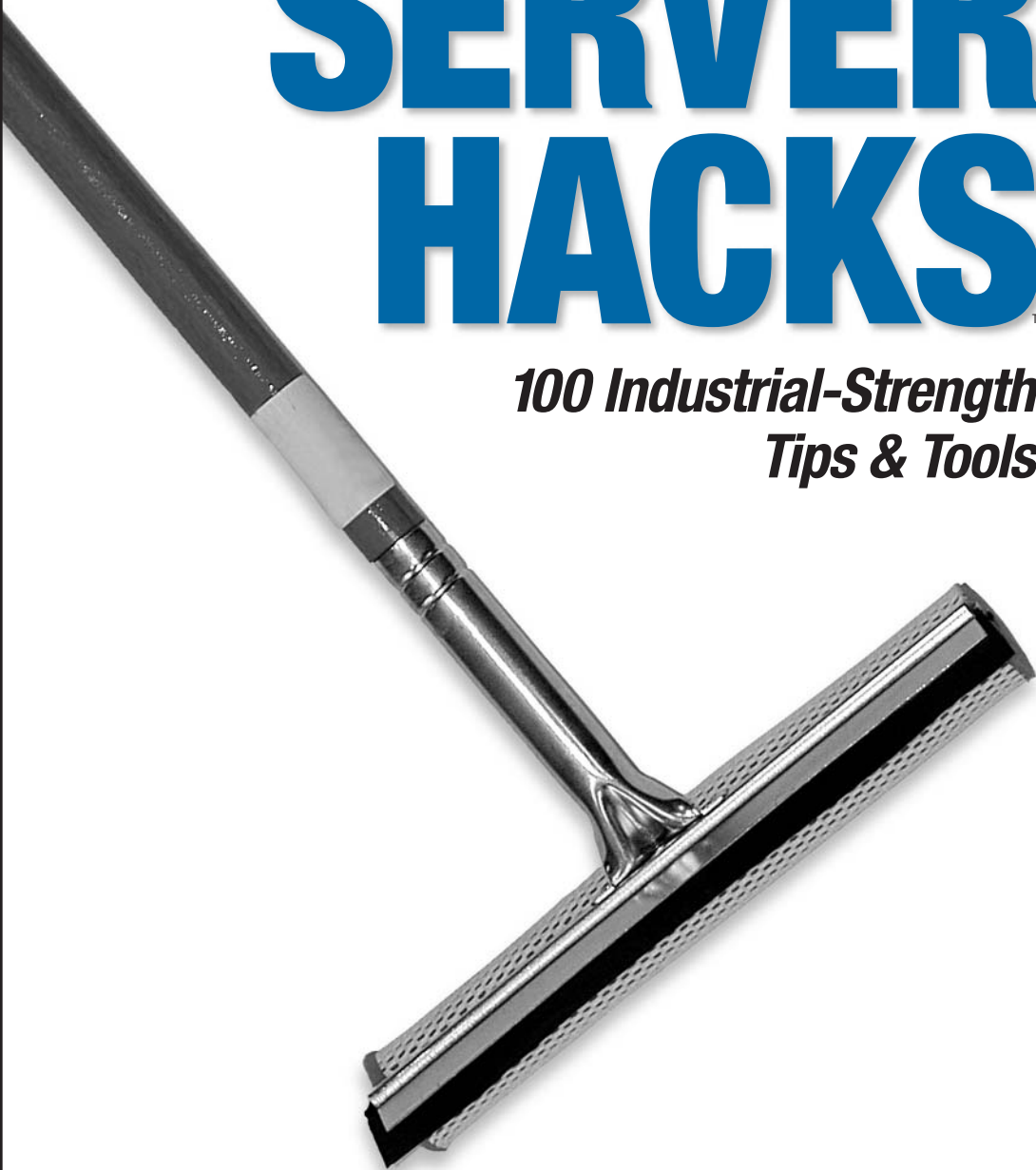


WINDOWS SERVER HACKS™

*100 Industrial-Strength
Tips & Tools*



O'REILLY®

Mitch Tulloch

HACK
#77

Security FAQ

Rod Trent, CEO of myITforum.com, shares his answers to common security questions.

At myITforum.com (<http://www.myitforum.com>), we often get questions regarding general network-security issues, and I try to answer them in the form of a Security FAQ. Here's a short selection of the most common questions we receive, along with my responses. You can find more security tips at myITforum.com.

Steps to Computer Security

Q: *What can I do to make sure my computer is secure?*

A: It depends on whether you are a consumer or a business.

Consumers. Consumers should start by using an Internet firewall on all PCs and laptops. An Internet firewall can help prevent outsiders from getting to your computer through the Internet. If you use Windows XP, enable the built-in firewall feature on that platform. You should also update your computer regularly, either by using the Automatic Updates feature or by regularly visiting the Windows Update web site to download the latest Microsoft security updates. Also, make sure your antivirus software is up-to-date; installing, configuring and maintaining your antivirus software is absolutely essential.

Businesses. Businesses should follow a similar but more involved procedure. Start by verifying the configuration of your firewalls for both Internet and intranet. By auditing your firewall configurations, you ensure they comply with your company's security policy. Firewalls are your first line of defense, and best practice requires blocking all ports that are not actually being used by applications on your network. Business should also protect their networks by requiring employees to follow the precautions outlined by Microsoft (<http://www.microsoft.com/protect/>) on both their home PCs and laptops, especially if they use these machines to connect to your enterprise. PCs and laptops that VPN or RAS into your network must be protected by a properly configured firewall.

Businesses must also keep their systems up-to-date with the latest security patches from Microsoft. To do so, subscribe to Microsoft's free security notification service and use Microsoft update services to automatically obtain patches for your network, see "Microsoft Security Tools" [Hack #78] for more information. Finally, business should invest in antivirus software,

because such protection is absolutely essential for keeping sensitive business data safe from attackers.

Vulnerability Types

Q: *What are the vulnerability types that I need to monitor against?*

A: A: There are three basic types of vulnerability:

Administrative vulnerability

The failure to observe administrative best practices, such as using a weak password or logging onto an account that has more user rights than the user requires to perform a specific task.

Product vulnerability

A security-related bug in a product that is addressed by a security bulletin/hotfix or a service pack.

Physical vulnerability

The failure to provide physical security for a computer. Physical vulnerability can include leaving an unlocked workstation running in an area that is accessible to unauthorized users, leaving a server room unlocked or open, or losing a laptop or leaving it at a customer site.

Strong Password Policy

Q: *What is the best practice to follow when creating policies for user passwords?*

A: Each company's security-level needs are different, but in general, strong passwords should be at least six characters long, should not contain all or part of the user's account name, and should contain at least three of the four following categories of characters: uppercase letters, lowercase letters, Base 10 digits, and nonalphanumeric symbols found on the keyboard, such as !, @, and #.

How Microsoft Handles Security

Q: *Is there any documentation on how Microsoft handles security against worms and viruses?*

A: Yes. Microsoft has released a "Security at Microsoft" white paper on how they handle security issues (<http://www.microsoft.com/downloads/details.aspx?FamilyID=73f1ba8e-a15c-4c05-be87-8d21b1372485>). This paper describes what Microsoft's Corporate Security Group does to prevent malicious or unauthorized use of digital assets at Microsoft. This asset protection takes place through a formal risk-management frame-

work, risk-management processes, and clear organizational roles and responsibilities. The basis of the approach is recognition that risk is an inherent part of any environment and that risk should be proactively managed. The principles and techniques described in Microsoft's white paper can be employed to manage risk at any organization.

Reporting Security Incidents to Microsoft

- Q:** *How can I report a security incident or vulnerability to Microsoft?*
- A:** If you have purchased Microsoft support, you should contact your Technical Account Manager (TAM). You can also use the web form at <https://s.microsoft.com/technet/security/bulletin/alertus.asp> to submit incidents and vulnerabilities.

Reporting Security Incidents to Government Authorities

- Q:** *We've just had a security incident. Who can I call to report it?*
- A:** The FBI encourages the public to report any suspected violations of U.S. federal law. Never think that your security incident is insignificant. Your incident might be part of a larger attack or the beginning of a larger attack. You can find your local FBI Field Division information at <http://www.fbi.gov/contact/fo/fo.htm>.

Getting Government Security Clearance

- Q:** *How can you apply for security clearance for a government job?*
- A:** In our daily newsletter at [myITforum.com](http://www.myitforum.com) (<http://www.myitforum.com/newsletter.asp>), we sometimes post open positions for jobs in the government sector that require special security clearance before applying. Several folks have wondered what it takes to get the security clearance, and a list of good tidbits of information were posted to the [myITforum.com](http://www.topica.com/lists/myOTforum/) Off-Topic list (<http://www.topica.com/lists/myOTforum/>). Here are some additional places you can find information on government security clearance:

FBI Information Sheet

<http://www.fbi.gov/clearance/securityclearance.htm>

Security Clearance for IT Pros

http://www.jobcircle.com/career/coach/jf_2002_09.html

Security Clearances

<http://www.taonline.com/securityclearances/>

—Rod Trent