31 Ways To Make Your Computer System More Secure

1. Move to more secure Microsoft® Windows® systems.

Windows NT, 2000 and XP can be made more secure than Windows 95 or 98. When replacing Windows 95 or 98 systems, replace them with Windows 2000 or XP machines. Windows NT, 2000 and XP are not very secure the way they are typically installed, but they can be made very secure.

2. Operate the computer using the lowest level of privileges.

If someone is both an administrator of a system and a frequent user of that system, set up two usernames for that person. One would be as administrator. The other username would be as a "normal user." That "normal user" should only have the rights needed to operate the computer for normal use.

Most of the time the computer's user should logon as the "normal user" username. When system changes need to be made, logon as the administrator.

This reduces the risk of someone hacking the system using administrator rights.

3. Secure Internet Explorer

Configure the Internet Zone.

CATEGORY	SETTING	SUGGESTED	OPTIONAL
ActiveX controls and plug-ins	Script ActiveX controls marked "safe for scripting"	Disable	
Cookies	Allow per session cookies (not stored)	Enable	Disable for more security.
Downloads	File download	Enable	
Scripting	Active scripting	Enable	Disable for more security.

These settings can be made less restrictive for Web sites that you trust.

4. What do you do with old computers?

Why bother to shred documents, and then set the computer out for anyone to take?

This could be the worst security hole! We have gone to seminars on security and read many books on security, but this topic has not come up. In our office building we have seen computers labeled "trash" for the cleaning crew to take. Those computers may have credit card numbers, Social Security Numbers and

customer lists. If someone takes a computer loaded with confidential information out of the trash he is a recycler, not a thief! This could be the easiest way to get hacked.

Washington Post 11/12/2000: "*Another CIA employee alleged in a lawsuit filed last year by Roy Krieger, an Alexandria lawyer, that she was disciplined for a 'major lapse of CIA security' after the CIA sold 25 laptop computers at public auction 'while still containing Top Secret information on their respective hard drives.*'"

5. Laptops require even greater security than desktop computers.

Laptop computers can be more easily stolen from an office. It is not unusual to have laptops stolen from hotel rooms. If you are using a laptop computer in a client's or customer's office, lack of security might send your client a message that you could be sloppy with his confidential information on that computer when you visit another client.

Password protect the screen saver, if the laptop is going to contain confidential information and if it going to leave the office. Set the screen saver to go off after either 5, 10 or 15 minutes of inactivity, depending on the nature of the information in the computer.

6. Be careful of new operating systems.

New versions of operating systems, such as Windows, often come with security issues such as buffer overflow problems. Avoid new operating systems, if possible, until the first service pack has been released.

If you must buy a system that has a newly released operating system, check for security patches.

7. Use the Windows Update Button.

Starting with Windows 98, you can use the Windows Update Button to see what updates your system can use to make it more secure and function better. The Windows Update Button will take you online to compare your system against available patches.

Some of these patches are huge. Often you can order an inexpensive patch or service pack from Microsoft, and they will send you a CD. This is the best way to go if you have lots of similar systems.

Be sure to backup your system first! Windows patches have been known to trash systems!

8. Use encryption or a Virtual Private Network (VPN) for confidential Internet correspondence.

In situations where sensitive or confidential information is going to be discussed over the Internet, use encryption or a VPN to scramble the information.

A VPN may be appropriate for communication between branch offices, between a home office and the main office or between business "partners".

If a limited amount of confidential information is going to be transmitted, consider using less costly but effective email encryption.

9. Make sure you don't have Microsoft's Internet Information Server (IIS) security holes.

Determine if IIS is running on your system. If it is and it is not needed, remove it.

If it is needed for some other program like FrontPage®, make sure you have taken advantages of Microsoft security patches.

Many of the IIS security holes are associated with its index server, ISAPI dll. You might want to consider removing application mapping with respect to ISAPI.

10. Use an appropriate backup policy.

It is important to have three to four, possibly more, sets of backups. The most recent set of backups should be stored away from the business.

Critical information, such as accounting system or customer lists, should be archived in some way after there has been a significant change since the last archive or backup. It is up to the business to determine what constitutes a significant change. Keep these archived files possibly for months.

Image saving products, like Norton Ghost™, might be considered in addition to the standard CD or tape backups.

If appropriate, buy an industrial strength backup system rather than the program that is included with Windows.

Backup the system before applying any Microsoft updates!

11. Backup tapes as security risks.

Backup tapes contain information that can be used to hack a system. Backup tapes contain the same sensitive material that is on the computer. Consider password protecting backup tapes.

12. Choose an appropriate password policy.

Lets face it. Passwords are a real pain. At the very least they should be "strong" passwords. Depending on the security risks, more password policies should be added.

A strong password should be at least seven or eight characters, contain numbers, special characters and upper and lower case letters. No names or words should be included in the password. If possible, include a non printing character. If password cracking software prints out a list of usernames and passwords, a non printing character often shows up as a blank. Thus, the

password cracking software might guess the non printing character, but whoever looks at the output won't be able to figure out what it is!

Windows NT, 2000 and XP have settings that can be used to help enforce password policies. Depending on security needs, passwords should be required to unlock screensavers or to shut down the computer. Those versions of Windows can require that passwords be changed at an appropriate interval.

One Windows setting is to remember user's old passwords. When this is set, it makes it harder for a user to change his new password to his old password.

Recommended password policy:

POLICY	RANGE
Maximum Password Age	30-60 days
Minimum Password Age	3 days
Minimum Password Length	7-8
Password Uniqueness – Remember	5-10 passwords
Lockout after	5 – 10 bad logon attempts
Reset count after	30 minutes
Lockout duration	240 minutes

Make sure notes that have passwords on them are not taped near the computer! Consider banning Post-It Notes near computers. Make sure documents with passwords are not in the same desk drawer where the pencils are kept! That is one of the first places that someone will look.

The ideal situation is for the user to simply remember the password. That is considered a "best practice" when it comes to security. In real life, remembering all passwords to access the computer and various Internet sites may be impossible. At the very least, make sure any password list is well hidden.

What happens if the Administrator quits? When the Administrator's password is chosen or changed that information should be put in a safe place such as a safe deposit box. This enables another person to logon as Administrator if needed.

13. Try to hide the Administrator's username.

First rename the Administrator's account username to something like "Nobody". Then create a new account with the name Administrator. That new account Administrator account should be given very restricted rights.

This will not stop a hacker, but it can slow a hacker down.

14. Use free security tools to check for vulnerabilities.

15. Lock down systems at night.

We know of someone who came to work one morning to find that the default language was changed to Spanish. The computer owner really preferred to work

on a system that communicated in English. Fortunately, is was trivial to switch the system back to English.

That just goes to show how easy a janitor or someone working with the janitor can gain access. Do the janitors know who can have access to the office? What if someone, pretending to be an employee, told a janitor that they had to work late?

Either turn the system off at night, or make sure that password controlled screen saver was activated. Depending on the value of the system and data, the system could be made physically difficult to remove.

16. Have someone try to hack your system!

This is one way to find out how easy it is to break into the system.

17. Beware of visitors.

Don't let unknown visitors or couriers wander in the office. The easiest way to steal information that is in the computer is to steal the computer first!

18. Keep your email addresses to yourself.

When sending one email to many people, use Blind Carbon Copy (bcc), unless you want others to see lots of email addresses. This could provide contact information to competitors, and your clients and customers may consider this a breach of confidentiality.

19. Set up appropriate security logs.

We recommend security log settings as follows:

Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory services	No auditing
Audit logon events	Success, Failure
Audit event access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Increase the log size to over 4MB. Change to above as needed for your systems specific needs.

When the log gets full, save the log to have an extension of .txt, and compress that .txt file. That way the archived log file can be reviewed if something needs to be investigated.

Use the Windows Event Viewer to view the logs. The Windows Event Viewer is pretty well hidden. Move it to the desktop so it can be more easily viewed.

20. Create an Emergency Repair Disk (ERD).

You probably made an ERD when a new system was delivered. That is not enough! After any major changes, update or create a new ERD. Also, backup the registry.

21. Make sure you are on email lists to find out about security holes and viruses.

Make sure you do this when you register your virus scanner.

We also recommend to get on CERT's email list. They might notify you of a problem before the developer of your virus scanner or firewall does.

22. Configure your email program for security.

Disable the use of JavaScript, Vbscript, executables and ActiveX components, if possible, in your email. This is particularly important with Outlook Express.

23. Beware of temporary workers.

Set up a new account for any temporary worker. When that temporary worker is no longer working, remove the account. We don't think that Windows yet has this feature, but it would be nice to indicate that if a temp is to work one week, you could then setup the computer account to last only one week.

24. Have an incident response plan ready.

Even if you don't formalize how security incidents will be handled, at least think about what you might do. It is best to write down how a security incident would be handled. What would you do if someone stole your computer that contained tax preparation software and files. If someone can access those files, they can get your clients' Social Security Numbers and the location of their financial accounts.

Recently, we were notified that our Web hosting company had a security problem. They recommended that we immediately change passwords. We were very appreciative that they acted so quickly.

25. Close the Server Message Block (SMB), Common Internet File System (CIFS), NetBIOS, Null Session security hole.

Windows ships with this vulnerability wide open. Microsoft calls this a feature not a bug! When you are on the Internet, it is fairly easy to find information about your system if this security hole is not closed. You can use firewalls or system modifications to close this. You might discuss this with the vendor that sold you the system.

26. Each system that accesses the Internet should have a personal firewall even if your network has a firewall.

Personal firewall software is quite good and inexpensive.

27. Clear Page File at shutdown.

The Page File is where Windows stores old information. Just because it is old doesn't mean it is not sensitive. A hacker could start your system with an alternate operating system to view the contents of the Page File.

Use the Windows setting to Clear Page File At Shutdown.

28. Don't let a hacker hide files from you.

Some hackers can put backdoors into your system. A backdoor makes it easier for a hacker to return to a hacked system. Part of a backdoor would be to put files onto your system that could be run from a remote location, then hide those files from view. Make sure your Windows Explore is configured to display extensions and hidden files.

29. Watch out for search engines.

Don’t expose your hard drive structure to be searched by public search engines. The default home of Microsoft’s Internet Information Server (IIS) is \inetpub. If you search for “inetpub” on many search engines you can find part of the Web server’s private directory structure. On Alta Vista “inetpub” came up only 137,835 times! Most of those search links were probably unwelcome, but the owners of those Web sites have no idea how easy it is for the public to look into their “bedroom windows”.

30. Schedule periodic security examinations.

Computer security is an on going process not a one time project. Policies that provided good security one year ago, may not be sufficient now. Check to see if there are security updates available to your systems. Backup your system immediately before applying any major update that effect a system!

31. Be careful what you put on mission critical systems.

Do not put Microsoft Office, MS Outlook Express or IIS on critical systems unless absolutely required.