10 Immutable Laws of Security (Microsoft TechNet)

Archived content. No warranty is made as to technical accuracy. Content may contain URLs that were valid when originally published, but now link to sites or pages that no longer exist.

Here at the Microsoft Security Response Center, we investigate thousands of security reports every year. In some cases, we find that a report describes a bona fide security vulnerability resulting from a flaw in one of our products; when this happens, we develop a patch as quickly as possible to correct the error. (See "A Tour of the Microsoft Security Response Center"). In other cases, the reported problems simply result from a mistake someone made in using the product. But many fall in between. They discuss real security problems, but the problems don't result from product flaws. Over the years, we've developed a list of issues like these, that we call the 10 Immutable Laws of Security.

Don't hold your breath waiting for a patch that will protect you from the issues we'll discuss below. It isn't possible for Microsoft—or any software vendor—to "fix" them, because they result from the way computers work. But don't abandon all hope yet—sound judgment is the key to protecting yourself against these issues, and if you keep them in mind, you can significantly improve the security of your systems.

On This Page

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore

It's an unfortunate fact of computer science: when a computer program runs, it will do what it's programmed to do, even if it's programmed to be harmful. When you choose to run a program, you are making a decision to turn over control of your computer to it. Once a program is running, it can do anything, up to the limits of what you yourself can do on the computer. It could monitor your keystrokes and send them to a website. It could open every document on the computer, and change the word "will" to "won't" in all of them. It could send rude emails to all your friends. It could install a virus. It could create a "back door" that lets someone remotely control your computer. It could dial up an ISP in Katmandu. Or it could just reformat your hard drive.

That's why it's important to never run, or even download, a program from an untrusted source—and by "source," I mean the person who wrote it, not the person who gave it to you. There's a nice analogy between running a program and eating a sandwich. If a stranger walked up to you and handed you a sandwich, would you eat it? Probably not. How about if your best friend gave you a sandwich? Maybe you would, maybe you wouldn't—it depends on whether she made it or found it lying in the street. Apply the same critical thought to a program that you would to a sandwich, and you'll usually be safe.

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore

In the end, an operating system is just a series of ones and zeroes that, when interpreted by the processor, cause the computer to do certain things. Change the ones and zeroes, and it will do something different. Where are the ones and zeroes stored? Why, on the computer, right along with everything else! They're just files, and if other people who use the computer are permitted to change those files, it's "game over".

To understand why, consider that operating system files are among the most trusted ones on the computer, and they generally run with system-level privileges. That is, they can do absolutely anything. Among other things, they're trusted to manage user accounts, handle password changes, and enforce the rules governing who can do what on the computer. If a bad guy can change them, the now-untrustworthy files will do his bidding, and there's no limit to what he can do. He can steal passwords, make himself an administrator on the computer, or add entirely new functions to the operating system. To prevent this type of attack, make sure that the system files (and the registry, for that matter) are well protected. (The [security checklists]() on the [Microsoft Security]() website will help you do this).

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

Oh, the things a bad guy can do if he can lay his hands on your computer! Here's a sampling, going from Stone Age to Space Age:

- He could mount the ultimate low-tech denial of service attack, and smash your computer with a sledgehammer.
- He could unplug the computer, haul it out of your building, and hold it for ransom.
- He could boot the computer from a floppy disk, and reformat your hard drive. But wait, you say, I've configured the BIOS on my computer to prompt for a password when I turn the power on. No problem – if he can open the case and get his hands on the system hardware, he could just replace the BIOS chips. (Actually, there are even easier ways).
- He could remove the hard drive from your computer, install it into his computer, and read it.
- He could make a duplicate of your hard drive and take it back his lair. Once there, he'd have all the time in the world to conduct brute-force attacks, such as trying every possible logon password. Programs are available to automate this and, given enough time, it's almost certain that he would succeed. Once that happens, Laws #1 and #2 above apply.
- He could replace your keyboard with one that contains a radio transmitter. He could then monitor everything you type, including your password.

Always make sure that a computer is physically protected in a way that's consistent with its value—and remember that the value of a computer includes not only the value of the hardware itself, but the value of the data on it, *and* the value of the access to your network that a bad guy could gain. At a minimum, business-critical computers like domain controllers, database servers, and print/file servers should always be in a locked room that only people charged with administration and maintenance can access. But you may want to consider protecting other computers as well, and potentially using additional protective measures.

If you travel with a laptop, it's absolutely critical that you protect it. The same features that make laptops great to travel with – small size, light weight, and so forth—also make them easy to steal. There are a variety of locks and alarms available for laptops, and some models let you remove the hard drive and carry it with you. You also can use features like the Encrypting File System in Microsoft Windows® 2000 to mitigate the damage if someone succeeded in stealing the computer. But the only way you can know with 100% certainty that your data is safe and the hardware hasn't been tampered with is to keep the laptop on your person at all times while traveling.

Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more

This is basically Law #1 in reverse. In that scenario, the bad guy tricks his victim into downloading a harmful program onto his computer and running it. In this one, the bad guy uploads a harmful program to a computer and runs it himself. Although this scenario is a danger anytime you allow strangers to connect to your computer, websites are involved in the overwhelming majority of these cases. Many people who operate websites are too hospitable for their own good, and allow visitors to upload programs to the site and run them. As we've seen above, unpleasant things can happen if a bad guy's program can run on your computer.

If you run a website, you need to limit what visitors can do. You should only allow a program on your site if you wrote it yourself, or if you trust the developer who wrote it. But that may not be enough. If your website is one of several hosted on a shared server, you need to be extra careful. If a bad guy can compromise one of the other sites on the server, it's possible he could extend his control to the server itself, in which he could control all of the sites on it—including yours. If you're on a shared server, it's important to find out what the server administrator's policies are. (By the way, before opening your site to the public, make sure you've followed the [security checklists](#) for IIS 4.0 and IIS 5.0).

Law #5: Weak passwords trump strong security

The purpose of having a logon process is to establish who you are. Once the operating system knows who you are, it can grant or deny requests for system resources appropriately. If a bad guy learns your password, he can log on as you. In fact, as far as the operating system is concerned, he **is** you. Whatever you can do on the system, he can do as well, because he's you. Maybe he wants to read sensitive information you've stored on your computer, like your e-mail. Maybe you have more privileges on the network than he does, and being you will let him do things he normally couldn't. Or maybe he just wants to do something malicious and blame it on you. In any case, it's worth protecting your credentials.

Always use a password—it's amazing how many accounts have blank passwords. And choose a complex one. Don't use your dog's name, your anniversary date, or the name of the local football team. And don't use the word "password"! Pick a password that has a mix of upper- and lower-case letters, number, punctuation marks, and so forth. Make it as long as possible. And change it often. Once you've picked a strong password, handle it appropriately. Don't write it down. If you absolutely must write it down, at the very least keep it in a safe or a locked drawer—the first thing a bad guy who's hunting for passwords will do is check for a yellow sticky note on the side of your screen, or in the top desk drawer. Don't tell anyone what your password is. Remember what Ben Franklin said: two people can keep a secret, but only if one of them is dead.

Finally, consider using something stronger than passwords to identify yourself to the system. Windows 2000, for instance, supports the use of smart cards, which significantly strengthens the identity checking the system can perform. You may also want to consider biometric products like fingerprint and retina scanners.

Law #6: A computer is only as secure as the administrator is trustworthy

Every computer must have an administrator: someone who can install software, configure the operating system, add and manage user accounts, establish security policies, and handle all the other management tasks associated with keeping a computer up and running. By definition, these tasks require that he have control over the computer. This puts the administrator in a position of unequalled power. An untrustworthy administrator can negate every other security measure

you've taken. He can change the permissions on the computer, modify the system security policies, install malicious software, add bogus users, or do any of a million other things. He can subvert virtually any protective measure in the operating system, because he controls it. Worst of all, he can cover his tracks. If you have an untrustworthy administrator, you have absolutely no security.

When hiring a system administrator, recognize the position of trust that administrators occupy, and only hire people who warrant that trust. Call his references, and ask them about his previous work record, especially with regard to any security incidents at previous employers. If appropriate for your organization, you may also consider taking a step that banks and other security-conscious companies do, and require that your administrators pass a complete background check at hiring time, and at periodic intervals afterward. Whatever criteria you select, apply them across the board. Don't give anyone administrative privileges on your network unless they've been vetted – and this includes temporary employees and contractors, too.

Next, take steps to help keep honest people honest. Use sign-in/sign-out sheets to track who's been in the server room. (You do have a server room with a locked door, right? If not, re-read Law #3). Implement a "two person" rule when installing or upgrading software. Diversify management tasks as much as possible, as a way of minimizing how much power any one administrator has. Also, don't use the Administrator account—instead, give each administrator a separate account with administrative privileges, so you can tell who's doing what. Finally, consider taking steps to make it more difficult for a rogue administrator to cover his tracks. For instance, store audit data on write-only media, or house System A's audit data on System B, and make sure that the two systems have different administrators. The more accountable your administrators are, the less likely you are to have problems.

Law #7: Encrypted data is only as secure as the decryption key

Suppose you installed the biggest, strongest, most secure lock in the world on your front door, but you put the key under the front door mat. It wouldn't really matter how strong the lock is, would it? The critical factor would be the poor way the key was protected, because if a burglar could find it, he'd have everything he needed to open the lock. Encrypted data works the same way—no matter how strong the crypto algorithm is, the data is only as safe as the key that can decrypt it.

Many operating systems and cryptographic software products give you an option to store cryptographic keys on the computer. The advantage is convenience – you don't have to handle the key – but it comes at the cost of security. The keys are usually obfuscated (that is, hidden), and some of the obfuscation methods are quite good. But in the end, no matter how well-hidden the key is, if it's on the computer it can be found. It has to be – after all, the software can find it, so a sufficiently-motivated bad guy could find it, too. Whenever possible, use offline storage for keys. If the key is a word or phrase, memorize it. If not, export it to a floppy disk, make a backup copy, and store the copies in separate, secure locations. (All of you administrators out there who

are using [Syskey](#) in "local storage" mode—you're going to reconfigure your server right this minute, right?)

Law #8: An out of date virus scanner is only marginally better than no virus scanner at all

Virus scanners work by comparing the data on your computer against a collection of virus "signatures". Each signature is characteristic of a particular virus, and when the scanner finds data in a file, email, or elsewhere that matches the signature, it concludes that it's found a virus. However, a virus scanner can only scan for the viruses it knows about. It's vital that you keep your virus scanner's signature file up to date, as new viruses are created every day.

The problem actually goes a bit deeper than this, though. Typically, a new virus will do the greatest amount of damage during the early stages of its life, precisely because few people will be able to detect it. Once word gets around that a new virus is on the loose and people update their virus signatures, the spread of the virus falls off drastically. The key is to get ahead of the curve, and have updated signature files on your computer before the virus hits.

Virtually every maker of anti-virus software provides a way to get free updated signature files from their website. In fact, many have "push" services, in which they'll send notification every time a new signature file is released. Use these services. Also, keep the virus scanner itself—that is, the scanning software—updated as well. Virus writers periodically develop new techniques that require that the scanners change how they do their work.

Law #9: Absolute anonymity isn't practical, in real life or on the Web

All human interaction involves exchanging data of some kind. If someone weaves enough of that data together, they can identify you. Think about all the information that a person can glean in just a short conversation with you. In one glance, they can gauge your height, weight, and approximate age. Your accent will probably tell them what country you're from, and may even tell them what region of the country. If you talk about anything other than the weather, you'll probably tell them something about your family, your interests, where you live, and what you do for a living. It doesn't take long for someone to collect enough information to figure out who you are. If you crave absolute anonymity, your best bet is to live in a cave and shun all human contact.

The same thing is true of the Internet. If you visit a website, the owner can, if he's sufficiently motivated, find out who you are. After all, the ones and zeroes that make up the Web session have to be able to find their way to the right place, and that place is your computer. There are a lot of measures you can take to disguise the bits, and the more of them you use, the more thoroughly the bits will be disguised. For instance, you could use network address translation to mask your actual IP address, subscribe to an anonymizing service that launders the bits by

relaying them from one end of the ether to the other, use a different ISP account for different purposes, surf certain sites only from public kiosks, and so on. All of these make it more difficult to determine who you are, but none of them make it impossible. Do you know for certain who operates the anonymizing service? Maybe it's the same person who owns the website you just visited! Or what about that innocuous website you visited yesterday, that offered to mail you a free $10 off coupon? Maybe the owner is willing to share information with other website owners. If so, the second website owner may be able to correlate the information from the two sites and determine who you are.

Does this mean that privacy on the Web is a lost cause? Not at all. What it means is that the best way to protect your privacy on the Internet is the same as the way you protect your privacy in normal life—through your behavior. Read the privacy statements on the websites you visit, and only do business with ones whose practices you agree with. If you're worried about cookies, disable them. Most importantly, avoid indiscriminate Web surfing—recognize that just as most cities have a bad side of town that's best avoided, the Internet does too. But if it's complete and total anonymity you want, better start looking for that cave.

Law #10: Technology is not a panacea

Technology can do some amazing things. Recent years have seen the development of ever-cheaper and more powerful hardware, software that harnesses the hardware to open new vistas for computer users, as well as advancements in cryptography and other sciences. It's tempting to believe that technology can deliver a risk-free world, if we just work hard enough. However, this is simply not realistic.

Perfect security requires a level of perfection that simply doesn't exist, and in fact isn't likely to ever exist. This is true for software as well as virtually all fields of human interest. Software development is an imperfect science, and all software has bugs. Some of them can be exploited to cause security breaches. That's just a fact of life. But even if software could be made perfect, it wouldn't solve the problem entirely. Most attacks involve, to one degree or another, some manipulation of human nature—this is usually referred to as social engineering. Raise the cost and difficulty of attacking security technology, and bad guys will respond by shifting their focus away from the technology and toward the human being at the console. It's vital that you understand your role in maintaining solid security, or you could become the chink in your own systems' armor.

The solution is to recognize two essential points. First, security consists of both technology and policy—that is, it's the combination of the technology and how it's used that ultimately determines how secure your systems are. Second, security is journey, not a destination—it isn't a problem that can be "solved" once and for all; it's a constant series of moves and countermoves between the good guys and the bad guys. The key is to ensure that you have good security awareness and exercise sound judgment. There are resources available to help you do this. The Microsoft Security website, for instance, has hundreds of white papers, best practices guides,

checklists and tools, and we're developing more all the time. Combine great technology with sound judgment, and you'll have rock-solid security.