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? 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. In modern operating systems, default settings largely prevent anyone but administrators from making such bedrock changes. Preventing rogue programs from gaining administrative-level access is the best way of protecting the operating system. That's best accomplished by not operating your computer from an account with administrative privileges except when specific tasks make it absolutely necessary and logging out of that high-privilege mode as quickly as possible once your task is complete. Home users should consider creating an "everyday" account set to operate with standard-level user permissions. On those relatively rare occasions when you really do need to make big changes, you can log into the administrative account, do whatever needs to be done, and switch back to the safer account when you're finished.

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 removable media, 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 chip. (Actually, there are even easier ways).
He could remove the hard drive from your computer, install it into his computer, and read any unencrypted data.
He could duplicate your hard drive and take it back to his lair. Once there, he'd have all the time in the