

21 May 2007

By: Marius Oiaga, Technology News Editor

Windows Vista
Microsoft

[When Windows Vista Is Not Your Windows Vista](#)

Anymore

There are certain scenarios when Windows Vista is no longer your Windows Vista. In this respect, Microsoft has outlined a set of situations that ultimately result in the users losing control over the operating system. I recently stumbled upon the Redmond Company's "[10 Immutable Laws of Security](#)" put together by the Microsoft Security Response Center. Each law describes a specific situation where neither Microsoft nor any other software vendor will be able to prevent an attacker from taking over the computer. Microsoft's immutable laws are generalized, but almost all can be interpreted and focused on Windows Vista. The first law involves social engineering. Users that are persuaded, or tricked by various incentives to run malicious programs on their machines will lose complete control over the computer, Vista or no Vista. Even if Microsoft has applauded its latest operating system as being the most secure Windows platform to date, once malicious code gets past the security barriers with the help of the user, Vista is compromised. In case an attacker manages to get access to the operating system files on the computer and also gains system-level privileges in the context, you can say goodbye to your Windows Vista. "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," Microsoft explained. Unrestricted physical access to your computer is also a guarantee that you'll lose Vista. BIOS passwords, users accounts and BitLocker Drive Encryption can all fall to attacks. Complete physical access is synonymous with a high level of risk. The same is valid for a weak password. Even in Windows Vista users are advised to choose strong passwords, combinations of lowercase and uppercase letters with numbers and punctuation marks and to keep them safe. But whatever you do, don't write them down on a yellow post-it stuck near the monitor. Additionally keep in mind that "encrypted data is only as secure as the decryption key." In the end, Windows Vista will remain your operating system if it and all the software that runs on top are up to date with the latest security patches. No code is foolproof or perfect and this is the case for Vista, an unpatched vulnerability is nothing else but an open door.