Networking: Protecting your MP3s

July 24 2006

You probably have a lot of MP3 files -- like the smash hit "Crazy" by the U.K.'s Gnarls Barkley -- on your PC. Maybe some oldies too, and a lot of other computer files, with extensions like .EXE, .MPEG, .JPEG, and other, often confusing, file formats.

With all that valuable content, maybe you should think about maximizing your Windows XP operating system, getting more out of it than just playing MP3s, and also securing those expensive files from iTunes?

There has been so much news about phishing expeditions, hackers, crackers and online Russian mafia scams, nefarious folks who want to damage your computer, and those expensive files, just for fun.

The anti-virus software developer McAfee recently released a report that indicated that the number of vulnerabilities discovered on the Macintosh OS X platform had increased by 228 percent, from 2003 to 2005, while Windows vulnerabilities discovered in the same time period had increased by "only" 73 percent.

But the good news is that you can prevent the loss of those valuable files -- 99 cents a download adds up fast, when you have hundreds of songs on your hard drive -- and improve the performance of your PC with a few simple steps to secure your network, experts tell UPI's Networking.

"Most losses -- are the result of human errors or system loopholes that can be easily and cost-effectively remedied," said Ira Winkler, president of the Internet Security Advisors Group, who has also been dubbed the "James Bond" of computer networking, because of his keen understanding of the high- and low-tech methods used to make computers susceptible to security breaches.

Here are some other, savvy bits of advice from Winkler and other pros:

-- Keep your PC and security software updated, constantly. Just as you put on a seatbelt when driving a car, make sure the operating system is up to date and utilizing the recommended security updates, every time you turn on the computer;

-- You should always install anti-virus, anti-spyware and a personal firewall to protect computer files. Keep your software updated as new viruses and spyware bugs are released virtually daily. One protective software package -- the Office Depot Internet Security Suite -- is available for just $49.99 and shields against viruses, spyware, hackers and phishing scams;

-- Be cautious when working with confidential information. Reviewing documents when traveling or working outside the office can maximize productivity, but if the files include sensitive information, always make sure no one can see what you are working on. A good way to ensure your information remains safe from wandering eyes is to install a laptop privacy filter so only you can see the information. For example, the 3M Notebook Privacy Filter, available for as little as $59.99, darkens screen data from a side view allowing only the user to view information on-screen;

-- Always use passwords and keep them private. Passwords are the simplest way to protect your information, but make sure you don't use basic passwords like your name, birthday or phone number. If you need to write down your password, keep it in a secure location and do not share it. If you need to share your password, change it as soon as you can. If you have trouble remembering passwords, the Microsoft Fingerprint Reader, available for $39.99, lets you log on to your PC and your favorite Web sites with the touch of your finger -- without having to remember all of your passwords;

-- Put your laptop on lockdown -- secure your notebook from theft by attaching a cable lock, such as the Targus Defcon CL notebook computer cable lock, available for as little as $29.99, which tethers it to a desk or other surface. Cable locks are portable and can go on the road, so if you use a laptop at a business center, it can also be secured;

-- Enable Auditing on your Workstations. While this is a fairly normal practice for servers, it is not usually performed on PC workstations unless there is a high risk of data theft. Auditing can include account log on events and account management;

-- Disable default shares. Windows XP automatically creates a number hidden administrative shares that the operating system uses to manage the computer environment on the network. These default shares can be disabled via the Computer Management console in the Control Panel;

-- Disable Dump File Creation. A dump file can be a useful troubleshooting tool when either the system or application crashes and causes the infamous "Blue Screen of Death." However, they also can provide a hacker with potentially sensitive information such as application passwords. You may disable the dump file by going to the Control Panel > System > Advanced > Startup and Recovery and change the options for "Write Debugging Information" to "None";

-- Disable the ability to boot from a floppy or CD-ROM on physically unsecured systems. There are a number of third-party utilities that pose a security risk if used via a boot disk. If your security needs are more extreme, consider removing the floppy and CD drives entirely. As an alternative, store the CPU in a locked external case that still provides adequate ventilation;

According to Dan Hubbard, a security specialist at Websense Inc., the network security consultancy, taking "a proactive approach" will preserve your PC and optimize your ability to use it. There's no better way to protect those MP3s.

Citation: Networking: Protecting your MP3s (2006, July 24) retrieved 25 April 2024 from https://phys.org/news/2006-07-networking-mp3s.html