



update!
update!
update!

STAYING SAFE THESE DAYS MEANS STAYING UP TO DATE.

It feels like we're constantly bombarded by pop-ups alerting us to software updates. But, more often than not, they're for our own protection. A disturbing number of major security threats target holes which were patched years ago. Millions of computers are still vulnerable to these threats because many people simply don't keep their software up to date.

The Conficker worm has been making headlines of late, yet it targets a vulnerability that was fixed by Microsoft in October 2008. Users of the Microsoft Windows XP, Vista and 7 operating systems should be protected, if they've installed the latest MS Service Packs and all the latest Microsoft software updates.

Check the Security tab in your Control Panel to see if your computer is set to install updates automatically. Worms such as Conficker often attempt to disable automatic updates, because their creators know how effective it is.

Naturally you've got your AVG security software malware definition and program updates happening automatically and frequently. You have haven't you? Perhaps you'd better check right now! They are set and forget, for most people. Yet, it's surprising that when we're contacted for help with a problem, we often find people have their automatic updates turned off.

Still, security software updates are only one part of the bigger security picture. While software like **AVG Internet Security** is designed to protect you against the likes of Conficker, prevention is better than cure.

Every second Tuesday of the month is Patch Tuesday over at Microsoft. They release important security updates for Windows, Internet Explorer and other products such as Microsoft Office. Occasionally a patch is so urgent that Microsoft doesn't wait until Patch Tuesday, such as July's fix for a critical security hole in Internet Explorer.



Microsoft's software updates are automatically downloaded in the background and often install themselves as you shut down your computer. If you're worried about bandwidth usage, at least ensure your computer is set to notify you of new updates so you can download and install them when it suits you. If you don't have the monthly bandwidth allowance to download Microsoft's hefty Service Packs, order a CD from the Microsoft website or look for the Service Pack on the cover disc of a computer magazine.

It's not just Microsoft products you need to worry about. You should also set third-party applications such as Firefox, Skype, iTunes and Adobe Reader to automatically alert you to new updates. Any popular application designed to connect to the internet is a tempting target for hackers looking to worm their way into your computer.

The other thing to watch out for is spam e-mail linking to fake patches. Never click on a link in an e-mail to install a Microsoft security patch. Always use the Windows built-in updater, or type **update.microsoft.com** directly into Internet Explorer. Spam is one of the most effective ways for hackers to get malicious software onto your computer, so a healthy paranoia is another important weapon in your security defences.

NZ 0800 284 000
avg.co.nz

AU 1300 284 000
avg.com.au