



TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial
arrangements with vendors.

For more reviews, please
contact TECHNOLEDGE.

T +61 2 9909 0246
E info@technoledge.com.au
W www.technoledge.com.au

The Security Landscape A Guided Tour

PART 3 – SECURITY LAYERS, A ROUGH GUIDE

User level Security

This is the obvious starting point. Most of us are good drivers but we can all have lapses of concentration out on the internet highway. Thousands have fallen for emails from Nigeria offering to deposit millions into their bank accounts in exchange for access to a paltry \$20,000. Thousands of others open email attachments from unknown sources every day, or download wallpaper, screensavers, video clips and movies from risky websites. Some users still fall for those flashing pop-ups that announce they've won a prize or those jumpy ones that offer to fix a few problems on their PCs at a single click.

The majority of accidents can be avoided, simple as that. For a set of effective techniques and tools, see [Driver Training](#) in this resource.

System level security

Windows XP isn't the most secure operating system for PCs. Apple's *OS X* is more secure, and *Linux* more secure again. *Windows Vista* offers many improvements in the area of security but the current implementation is not the most elegant, interfering too much with the user experience.

Windows XP is the most popular operating system for home and business users, and that won't change in the next year or two. Most business users will wait until *Vista's* sharp edges are knocked off and the current compatibility issues are fixed. Meanwhile, *Windows XP* can be made more secure by adjusting some of the inbuilt settings. Here's a full rundown:

<http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm>

You can also read Microsoft's own guide to securing XP here:

<http://www.microsoft.com/downloads/thankyou.aspx?familyId=9faba6ed-2e9c-44f9-bc50-d43d57e17078&displayLang=en>

Network level security. To protect your internal network from malicious attacks, a solid firewall is the first step. Hardware routers can shield your network effectively, while software firewalls can do the much the same for individual PCs. There are many choices and some of these will be covered in a future article.

Application level security. The nastier malware types tend to target the applications we run on our PCs. Using non-Microsoft browsers and email clients for online work can improve overall security, but malicious code can still sneak through.

Some AV products have the ability to check applications for integrity whenever they're launched. Newer products like Host Intrusion Protection Systems do that routinely, once the commonly used applications have been 'white-listed'. *HIPS* concepts and *sandboxing* techniques are new concepts we're exploring at present and will report on in the near future.

PART 1 – [TREACHEROUS TERRAIN](#) PART 2 – [A SNAPSHOT OF CURRENT THREATS](#)