



THE OUTER EDGE

Tall Tales from the
Brink of Sanity

These are BRIARD's own
opinions and may not reflect the
views of TECHNOLEDGE.

Contact BRIARD @
briardpuppy@gmail.com
www.technoledge.com.au

Browser Brawls

PART 3: In the grip of security

The Protection Business

Protection is a thriving business and still we hear security experts complain that we dumb users don't take the dire threats that face us seriously enough. They say things like: The most common cause of an accident is the nut behind the wheel.

As a user, I can tell you what it's like behind the wheel and why some of us have given security away as all too hard. There's also a whiff of suspicion on our side that the threats are hyped up, that the WMD don't really exist and that fear is driven into our hearts to make us buy more protection.

My search for solid protection that was easy to live with led me down a long and winding road.

Norton Nonsense

My first stop was **Norton Antivirus** a few years ago, after I'd switched from a Mac to a PC, a move I now regret. Installing **Norton** was a little like hiring the mafia to protect your shop in the bad old days of the Bronx. The body guard I ended up with made all kinds of demands, turned my house upside down, took over my phone line to get orders from head office and insisted on checking everything I mailed out, despite declaring the contents of my house clean after various exhaustive inspections. I adjusted my working life to accommodate **Norton** – what else could I do? I needed protection and I'd paid good money for it.

When it was time to renew the contract, the mafia made me an offer I couldn't refuse: more protection. I opted for the bundle with the works (**Norton Internet Security**), a 70mb download that took over two hours to trickle down my dial-up line. It popped an icon on my desktop but when I double-clicked on it, nothing happened. The little lump just sat there and sulked, no matter how hard I clicked or how loud I screamed at it.

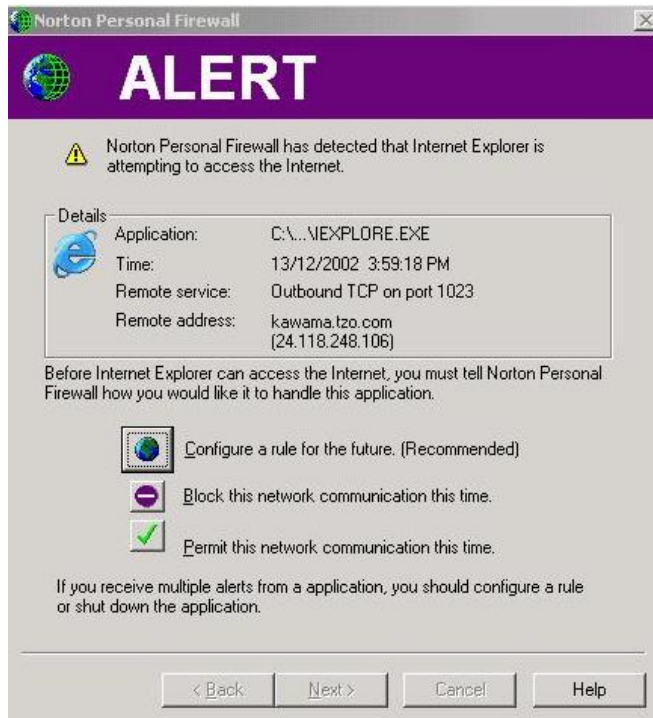
I got on the phone to Symantec Support and, after waiting in the queue for a while, a cheerful fellow in Pakistan told me very politely that something must have gone very, very wrong with the download and that I had to do it again. He wished me better luck this time. I told him it had taken hours and tried to explore other options but he was adamant. He remained impeccably polite even when I ended up yelling at him.

I didn't have time to jump through the hoops again so I called a computer guru a tennis friend recommended. He came the next day, big guy with a baseball cap on his head and an enormous watch on his wrist. He listened to my tale of woes, fiddled with the Norton icon on the desktop, shook his head, opened Windows Explorer, found the installer.exe file and coaxed it into life. The rest was the usual **Norton** merry-go-round of downloading the latest updates, rebooting and the rest. He gave me instructions on how to set the thing up, pocketed his \$75 and left. That was about the same as the cost of the upgrade.

Norton turns Noxious

New **Norton** brought two of his mates, Firewall and Spam Filter, and I found myself running into them at every turn of the dial-up connection. They told me to turn XP's firewall off but when I tried to do that, Windows got really shitty and flashed red alerts and warning signs at me like those on the freeway that say: Go Back, You're Going The Wrong Way, you Moron. I sat there in a cold sweat, my fingers trembling over the mouse. Will I or won't I? **Norton** said there could be a serious conflict – is that what they mean by deadly embrace? Two firewalls colliding in cyberspace?

The new guys **Norton** had brought along weren't very bright. Firewall even stopped apps like Internet Explorer from accessing to the Net.



It took me hours to acquaint Firewall with the facts of life, while his sidekick Spam was busy creating chaos in Outlook. He threw emails from trusted friends into the Spam folder and others into the Junk folder. Real spam still got through, mails offering me cheap Viagra and penis enlargements. How do they know ...?

Spam Filter had to go. What was the point of having him sort my emails when I had to check that he did it right? And he was as slow as an old clerk with eyeshades and sleeve protectors. He kicked up a big fuss but I put my foot down and chucked him out. His boss yelled at me; Firewall didn't seem to care. I tried to get on with my work but, with Norton's heavies in the backseat, my PC had become a slug to drive. **Norton's** big updates also competed Windows doing the same thing whenever I was online. It was like watching two bodybuilders trying to squeeze through the eye of a needle. While they were at it, me and my work didn't get a look in.

The Empire strikes back

They say viruses can bring your PC to a grinding halt but **Norton** did a pretty good job on his own, insisting on scanning every document I opened, even working offline. The mafia was making my life a misery and I resented it. As I thought back to the simple life I once led, my PC started crashing. I'd be typing away and a message would pop up saying: *Word has encountered a problem and needs to close. Sorry about the inconvenience.* Then I started getting regular messages that worried me deeply.



I called my guru and told him what was happening. He said it was a virus. I said it couldn't be, with the mafia in charge of security. He said: it could be spyware or a Trojan – Norton doesn't see some of those guys. I used to think spies worked for the CIA and Trojans were the people of ancient Troy. The guru came and installed **Spybot** on my machine and told me to run a full scan. I did that but the little bot found nothing.

When I phoned my guru with that news he asked how much memory I had in my system. 128mb, I answered. That could be the reason for the crashes, he said: not enough memory for the apps I was running. He offered to install another 128mb and I agreed, thinking it would ease the load.

The extra RAM didn't stop the crashes. I needed a second opinion, so I took the machine to another guru's shop in the next suburb. He listened to my tale of woes, nodded sagely and said: it's a virus. I shook my head and left my PC with him, thinking viruses must be the flavour of the month.

It turned out to be a corroded motherboard, not a virus - the joys of living by the sea. I began to wonder if this whole virus thing was just a ruse to suck us mug punters into

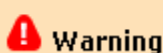
buying more software. I ended up buying more hardware instead – another 256mb of RAM - since the guru recommended it and gave me a good price. By now I knew the game **Norton** and **Microsoft** played, force-feeding my PC like a Strasbourg Goose. When I let off some steam about **Norton**, the guru said I should try Trend Micro's **PC-cillin**.

Rebellion

I checked PC-cillin out on the Net and people seemed to like it. I also found that I wasn't the only one who'd had problems with the boys from **Norton**: the whole world seemed to complain that **Norton** was hard to install, hard to update, high on interference and harder on RAM than a pacman. The only low marks were for support - one disgusted user summed it up this way: 'Is there any way at all to complain to Symantec, on line or by phone?'

Some months later, when the mafia's contract came up for renewal, I refused to sign. I half expected their pals to come knocking on my door but **Norton** HQ just sent me taciturn emails. I bought a copy of **PC-cillin**, but first I had to get rid of the mafia. I consulted the Web for advice – it's a blessing when you need help - and it pointed me to the **Norton Removal Tool** as the best way to get rid of the mob.

You can download it from Symantec's website. It's designed to remove Norton software that misbehaves and requires a fresh install.



Warning

The Norton Removal Tool uninstalls all Norton 2007/2006/2005/2004/2003 products from your computer. Before you continue, make sure that you have the installation CDs or downloaded installation files for any Norton products that you want to reinstall. Also, if you use ACT! or WinFAX, back up those databases and uninstall those products.

I set the smokebomb off and eventually the **Norton** boys departed, spluttering that I would come to regret what I'd done. They left a lot of baggage behind, it turned out, and it took ages to get rid of. They had the last laugh in the end: to this day there's a remnant on my system, an old stain that none of my cleaning tools can shift: a *Symantec Network Drivers Update*.

Peace in our time

PC-cillin was easy to install and behaved like a discreet butler from day one. He had manners and understood his role in life. He also brought a firewall but didn't complain when I turned the Windows firewall back on.

Now I had antivirus software I could live with, and two firewalls that didn't make a fuss. Once a week I'd get the little **SpyBot** to scan for spyware. Peace returned and so did performance: tossing **Norton** out gave my PC a bigger shot in the arm than all those memory upgrades.

I swear I heard my machine breathe a sigh of relief. Now Windows was up and running in 40 seconds from a cold start and every program I launched burst onto the screen like Jackie Chan crashing into a den of bad guys.

There was only one thing that bothered me: why did these security guys dress so badly? The Norton boys in their bile green and yellow outfits were bad enough, but Trendy Micro lowered the bar a few more notches.



It reminds me of an old question: Why do Americans talk so loud? Answer: So you hear them over their clothes. (Apologies to my quiet American friends).

A New Enforcer

Last year I bought a new laptop, a Dell Inspiron 6400 with the latest Intel Core Duo on board and 1gb of RAM. It should've flown like an eagle but this lapdog dragged along like a Dachshund. It took over two minutes for Windows to come up and everything else opened like doors on stiff hinges.

Removing the bloatware Dell had stuffed my new toy with still didn't give the lapdog the legs of an impala. Even my aging desktop PC was faster. The next suspect was **McAfee** (\$50 for 3 years was an offer I couldn't refuse) who was throwing his weight around just like the boys from **Norton** had.

Some checking on Big Mac turned up a review at CNet.com that confirmed my suspicions. It said: 'Norton AntiVirus 2006 showed a definite performance hit during our "real-world" performance tests, but it was less severe than with McAfee.'

That was akin to praising a Hummer for using less fuel than an Abrams tank. Big Mac had to go, but I suspected he wouldn't go without kicking up a stink. I turned to XP's Control Panel and clicked ADD/REMOVE programs, found **McAfee Security Center** and hit REMOVE, ignoring the dire warnings Mac fired at me. When he realized I wasn't paying attention, Mac decided to call home again. When I said No, the bugger promptly froze up the screen.

I turned to Task Manager and terminated every process that started with mc and tried REMOVE again. The screen froze up a second time. I killed off the mc processes once more and dived into the program files, starting at the bottom of **McAfee's** program list and deleting the SpamKiller, then working my way up through Privacy Service, Firewall and VirusScan. They all disappeared but the Security Center, MI6's control room, was still standing tall in the surrounding rubble.

I turned to Google for help and the oracle pointed me to Mac's own website, which provided helpful instructions along these lines: comb through program files and delete the main folder, the agent folder and app folder, then do a final house-to-house hunt for files that end with .adf to flush out the last pockets of resistance. It worked – MI6 was no more.

Exposed

Having paid money for **McAfee**, I didn't feel like shelling out more for security software, so I thought I'd check out some freeware options. I started with **AVG** from Grisoft because I liked the company's slogan: *Tough on Viruses, Easy on Users*. **AVG** was a cinch to set up, had the footprint of a ballerina and the updates tiptoed down the line without elaborate choreography. A tasteful control panel added to its attraction.



AVG doesn't come with a firewall so installed **Comodo's** free one, which I'd read good things about. It had a friendly interface but refused to learn despite assuring me that it was in the mood, sorry - mode. Every day it asked me the same dumb questions about every program that needed to access the internet. I got tired of that so I went looking for a smarter firewall.

Zone Alarm was the popular choice but seemed to cause some people problems. On security forums, many users said **Sygate** made a great firewall, and bemoaned that Symantec had bought the company. That meant updates and support were no longer available but updates aren't a big issue with firewalls since they're not built against specific threats - they're more like a kangaroos fence that keeps out dingos and rabbits as well. And support didn't worry me after getting none from

Symantec.

Sygate's firewall turned out to be a fast learner and made few demands on my laptop or me. In short, it was a model of quiet efficiency.

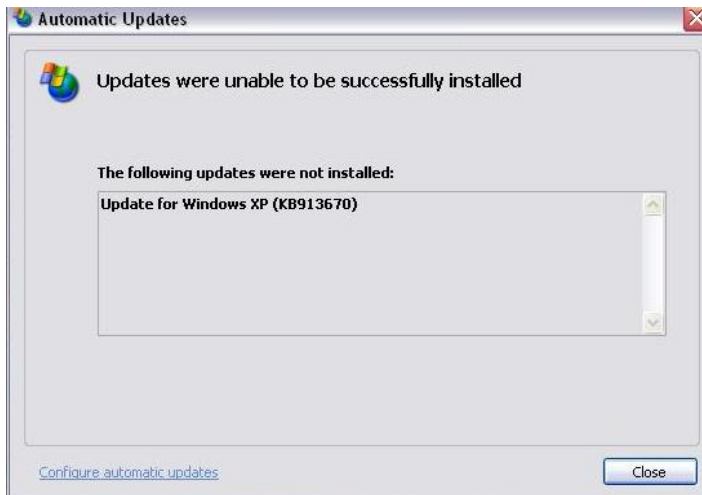
Spy vs Spy

I was still exposed on the spyware flank since **AVG** didn't handle spies and the little **SpyBot** only scanned files, not incoming traffic. **Ewido** anti-spyware was said to be a good choice and had been acquired by Grisoft, so I thought it'd make a good companion to **AVG**. The install and setup were easy enough but the live guard kept crashing for no reason. I downloaded version 4, which came out about that time, but couldn't install it - Windows said the installer was corrupt.

This kind of stuff is sour milk in the latte of a simple user. I have neither time nor skill to make gremlins like these go away, so **Ewido** had to go instead. I'd read good things about **Windows Defender**, a product Microsoft acquired when it bought Giant Software.

Downloading **Defender** turned into an effort akin to crossing Sydney in peak-hour on a pushbike, since I run Mozilla **Firefox** on my laptop and the big M doesn't seem to like the little M much. And big M now goes through this routine where it reaches into bowels of your computer and reads the entrails to make sure they're kosher, and it gives you the third degree if you accessed the download site with **Firefox**.

I still have IE on the laptop but it's broken – how that happened is another story (see [BROWSER BRAWLS PART 2](#)). Once I got hold of **Windows Defender**, it was easy to install and set up, thanks to a simple interface. These spy fighters also have a better dress sense than the AV guys. Less attractive were the constant reminders that I hadn't scanned for spyware in 15 days, even when I'd run a scan the night before. A couple of weeks later, Microsoft sent me a **Defender** update that wouldn't install. Every time I cranked the lapdog up, it would download the same update and give me this message:



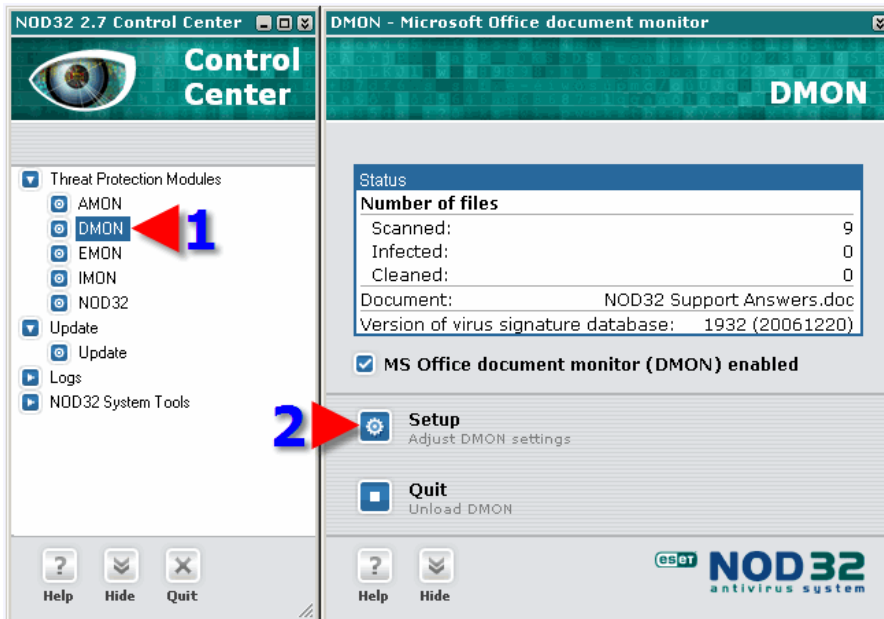
It seems the big M has taken the same high ground as Rolls-Royce whose cars don't break down but merely 'refuse to proceed'. Turning Automatic Updates off didn't solve the problem either: every time I turned the laptop on, it told me that the same tiresome update was ready to install, and I couldn't find a way to turn this moron off. So out the Microsoft Offender went.

End of the Road

The quest of building a good security set-up from freeware had lost its appeal, and the more I read about security, the more I worried. I checked out spysweepers and counterspies, Trojan Hunters and anti-hijack weapons. Fear had me in its grip. In passing I read that **AVG** was pretty basic protection, and even **PC-cillin** wasn't up there with the best. A product I'd never heard of came up a lot on the security forums: **NOD32**.

They said it was as unobtrusive as **AVG** but stronger. It also took care of spyware and that would solve a problem that had defeated and depressed me. The maker's website (<http://www.eset.com>) said **NOD32** hadn't missed a *Virus Bulletin* Award in 8 years, so I didn't hesitate grabbing the 30-day trial on offer.

The first thing that impressed me was the 11mb download – the big boys were heading for 100mb. I was offered a 'typical config' option for the install, which took minutes not hours. After that, all I saw of little Noddy was the icon in XP's notification area and a bubble whenever he'd updated his database of fingerprints. In short, **NOD32** made less fuss than a goldfish in a bowl. The only thing I didn't like about Noddy were his clothes, which were a mess:



Now I noticed that my desktop (which runs the same software except for **PC-cillin** in place of **NOD32**) used 420mb of RAM at idle, whereas my laptop made do with 320mb. I checked the Task Manager and found that **PC-cillin** (2006) had put on a lot of weight with maturity: it chewed up 120mb of memory at runtime, while **NOD32** got by with 20mb.

Trendy Micro was a lot faster than **Norton**, but he wasn't in the same league as Noddy. Of course it's not a fair comparison because **PC-cillin** is the deluxe barbeque with automatic ignition and built-in rotisserie. I don't use its anti-spam and parental control burners so the AV, firewall and anti-spyware are the only things cooking here. **NOD32** takes care of spyware and **Sygate** Personal firewall weighs in at another 14mb, total 34.

I'd found what I was looking for: a great security team with impeccable manners. I began to wonder why people put up with Symantec or McAfee and their bloated wares. I also wondered why I'd never heard of a product that was a fresh breeze on a stifling summer night.

One thing had me intrigued: that strange name, NOD32. I did some checking and found this strange tale on wikipedia.com: 'NOD32 was born in the early 1990s when computer viruses were becoming increasingly prevalent. At the time of its creation, the popular television program Nemocnica na Okraji Mesta, or "Hospital at the Edge of the City" was broadcasting on many European television networks. Early viruses often targeted hard disk boot sectors, located near the edge of the disk. As a pun, the program's creators named their new anti-virus program the "Hospital at the Edge of the Disk", or "Nemocnica na Okraji Disku", giving it the initials NOD.'

When the CPUs of PCs changed from 16 to 32 bits years ago, the 32 was presumably added to NOD. And ESET, I hear you ask? Apparent it's the name of an ancient Egyptian Goddess who had the power to bring the dead back to life.

Now you know.