

# Shoring Up Your Browser

By Bill Hely

As computer programs become more and more complex, the likelihood of errors somewhere in the thousands, even millions, of lines of programming code becomes so high as to be almost guaranteed.

Obviously it is thus essential that there be some way to correct any errors that may be discovered after a program has been released into the market. The method of making such corrections is referred to as “applying patches” or “applying updates”.

What's the difference? Broadly speaking, we can say that patches “fix broken things”, while updates add new functionality. In either case it is usually a simple process of downloading a small corrective file and running it to apply the fix/update to the main program.

These considerations apply to all computer programs, but Web browsers (such as Internet Explorer, Mozilla Firefox, and others) deserve particular attention in this regard, as they are the computer user's interface, as it were, with the potentially dangerous terrain we know as the world wide web.

Unfortunately, if they even think about it at all, millions of browser users the world over take the position *“if it works, why mess with it?”* Their browser gets them around the World Wide Web and that's all they want of it. But they are giving no thought to what is happening behind the scenes.

Some shadowy character, in a country you may never have heard of, may be taking advantage of the program faults you haven't bothered to patch — to his personal benefit and your loss.

Think that's hype?

A great example of the dangers of complacency can be found in a short article from USA Today. The article is actually more to do with firewalls than browsers, but it graphically illustrates the dangers.

I urge you to read this article now, paying particular attention to the fact that the malicious exploits mentioned were all targeted at, and made possible by, known flaws in Internet Explorer. But the really important point is that these were flaws for which a patch was available but had not been applied. Please do read this article before continuing. I have preserved the original article as a PDF file here...

<http://hackersnightmare.com/FreeContent/Other/HoneyPots.pdf>

Patches were freely available to plug the holes that were exploited by the MS Blaster and Sasser worms (as described in the article) before those attacks ever took place. It was the sheer number of unpatched Internet Explorer installations globally that allowed those very costly and near-catastrophic attacks to take place at all.

Instead of going off with a bang that was heard around the world and echoed in all the mainstream media, those attacks should have resulted in nothing more than a fizzle.

And if you think you will be safe by avoiding Internet Explorer and using another browser such as Mozilla Firefox ... THINK AGAIN! My article *“Browser Wars”*, which you will receive later in this series, looks at that situation in detail and dispels a few myths.

## Shoring Up Your Browser

---

Any Internet users who don't patch their Windows Operating System and Web browser regularly are doomed to get infected. If you enjoy the benefits of an always-on broadband connection, then make that a guarantee.

The really insidious thing about infected computers is that often you will not even know that someone or some thing has squirreled away inside your PC. Only if you are very lucky will you be alerted by "strange things" happening or some sort of obvious problem.

These days interlopers are more interested in profit than mayhem, and will try not to alert you to their presence, thus giving them more time to browse, copy and misuse your stored information.

So be aware that an infection can be more akin to a slow cancer—invisible but "deadly" to your safety, your security and possibly to your bank account. Your files can be altered and your precious data browsed by strangers without your knowledge.

For the private individual on a home PC it is an unnecessary risk, and far from "relatively harmless". In my book *The Hacker's Nightmare*™ I include a contribution from a retired FBI Special Agent who relates just how little information is needed to steal someone's identity. There is enough such information on just about any home PC.

For a business it's just plain crazy to ignore these threats, and possibly even criminally negligent. In many jurisdictions the holder of data about others is legally responsible for its safety. If you store information about customers, suppliers, employees, patients, etc. then data carelessness could leave you exposed to legal and financial penalties.

Exacerbating the danger further is the fact that often management is legally responsible for the actions of employees, so the onus is on business operators to take all necessary steps to ensure data security. Oh, and claiming that you are only a small business, a sole operator or just work from home is unlikely to elicit much sympathy when the letter of the law is applied.

By itself, regularly patching and updating your browser, operating system and other major software applications will not give you 100% protection. But it is a very necessary component of a sensible defense-in-depth strategy.

With specific regard to the browser, you'll find numerous articles on the web exhorting you to make all sorts of modifications to your browser's configuration settings to tighten its security. But if you have ever looked into the configuration bowels of any mainstream browser you'll be aware of just how many settings there are to "play with".

Have a look through the various Tabs and options with which you are presented (just look, don't touch!). There are options and custom settings for this and that, zones, advanced privacy settings and so on. An inappropriate selection or a clash of options can make things worse instead of better, so don't experiment!

Do you really want to get involved with all that complexity? It's much better and much safer all round to use sensible defense-in-depth strategies to protect the browser and much else besides.

Exactly how you should implement regular, scheduled patching and updating depends on a number of variables, including the specific version of Windows and the make/version of the Web browser you use.

In all fairness I should say that you can find all the necessary information and instructions at the Microsoft website (for Windows and Internet Explorer), at the home

## Shoring Up Your Browser

---

sites of other browsers, and in the Help files that accompany Windows and your browser program. But these documents can be difficult to find and difficult to understand for the technically uninitiated.

A much better option would be to consult the chapters on "Patches, Updates and Service Packs" and "Microsoft's Patch & Update Services" from *The Hacker's Nightmare*<sup>™</sup>. There you will find all the details and instructions in one place, presented in a logical, jargon-free and easy to follow manner, with the added bonus of having ready access to all the strategies and tutorials in the rest of the book to really implement solid defense-in-depth protection for your PC.

Yes, that's a shameless plug, but I honestly know of no other resource where you can get all the information you need in one place, and presented in a manner understandable to people without technical computer experience. To fill such a void was the reason I was compelled to write *The Hacker's Nightmare*<sup>™</sup> in the first place.

Anyway, however you go about it, there's one thing you must be clearly aware of...

Sooner or later complacency will cost you—perhaps very dearly. Keeping your Operating System and your Web browser patched right up-to-date is NOT optional.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*<sup>™</sup> --- <http://www.HackersNightmare.com>

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation  
— and especially testimonials —  
are most welcome.