

Online Security Davey Winder

# Little green idol

IT'S ALL A MATTER OF TRUST, AS DAVEY WINDER HITS WARP SPEED IN HIS MONTHLY LOOK AT THE WORLD OF IT SECURITY

A press release from VeriSign informed me that just over half the people who access the internet do so using an EV SSL-enabled web browser client, most of course being Internet Explorer 7 users (47.1%) with 5.7% using Firefox 3. Opera 9 also comes EV SLL-enabled, although I doubt that will improve its tiny share. A statistic not included in the VeriSign release – because I just made it up – is that 50% or more readers of this column have absolutely no idea what EV SSL-enabled actually means, and are fumbling for Google or Wikipedia right now.

Well, the EV bit stands for Extended Validation, while SSL still stands for Secure Sockets Layer. EV SSL is needed, so the argument goes, because there are no generally accepted standards for organisational data verification via certificates. Some site owners employ a graphic of the SSL padlock on their pages, which has helped confuse the real significance of the padlock icon. Throw in the obfuscation of URLs due to dynamically-generated content, which results in ever more complex and obscure page addresses, and it's little wonder that end users get their knickers in a twist over security and trust issues.

What was needed was some accepted method of providing clear and obvious information about the trustworthiness of the site you're doing business with, and so a bunch of browser developers and certification authorities got together to specify EV SSL. This is an open standard, established by the CA/Browser Forum (see [www.cabforum.org/certificates.html](http://www.cabforum.org/certificates.html)) and intended to provide a measure, or rather an improved measure, of the authenticity of the digital certificates requested in order to secure a web-based transaction. That's how the CA/Browser Forum describes the function of EV SSL certificates, but you might prefer to think of them as those things that turn your browser address bar green to show that you've arrived at the site you were intending to visit, and not at some cloned mirror-site operated by fraudsters. Or at least that's the idea.

I have a problem accepting VeriSign's 50% milestone for EV SSL certificates, though. For a start, that statistic refers to potential rather than actuality: it means that more than 50% of browsers by *market share* are in principle capable of distinguishing between ordinary SSL certificates and Extended



Go green for trust validation with EV SSL, or send a box of poo to your customers – your choice!



## DAVEY WINDER

Award-winning journalist and small-business consultant specialising in privacy, security and usability issues. Contact [davey@happygeek.com](mailto:davey@happygeek.com) or join him in the *PC Pro* conference on Cix.

## SPAM STATS

Ever bought anything as a result of some obnoxious bit of spam dumping itself in your email folder? No, me neither. However, according to a recent Marshal poll it seems that 29% of folk have done just that! The last similar poll, way back in 2004, suggested that 20% would do so. Which either means more of us are becoming morons, or there are simply more of us online. I suspect the latter. Slightly less surprising was the revelation that 85% of all email by volume is spam. Mind you, with the FBI reporting that it costs around a fiver to order a million spam messages sent via a spambot, I'm amazed that figure isn't even higher.

Validation versions. But according to VeriSign itself only around "6,000 websites already rely on VeriSign EV SSL certificates", so you can probably guess the big spanner-shaped question that I'm about to throw into the works – if there are millions of websites out there but only 6,000 of them are using EV SLL, how exactly does this make us feel better protected from those who'd steal our data?

The situation isn't quite as dire for VeriSign as it initially appears, because first you have to strip away from that the millions of websites that have absolutely no transactional component at all. Think about it, how many business-orientated sites that require you to share personally identifiable information (PII) – be it in the form of a credit card transaction or a membership login – do you visit compared with those myriad sites that you just skip through without having to reveal any of your PII?

## Box of poo

Tim Callan, vice president of SSL marketing at the VeriSign SSL business unit, says on his blog ([https://blogs.verisign.com/ssl-blog/2008/08/over\\_50\\_of\\_client\\_systems\\_are.php](https://blogs.verisign.com/ssl-blog/2008/08/over_50_of_client_systems_are.php)):

"a consumer doesn't need protection from phishing attacks when visiting your personal blog or *Star Wars* fan site, or even your company's brochureware site. It's only where the actual commerce takes place." And, of course, he has a point: if you concentrate on the transactional business parts of the web, rather than trying to cover everything, then EV SSL makes much more sense, or at least you'd think so. However, Callan reports that one of the arguments against adoption he hears from some businesses evaluating EV SSL is that there's no benefit for them until their main competitor – business B – also starts using it.

This is what Callan calls an "evaluation fallacy", and what I call a bloody big business blunder. Waiting for your competitors to implement a security solution before you do is probably the most ridiculous argument I've ever heard. As Callan goes on to say: "If your competitor started sending big boxes of poo to its frequent customers, would you run out and start sending poo to your own customers as well?" I'm not sure I'd have chosen this box of poo analogy myself, but it does strongly make the point that anything that helps validate the trustworthiness of a transactional website has got to be good news. When it comes wrapped up in something as obvious as a big green address bar that news is easy enough to understand, and that should be as true for the transactional business at one end of the line as it is for the consumer at the other end.

## WARP speed for security

I first heard of a WARP back in 2005 – and even then it turns out it had actually been around for a couple of years – yet rather

# I've heard it said that if a WARP community is too savvy, it will most likely fail – the reverse is just as true

surprisingly at least half the information security professionals I talk to have never heard of it, and when it comes to anyone outside the security business that figure rises to 99.9%. So assuming you're not in that extremely clued up 0.1% minority, I'll explain exactly what a WARP is and why the heck you should care about it. A Warning, Advice and Reporting Point is quite simply a small and focused security community for sharing advice on threats, exploits and solutions, and simplicity is at the very heart of the WARP concept.

The brainchild of the Centre for the Protection of the National Infrastructure ([www.cpni.gov.uk](http://www.cpni.gov.uk)) and originally developed to help protect national communications systems from tampering, WARPs have remained small while expanding to fulfil a broader security brief. A WARP will be no larger than 100 members at the most, and more typically between 20 and 50 in order to ensure the community focus is retained. What you end up with are numerous small and discrete security communities consisting of a select and secure membership, rather than a handful of huge, impersonal and unfocused security resources that end up being too diluted to be anything more than generic and broad interest.

## Neighbourhood Watch for the IT crowd

WARPs function by having a single security savvy operator at the helm that steers a course through the specific security information needs of a highly-targeted, but not so savvy, community of members. The information is propagated by way of websites, email, SMS and telephone messages, which the community supplements by encouraging members to become involved in forum-based discussions as well. As a small, local, targeted and not-for-profit community-driven resource, a WARP is pretty much the online equivalent of a Neighbourhood Watch scheme.

It's vital, in my never very humble opinion, to understand the importance of the fact that the community is largely less savvy regarding IT security than the operator, when it comes to the success of a WARP. It isn't as if the information that's being distributed can't be found elsewhere – it's all out there online for those who know where to look for it. Indeed, I've heard it said that if a WARP community is too savvy it'll most likely fail, and the reverse is just as true. Keeping on top of security



CPNI has been instrumental in getting WARP out to the community, albeit very slowly.

consists of three core services: Filtered Warning, Advice Brokering and Trusted Sharing. I think it's worth looking at each of these in a little more detail to grasp the mechanics of a WARP, and get to grips with the notion of whether one could be of use for your particular industry application. Filtered Warnings are just what they say, a security-related warnings and advisories feed tailored to the needs of not only the particular community, but to individual members within it. Collecting information from many different sources, the WARP operator can match it against a list of relevant subjects, as well as filtering by urgency, before distributing it to only those members of the community for whose specified interest it's a good match. Think of this as fulfilling the Warning part of WARP.

Next comes the Advice part, and the Advice Brokering service is really pretty self-explanatory: it provides members with a route for establishing dialogues with each other to discuss best security practices, most often through some kind of online forum. Finally, there's the Trusted Sharing service, which brings anonymity where needed into a trusted environment to encourage incident reporting and to exploit sharing by the community. This is vital to the success of any WARP, as without trust there will be no disclosures, and without disclosures of actual attacks the WARP is nothing more than a security newsfeed.

## Live long, and prosper

The CPNI's WARP website ([www.warp.gov.uk/Index/indexwarpbenefits.htm](http://www.warp.gov.uk/Index/indexwarpbenefits.htm)) contains an interesting example of how a WARP can actually make a difference, in this case for members of a local authority who were using the same housing benefit software application. The WARP was able to immediately inform members after one of them installed a Microsoft security patch that made the software unusable, resulting in delays to housing benefit payments and all the disruption that goes along with that. By dispersing this highly focused information quickly to just those people who needed to know it, along with the solution, an early warning was established that prevented others from suffering the same problem and potentially wasting time and money as a result.

It's taken plenty of time for the concept to catch on outside local government and public services sectors and, in fact, still remains something of a well-hidden secret. The Law Society has its own WARP, the Radio Amateurs' Emergency Network has



WARP communities let you set your security phasers to stun.

a WARP and there's even a specialised WARP for journalists, but for this concept to really make sufficient impact it needs to spread much further outside of the local government and professional arenas. The CPNI devotes a whole area of its WARP website to building one of your own, and this includes a WARP Toolbox complete with documentation, tutorials and software to help get you on your way. I'm feeling a *Star Trek* moment coming on, and no it isn't the obvious one of "Warp Speed Mr Sulu" either. I was thinking more along the lines that perhaps now is the time to start investigating a WARP more closely if you want your data-processing systems to live long, and prosper.

## Houston, we have a problem

Sticking with the space exploration theme for a moment, NASA has officially confirmed two fascinating facts for space monkeys everywhere, the first being that at least one laptop aboard the International Space Station has been infected with a worm, and the second that it uses Norton AntiVirus to scan computers while in space. You kind of expect that IT kit that's taken into an environment such as outer space, or more to the point on board such a hard-to-reach location as the International Space Station, would undergo some pretty thorough quarantining before it leaves Planet Earth. At least that's what I'd have assumed, but it looks likely that the source of infection on the ISS could well turn out to be a USB stick or digital camera flash card used by one of the astronauts.

Luckily, no harm was done on this occasion since the worm involved was only W32.Gammima.AG, which exists solely to harvest data from players of a specific online game in China and to transmit it to a remote server. Or at least, that's the spin that's being put on it, but "rhubarb" say I. As with most such exploits, the harm is done less by the payload of the infection, and more by the lapses that allowed it to be installed in the first place. This is especially true in a hi-tech business such as this one with an environment that's so costly both in terms of money and human life should something go pear-shaped as a result of systems failure. The fact that this worm has been a known quantity for at least a year here on Earth would suggest that the device on which it hitched its ride into space wasn't subjected to any antivirus scan before blast off. Since NASA has confirmed the antivirus software it uses on the ISS is Norton, when I next meet up with Symantec I'll be sure to ask how much a licence for Norton AntiVirus (Space Edition) costs.



In space, no-one can hear you scream: "Who used the infected USB stick?"

**Applications unlike anything you've seen on a phone before.**

Applications designed for iPhone are setting a new bar for amazing. That's because they leverage the groundbreaking technology in iPhone — like the Multi-Touch interface, the accelerometer, GPS, real-time 3D graphics, and 3D positional audio. Just tap into the App Store and choose from over 3000 applications ready to download now. Browse the App Store in iTunes.



**eBay auctions move faster with Multi-Touch.**  
Tap, flick and pinch to browse eBay auctions, photos and place bids on the go. And respond to buyers fast with built-in email.



**Super Monkey Ball rolls with the accelerometer.**  
Finally, a mobile game genre that responds to your movements. iPhone gives you tap-and-tilt games like Super Monkey Ball.



**Leap finds friends with Maps.**  
There's nothing like a social network on an iPhone. Applications such as Leap use location feeds to help you find friends on the go.

↑ Apple can engage a "kill switch" to remotely disable the iPhone apps you've bought.

## Next time I meet Symantec I'll be sure to ask how much a licence for Norton AntiVirus (Space Edition) costs

### And finally...

I know that this is *PC Pro* magazine with its emphasis on the PC, but it's impossible to ignore Apple products these days, and that's true with regards to the iPhone. At the risk of treading on the toes of Mr Ockenden of the Mobile & Wireless column, I just have to mention a little bit of security-related controversy that's been stirred up as far as iPhone 3G users are concerned.

It would appear that the much rumoured "kill switch" built into the iPhone firmware is no myth: Apple has confirmed it exists. But what has this got to do with security? Well the reason given by the company for this hidden code — which apparently would enable Apple to remotely disable any application — is an interesting one. It's there for your own good, the company says. Playing the security card, Apple CEO Steve Jobs is reported in one interview with the *Wall Street Journal* as saying that the kill switch is there just in case some malicious software were to be inadvertently distributed through the iTunes App Store.

This excuse sucks elephants through a straw for two very good reasons: one, it makes me think the "all Apple approved" App Store security checks aren't as thorough as they should be; and two, it makes me wonder if Apple is turning into the Nanny State of the IT world. If I've bought and paid for an application and it then turns out to be "malicious", by whatever definition is deemed to be accurate at the time, then I'd certainly appreciate being informed of that fact so that I can make an informed decision about the likely impact upon my hardware, software and data, rather than having Apple just turn it off remotely for me. That way, I'm left in control of the security of my own device.

Try to imagine the kind of media firestorm that would greet Microsoft if it were discovered that there was a backdoor in the Vista code that allows some geek in Seattle to remotely deactivate the software that you've paid for because it might look a bit iffy in Redmond. ■