



## ESET SHORT WHITES

White Papers that get to the point

# Internet Security - Code of Conduct

## The Internet – a Boon to Business, a Haven for Hackers

The treats lurking online are many and varied, and growing in number and sophistication. However, most security breaches aren't caused by viruses or hackers but by ignorant users. Last year, Revenue & Customs in the UK lost two disks with personal data on 25 million British citizens. Also in the UK, a public servant mailed a copy of the whole national child database to the National Audit Office in London.

Carelessness is not limited to government organisations. Last year, spammers hijacked computers at Pfizer and used them to send junk e-mails advertising the company's product Viagra. According to one survey, it's corporate PC users who are the weakest link in the security chain<sup>1</sup>. In this paper, we explore simple, low-cost means businesses can use to raise their security status.

## Ignorance is the weakest Defence

Most human security failures have no malicious intent. Documents are left on a web server by accident and become accessible to search engines; back-up disks are left in a car that is stolen; someone is tricked into revealing a password that allows an outsider access to company confidential data. Some surveys have found that accidental human security breaches make up 80% of the total<sup>2</sup>.

Most attacks are aimed at the 'endpoints', the PCs and laptops that connect users to the internet. Phishers and Scammers have worked out where the weakest link is too – that's why they're increasingly aiming their attacks at users.

## An ounce of prevention is worth a tonne of cure

Every business has policies, safety checks and fire drills. How many have a code of conduct for the internet? How many businesses ensure that the code is known and adhered to? How many wait for a major breach before conducting a security audit?

According to some surveys<sup>3</sup>, only 30 – 40% of organisations offer internet security training for their staff. Mike Maddison, Deloitte UK's head of security and privacy services, said in a recent interview: "You can have the best technical systems in place but they are unlikely to operate effectively unless you educate people on their obligations and how to fulfill them<sup>4</sup>."

## Code of Conduct

It makes enormous sense to train staff on the sensible, responsible use of the internet. Training is a small investment that can turn the weakest link in a business into its greatest security asset. Training causes a mind shift that can make users see the business as a plane and themselves as the crew. The crew needs to know the dangers, the preventive measures and the survival drill.

Of course, it's not just staff – conduct is a culture that has to be embraced and lived by senior and middle managers first and foremost. And like all company culture, the code of conduct needs to be

1. <http://www.itnews.com.au/News/NewsStory.aspx?story=55531>
2. <http://blogs.zdnet.com/projectfailures/?p=480>
3. <http://software.silicon.com/security/0,39024655,39158023,00.htm>
4. <http://news.zdnet.co.uk/security/0,1000000189,39289394,00.htm>



reinforced at regular intervals. If the resources aren't available in-house, there are IT consultants who specialize in security training.

### Secure your systems

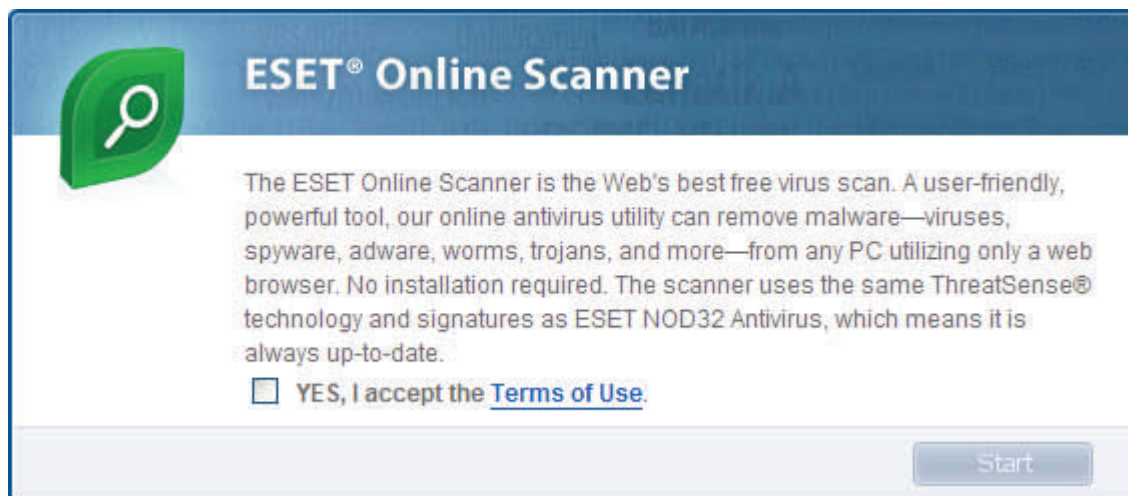
Even with management and staff trained, effective endpoint security systems remain essential. With staff trained in their proper use, they become more effective. Here as well, a few additional precautions can make a big difference. Strong user passwords are a good start<sup>5</sup>.

It also pays to ensure that all PCs, laptops and servers have the latest software patches applied – many of them plug gaps that can be exploited by malware. *Secunia* provides a free 'software inspector', a program that highlights and updates PC software<sup>6</sup>.

Web browsers on PCs and laptops should be secured with JavaScript and have phishing protection enabled<sup>7</sup>. A small utility like McAfee's Site Advisor, which sits in the internet browser and flags suspect internet sites for users, is a valuable early warning system.

### Independent checks

Don't wait for a major security breach before carrying out a security audit – it's more valuable as a preventive measure. It also makes good sense not to rely on one single security vendor. Systems vary in their ability to detect certain types of malware, therefore it is good practice to check the most exposed PCs and laptops (those used by mobile workers) with an online scanner from a different vendor from time to time.



ESET's Online Scanner detects known and unknown forms of malware, including viruses, worms, Trojans, phishing attempts and spyware. EOS scans inside archive files, runtime packed executables and email messages. Unlike most other scanners, it also removes the malware for free. It's a small 15mb download and easy to use.

### Additional Resources

<http://www.security.iaa.net.au/>

<http://www.e-businessguide.gov.au/protecting/tips>

[http://www.dbcde.gov.au/\\_data/assets/pdf\\_file/0007/18952/ISEbooklet\\_06.pdf](http://www.dbcde.gov.au/_data/assets/pdf_file/0007/18952/ISEbooklet_06.pdf)

5. <http://www.securitystats.com/tools/password.php>

6. [http://secunia.com/software\\_inspector/](http://secunia.com/software_inspector/)

7. [http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45\\_qci1241319,00.html](http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45_qci1241319,00.html)