Small Business Security Guides

Five steps to securing your business website and its content

AVG AT WORK

Five steps to securing your business website and its content

If you're running an online business, then you have a whole lot more threats to your business operation and reputation. And the more successful you are, the more likely it is that the bad guys will target your web site.

The bad guys will try to hack your web site and use it to phish people off to poisoned web pages, or even hack your web site and put download exploits onto your web pages. They succeed in doing this to hundreds of thousands of web pages a day.

You don't want your web site being hacked in this way because all of the money you've invested in search engine optimisation (SEO), search engine marketing (SEM), brand reputation and customer loyalty can disappear overnight.

The bad guys will also try to exploit web site software errors to access customer information in the databases the web site utilises, or to put through fraudulent transactions.

At AVG we have just launched an online information portal that will help you establish whether your web site is safe and secure or not. **AVG Threat Labs** gives you a site report for the real-time status of your website, whether it has been compromised, if so by what and where the malicious code has come from.

If you're worried about your web site safety then check it out on Threat Labs.

If it has been compromised you can take action and soon as the security holes have been patched up, Threat Labs will list the site as safe again. For more on Threat Labs for web site owners then check out this **Threat Labs FAQ**.

Business basics:
Five steps to making a business website and its content secure

1. Maybe you're developing your own online solutions. More likely you're using an external web applications provider, or just common open source solutions like WordPress, phpBB, ZenCart etc. Whichever it is, you need to ensure that those responsible for the web site code, installation and ongoing management are fully aware of the **2010 CWE/SANS Top 25 Most Dangerous Software Errors list**.

   They need to understand the problems, put in place the mitigations to address them, and keep checking that they're working.Thankfully, the nine 'Monster Mitigations' given in the document above will be effective in eliminating or reducing the severity of the Top 25 problems, plus address many weaknesses that are not even in the list.

2. Make sure the servers hosting your web site are kept up-to-date with the latest software updates and Internet security software. Make sure any third-party or open source web applications are also kept up-to-date. Apply any security patches as soon as they become available.

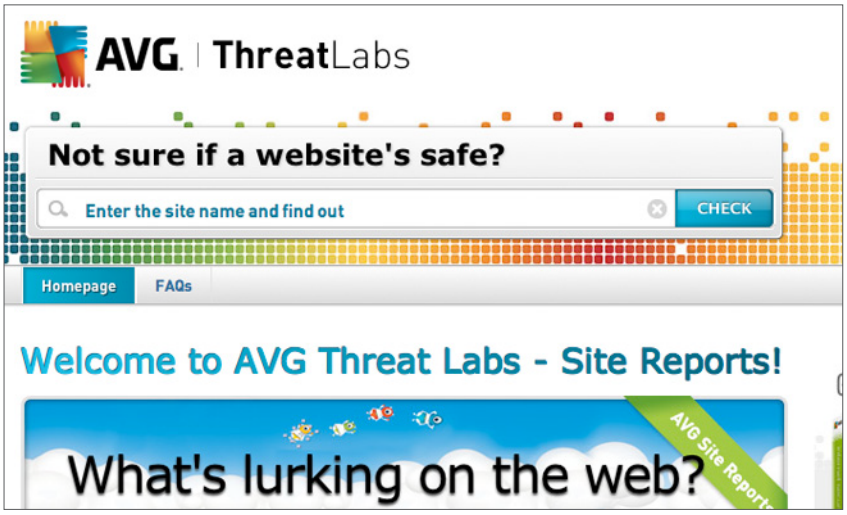
3. Now do the same to your own business network and the PCs on it. For some great advice on how to get this right, check out "**35 Strategies to Mitigate Targeted Cyber Intrusions**" from the Australian government's Defence Signals Directorate.

4. Make sure the passwords used to access your web hosting accounts and the administration areas of your web application software are changed on a regular basis and that they are "heavy" passwords. See "**The Guide to Password Best Practice**".

5. Ensure you are familiar with all of the relevant standards, compliance requirements and legal implications including your government's privacy and data protection requirements. These may vary across territories and countries. If you accept, store or transmit credit or debit card data then you need to be PCI compliant – checkout the **PCI's website** for more information.
   All of this isn't a once off thing. It requires a lot of vigilance and there are some other common security flaws that businesses operating online should be aware of.

   You need to be on the lookout for fraudulent transactions. Treat any order with credit card payment requiring you to ship goods overseas with great suspicion. Even go so far as not allowing online credit card payments for overseas shipments

   Make them pay via PayPal, bank transfer or other more secure means. You may even consider blocking all orders from high risk countries including developing nations like Indonesia, Malaysia, Benin, Nigeria, Pakistan, Israel, Egypt, India, China and some Eastern European countries. For more on this you can check out "**31 Ways to Minimise Credit Card Fraud**".



AVG SMB group at:
bit.ly/AVGSMB

Become an AVG Fan at:
facebook.com/avgfree

Read our blogs at:
blogs.avg.com

Follow us at:
twitter.com/
officialAVGnews

Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

AVG AT WORK