

AVG Security Guide

Your Online
Security –
11 Q&As in
2011

Brought to you by AVG Australia and New Zealand

AVG Security Guide: Your Online Security – 11 Q&As in 2011

2010 was another big year for security threats. Across the globe AVG saw a huge increase in the amount of malware affecting both users at home and at work. Whilst the security industry has been doing a lot to combat this, online threats continue to grow as the cyber criminals realise that it's easy to target consumers and small businesses.

Identity theft is on the rise; cyber criminals find it very easy to obtain bits of our identity to use or sell it. The rise of Smartphones, and their resulting mobility issues, also brings even greater threats.

Similarly, businesses are moving to use 'the cloud' more and more, but may not be investing in the security needed to combat the threats that these new web technologies bring.

So, how will we fare against the bad guys in 2011? Well, if we continue to be as careless as some of us have been in the past, the bad guys will still reign supreme.

Here are 11 questions and answers designed to help better protect yourself and/or your business in 2011 and beyond.



1

What are some of the main misconceptions people have around Internet security?



People are still inclined to think that security threats are the work of hackers trying to make a name for themselves. But today it's almost entirely about organised cyber criminals doing this on a HUGE scale and making billions of dollars. They want to scam money out of you, get enough of your identity details to scam money out someone else, and/or make your PC part of their botnet (i.e. steal your computer resources and Internet bandwidth).

Installing basic security software will protect you from basic threats. But the more you bank, shop, work and game online, the more you need the additional protection layers of a good Internet security suite like [AVG Internet Security](#).

However even with the best security software installed on all of the devices you use, you still need to educate yourself, your family, friends and work colleagues about the risks.

We still get those Nigerian scam emails because so many people, you think, would know better than to fall victim to them. People infected by malware often explain that they had security software installed and it warned them, but they wanted to see what would happen anyway!

2 What are some of the current emerging security threats in 2011?



It's not so much that the threats change, it's more that the cyber criminals change the ways they try to get to us.

In 2010, we saw a huge increase in the frequency and intensity of utility application software attacks (e.g. Adobe Reader, Flash, iTunes, Quicktime etc.) and various Facebook application attacks. The bad guys realised that most people had these applications and that there were plenty of security holes to exploit.

Unfortunately the first quarter of 2011, revealed an explosive increase in the overall number of global attacks.

The most notable developments were:

- Major growth in malicious campaigns which exploited the viral nature of Facebook users which has increased threefold in the last 12 months.
- An increase in risk for Smartphone users, as cyber criminals extend the battlefield to mobile devices.

The second quarter of 2011 has seen these trends continue. However, the cyber criminals are now also using rogue anti-virus applications to target Apple Mac users.

These developments demonstrate an increased professionalism in the structure and operations of global organised cyber crime.

Identity theft continues to rise because of how easily cyber thieves can steal it, sell it, and get away with using it. Especially now that so many people are careless about the information they share and who they share it with via social networks.

Smartphones are taking over many of the functions of a computer, yet few users have installed even basic mobile security. Thus we see the bad guys targeting this fast growing and vulnerable platform.

Meanwhile in both the consumer and business worlds, we're relying more on web-based technologies but aren't investing in stronger security defences.

Staying safe when using Facebook

- Check your privacy settings - make sure your privacy settings aren't sharing information that you want to keep private.
- Pay attention to whom you share your information with.
- Protect your mobile device to the same level as your PC or laptop.
- Use [AVG Social Networking Protection](#): links that are exchanged within Facebook are automatically checked in real time so that you, your friends, your company and your employees remain safe. AVG Social Networking Protection is activated automatically as soon as [AVG Internet Security](#) is installed.

3 How has social media affected computer security?



Social networking sites are a cyber criminal's playground. People engaging in social networking with people they do know will inevitably be followed by, and receive friend requests from, people they don't know. Is it really an 18-year-old girl from Perth? Don't leave yourself open to attack by going onto social networks unprotected — and always log out of sites as soon as you're done. AVG research shows the top 50 social networking sites have 20,000 compromised pages containing web threats or illegal content that could harm your computer or lead to their personal data. More than half of those pages were on Facebook, and one-third on YouTube.

Notably, in the first quarter of 2011 AVG Technologies [AVG Community Powered Threat Report - Q1 2011](#) identified a threefold increase in the number of malicious campaigns which exploit the viral nature of Facebook users.

As the Internet's second most visited website, Facebook is an obvious target for cyber criminals. Click-jacking scams have increased in frequency from once a week to once every other day, and defence from these scams requires constant vigilance. Profiles without suitable privacy settings are liable to be exploited by marketers or cyber criminals and could be used for identity fraud.

Protecting your Smartphone

- Treat your Android phone like a PC. It is unsecured unless you take steps to protect it.
- When downloading applications, make sure you get them from a trustworthy source - if you're unsure about the validity of an application, don't install it.
- Protect your Android Smartphone with security software such as [AVG Mobilation for Android](#).

4 Are Smartphones the new point of entry for hackers?



Smartphone users are constantly connected and substantially less protected than when using a personal computer. They tend to shrug off mobile security solutions and carelessly broadcast financial, account and other personal data, such as their exact location, while on the go.

Smartphones and Tablet computers are becoming a more important target for cyber criminals.

Mobile devices are constantly connected and substantially less protected than a personal computer. Users tend to shrug off mobile security solutions and carelessly broadcast financial, account and other personal data. That's why it's important to protect your Smartphones with security software.

[AVG Technologies' AVG Community Powered Threat Report - Q1 2011](#) demonstrates the first quarter of 2011 saw a notable increase in risk for Smartphone users, and the Android platform in particular. AVG blocked an average of 100,000 spam and phishing text messages per day.

The open source nature of the Android operating system, as well as the open-garden approach to allowing users to install software on their mobile devices, opens the door for cyber criminals to write malicious code.

A recent [survey](#) carried out by AVG Technologies and The Ponemon Institute found that a third of Smartphone owners are unaware of the increasing risks posed by malicious software, with only 29% having considered protecting their device - and their data with a free or paid anti-virus program.

Security that is specific to the mobile environment should be considered. Cloud-based protection offloads the process from the mobile device which can then be kept safe without draining resources.

In keeping with AVG's belief that everyone has the right to free anti-virus protection, [AVG Mobilation for Android](#) is helping prevent users from downloading over 10,000 infected applications a day.

5 When it comes to Internet security, are all browsers created equal?

All browsers and all operating system platforms are pretty much as strong and as weak as the others when it comes to security. But cyber criminals are simple creatures, really. They will go where the money is and follow the path of least resistance to get there. Thus if the majority of people are using Microsoft Internet Explorer®, then that's the browser the bad guys will target the most.

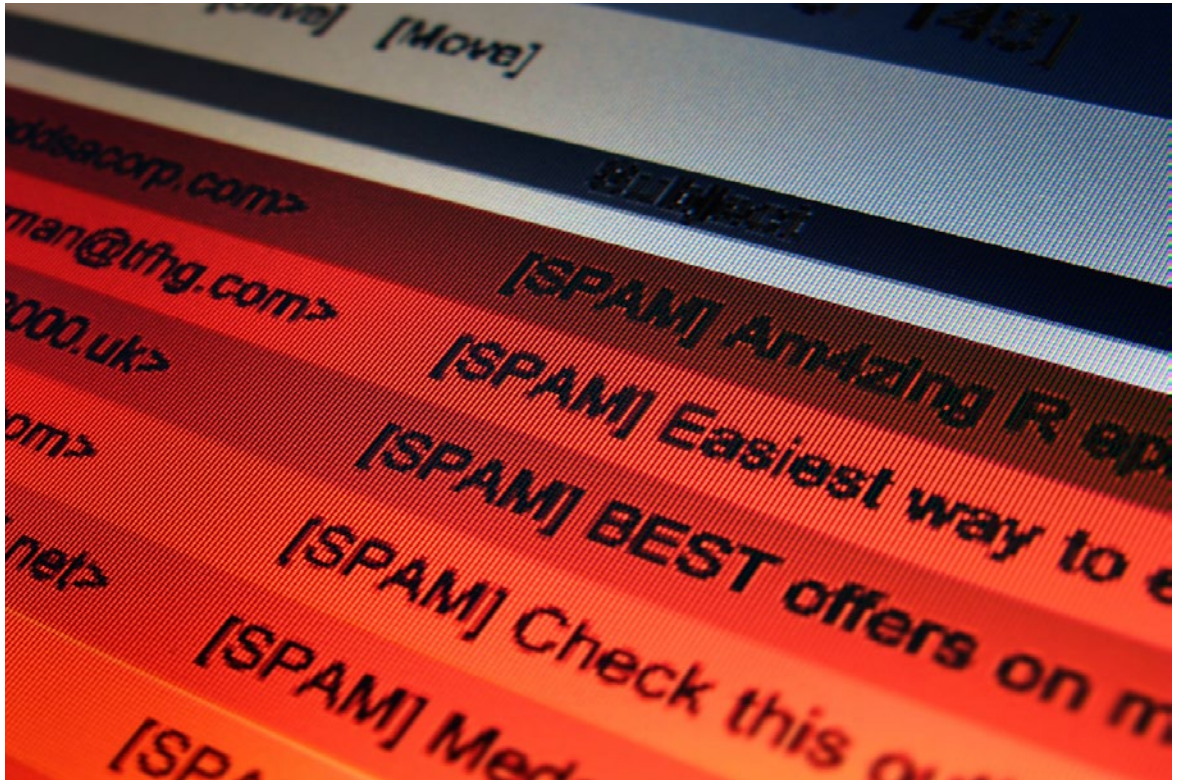
While the bad guys will target security flaws in most of the major browsers as they become aware of them, they more often target security lapses in operating systems and other utility software like Adobe Acrobat Reader®, Adobe Flash®, Apple iTunes, etc.

This is why it's essential that you keep your security software, your operating system, your software utility and applications up-to-date. Make it easy on yourself and use the automatic update features now commonly available to achieve this.



6

How has spam changed - what do people need to beware of in 2011?



Certainly email based spam has changed. For a start it's now a huge percentage of all email delivered over the Internet, which is why we all need good anti-spam protection.

There was a time when the bulk of spam email had files attached that contained various forms of malware. This attack vector is now less used

by the cyber criminals, as even basic email security software protects people from it. Today the email is more likely to have a link off to a web page hosting malware, or off to a phishing web page where you'll be asked to provide identity and/or financial account details. Often tiny URLs are used to make it hard for you to identify the real URL of the page you'll be taken to.

There is also a new form of spam — search spam. The bad guys now manipulate search results via social networking websites and other means to pollute search results with malicious links.

7 What threats exist from legitimate websites that have been corrupted? How can people spot these threats?

There are two main ways the cyber criminals use legitimate websites. Firstly, they hack into the website itself through security holes and often embed links to malware or phishing web pages into the website's legitimate web pages.

Secondly, they post content onto the blogs or forums of legitimate websites, or even put adverts on these websites. Again this content will have links off to malware or phishing web pages.

Having good [Internet Security](#) software in place will help you to spot these threats. Web protection software like [AVG LinkScanner](#), (included in AVG security products and available free for Windows and [Mac PCs](#)), will block these threats.

Use AVG ThreatLabs if you are unsure of a URL, tiny or shortened URL, or website in general. AVG ThreatLabs is a free tool that tests any website, checks its reputation and provides you with a 'safety' rating. Bookmark AVG ThreatLabs at www.avgthreatlabs.com/sitereports/

AVG | ThreatLabs

Enter a website name and get its safety rating

Site Reports | Web Threats | Downloads | Free Tools | About Threat Labs

30-day site report for:
facebook.com

Surf with caution

Sometimes Facebook applications or links can be unsafe. We recommend that you surf carefully with AVG to help you stay protected.
(updated May 08, 2011 23:59 GMT)

Click to download a free trial of AVG Internet Security 2011 and surf facebook.com safely.

Compromised Web Pages **235**
in the last 30 days

Threat Types Found **5**
in the last 30 days

Visit the site

Is your PC slow? Increase the speed of your PC with AVG PC Tune Up. Click to download a free trial.

TELL YOUR NETWORK

The results provided by this website are provided on an "as is" basis with no warranty as to accuracy or completeness. You acknowledge by using this website that you have read and agree to the terms and conditions available [here](#)

Steps to password perfection

Follow these steps to create secure passwords:

1. Think illogically; computers rely on logic to operate.
2. Don't use cardinal numbers in order: 1,2,3,4,5 etc.
3. Be obtuse, think outside the box. Don't use dictionary words, invent new words!
4. Never use your mother's maiden name or any password that your bank might use.
5. Mix keyboard characters such as the asterisk with letters and numbers.
6. Use a mixture of upper and lower case letters.
7. Always change default passwords from 'password' or 'admin'.
8. Make sure the password is at least 8 characters long. The longer the better.

Make sure you log out of any user account, web service or program you are logged in to. Use different passwords and email addresses to register for different services. Change your passwords regularly.

Don't keep your passwords on a Post-It note on your desk! If you can't remember them, write them down and put them in your wallet. Then if you lose your wallet, you'll be replacing your credit cards, identification licences, and changing all of your passwords.

8 What is the best password strategy?



It's a sad fact, but people don't take passwords seriously enough. You could almost write a comedy sketch about the 'obvious' passwords that so many people use. A password consisting of the numbers 'one to 10' is not uncommon, as is simply the word 'password' or 'admin' or the user's first name. In 2009, 20,000 Yahoo, AOL and Hotmail passwords were hacked only to find the most popular password was '123456'!

Using the name of your first pet or school, your birth date or your mother's maiden name, is not smart either as this information is often favoured by banks as a means of identifying you. Putting it out digitally in any form (even if that is onto a comparatively secure website or not) is simply not good sense.

"To continue reading this piece, please enter a password. If you do not have a password please create one now of at least eight characters in length. Please use a combination of upper and lower case letters, plus numbers."

How familiar is that? How many times do we see those instructions and just blindly type in something meaningless so that we can continue surfing?

The problem is that there are so many 'light' password gateways today. Websites seek to create 'sticky' pages that users will repeatedly revisit by offering password access only. But these gateways obscure the importance of the 'heavy' passwords that you need to keep close to your chest and that you need to create intelligently.

Just to be clear, there is no industry de facto term that defines a 'heavy' password. We are simply drawing a distinction between a casually used password that might, for example, let you view an online news item, to that of your online banking password, which should be ultra-robust. Definitely then, do not use the same password you use for banking and transacting as the one you use to access social networking sites like Facebook.

So what makes a good password?

Firstly and most importantly of all, a good password is a password you can stick with. There are no ground rules on this one and the jury is

out from a technical perspective as to whether this process simply opens up more hacker gateways or whether it closes them down.

What is important is that you are supremely obscure. Don't use any of the cardinal numbers in order, even if you start at 3, 4, 5. Don't even use them in sequence as in 3, 5, 7. Use them backwards and interspersed with letters (both upper and lower case) and characters from the top line of your keyboard such as !, #, - and *, for example.

But that is just the start. If a hacker has managed to steal a copy of your password, it is most likely that he or she will only have an encrypted value of your password. The hacker will start using password hacker systems, which will initially attempt to use human language dictionaries and human behaviour logic to crack your secret code.

So be as illogical as you possibly can be. Don't use the word 'frogspawn' when you could use 'spawnfrog' and so on.

Carrying that 'illogical' theme forward, use your brain to outwit any computer password hacking software. Humans are visual thinkers, so this means we can visualise clearly in our own heads something that might not be part of the real world.

Have you even seen a purple elephant? Neither have we, so that's a good image - and therefore a good phrase to use. Why stop at purple, let's choose a more creative colour such as ochre, fuchsia or puce. Why stop at elephants, let's choose echidnas, possums, wombats and so on.

Of course, some security experts say that we shouldn't use any dictionary words from any language in a password. One way around this is to use product names and numbers instead. Most of us can easily visualise an obscure product we own (e.g. scuba diving regulator) and recall its product number (e.g. Apeks XTX200). Then we just change the product number a bit.

So let's be clear - we are not saying that 'OchrE59EchIdnA18!*' or 'ApEx!xtx-2o0' are not the best passwords you'll ever come up with, but it's certainly going to help you if you think along these lines.

9

What are the main IT security issues that small business face?

Protecting your business

AVG have a range of resources and guides to help small businesses. Visit <http://www.avgatwork.com.au> or <http://www.avgatwork.co.nz> that has a wealth of information and tools for those interested in better protecting their business.

Take AVG AU/NZ's [Online Security Audit](#) to get a personalised security action plan, download our [guide to securing your start-up or small business](#), or understand the [practices that can open the door to cybercriminals](#).



You name them! Small business faces numerous threats including, and certainly not limited to:

- Online or web security against malicious websites.
- Email problems including spam, phishing and malware.
- Securing data so that sensitive information isn't accidentally or deliberately distributed.
- Employee behaviour that may unwittingly introduce malware onto networks.
- Remote access, and the use of Smartphones and Tablets.
- Plug in USB memory sticks and portable data storage solutions.

99% of malware is now delivered via the web — 90% from popular websites. More than 70% of websites with malicious code are legitimate sites that cyber criminals have infected. More than 85% of all email is spam and more than 80% of those spam emails contain malicious links. It's very easy for customer databases, price lists, contracts and other sensitive information to be accidentally shared online.

Securing your business from malware and other threats is a relatively simple matter, but it does require some forethought and a small

investment of money and time. By taking action now, the time and cost will be more than offset against the potential lost revenues and wasted management time in dealing with security issues.

When thinking about online security for your organisation, consider the age-old medical adage: 'prevention is better than cure'. The essential steps to take can be broken down into three categories – Policy, Technology and Process.

9

Continued...

What are the main IT security issues that small business face?

Policy

- Decide whether computers, laptops and software are to be supplied by your company or by your staff – and reflect these decisions in your policies, purchasing and processes.
- Document a simple acceptable-use policy for any computer that is used for company business or media used to store or transport company data.
- Create an acceptable password-strength policy and ensure that all computers and other IT equipment are password protected.
- Require all security incidents to be promptly reported and managed by a business stakeholder.

Technology

- Ensure all operating systems and application software are updated with the latest security patches as they are developed – preferably using automatic update technology.
- Ensure all computers have an up-to-date security software suite on them.
- Every computer should have its own firewall software, in addition to any premises-based network firewall you may be running.
- If managing your own file storage and email servers, ensure these are also running up-to-date security software.

Process

- Ensure all staff gain basic online security training and instruction in your policies.
- Ensure regular backups are taken of all company files, data, email and other systems.
- Change all passwords regularly, especially when an employee or contractor leaves the company, and in particular change administrator passwords or shared passwords to centralised networks or systems.
- Take security breaches seriously – isolate any compromised systems from the network and involve an IT security professional if necessary to ensure the malware is fully removed.



10 Small business is increasingly hearing about 'cloud computing'. Is the cloud secure?



Security concerns have arguably been one of the biggest stumbling blocks to cloud computing's general uptake. As a security company, AVG advocates caution at all times, but especially during periods of IT change or transition. So how real are the perceived dangers in this area?

Cloud computing's central premise is one of taking applications and data outside of a customer's own premises and 'hosting' them as a 'service' from the cloud's data centre, which is connected back to the company via the Internet. This might sound like the opening of a security trapdoor straight away. But if best practices for security attacks and malware prevention are adhered to, then the cloud model is not inherently insecure.

The problem here is more likely to arise from IT staff not knowing which applications across the corporate network have been deployed from

the cloud. In many instances the culprits are the end users, who bring new cloud-powered web applications online without ensuring they are evaluated for security.

Technology analysts *Aberdeen Group* have conducted a study which found that users of cloud-based web security had substantially better results than users of on-premise web security implementations in the critical areas of security, compliance, reliability and cost.

Cloud computing "done properly"

So for want of a more formal term, if cloud computing is "done properly", then it can, by and large, work properly - and securely.

Our watchwords and guiding principles are: process control, rules, regulations and user policy enforcement.

Groups including the [Cloud Security Alliance](#) are active right now in the pursuit of security standards for cloud computing. This Alliance has correctly surmised that there are both secure and insecure cloud deployments; just as there are secure and insecure cloud local 'on-premise' data centres.

Cloud computing's pre-flight checklist

What makes the difference is the approach taken to encryption in any given data environment and, crucially, across any given software application lifecycle system.

As we now send more and more data and applications to be outsourced and hosted, the cloud computing pre-flight checklist is growing and becoming more rigid. But that's natural for any trip to the clouds isn't it?

11

So how do we stay safe online in 2011 and beyond, be it at home or at work?

The Australian government Stay Smart Online website has eight simple tips for staying safe online.

- **Install Internet security software**

This protects you from identity theft, spyware, viruses and other malicious software. Make sure that your security software stays up-to-date, have it scan all of your files regularly, and if you have a paid solution, make sure that you renew your subscription before it expires. AVG has both [free](#) and [paid](#) antivirus and Internet security solutions for Windows, [Mac](#), Linux and [Android](#) users.

- **Turn on automatic updates for all of your software.**

By switching on the automatic update features of your operating system, security software, utilities and other applications, your computer will be defended against security vulnerabilities that crop up every day, because it has the latest fixes or patches. Once you've done this, you don't have to remember to do it yourself.

- **Think carefully before you click on links and attachments.**

Always be wary of clicking on links and attachments in email messages or links posted on social networking sites, because these can take you to web pages with viruses, malicious software, or scam websites designed to steal your personal information. The best and safest practice is to only open attachments or follow links from trusted sources. Don't be tempted by offers that look too good to be true, because they usually will be.

If you're not sure if a website is safe, then go to www.avgthreatlabs.com and enter the website's URL to get its safety rating. [AVG LinkScanner](#) for Windows and Mac PCs provides web protection wherever you go online by actively checking web pages in real time before they open. If it sees trouble ahead, it warns you.

- **Regularly adjust your privacy settings.**

You're not the customer of the social networking websites, you're the contributor of often sensitive information. So make sure you properly manage what is shared and with whom it's shared.

The rules that protect your privacy on popular social networking sites like Facebook, Twitter and LinkedIn change frequently. Make it a priority to check the privacy policy and your privacy settings when you join a social networking site, because many sites will share your personal information with advertisers and people you don't know by default.

When new features are added to social networking sites this could impact your privacy, so make sure you go back often and check for any changes to how your privacy is managed, otherwise you could be sharing more about yourself than you realise.

- **Report or talk to someone about anything online that makes you uncomfortable.**

If you experience anything online that makes you uncomfortable, the best defence is to report it.

You can install the Australian Government's Cybersafety Help Button onto your desktop or task bar and have help just a click away. It's designed to protect families, including teenagers and children — from cyber bullying and improper behaviour, as well as Internet scams and frauds. Simply press the big red button to report offensive or suspect activity. Kids can get twenty four hour access to the Kids Helpline, as well as plenty of information about safe Internet practices. The Cybersafety Help Button is a free application and you can download it from dbcde.gov.au/helpbutton.

- **Stop and think before you share any photos, personal or financial information.**

If you are asked to share or post any personal or financial information — such as personal photos, credit card details, banking passwords, driver's licence numbers, Medicare numbers, or address details alarm bells should start to ring. As a general rule, never provide this information.

Even if the source appears to be legitimate — unless you've initiated it, or know the contact personally — your identity could be at stake here. Financial and government institutions will never request your personal details via email.

If you are asked to provide such sensitive information, the request is probably from a thief! So play it safe: simply don't provide the information.

- **Use a strong password and change it at least twice a year.**

See our advice outlined in Question 9 for advice on highly effective password strategies.

- **Know what your children and/or staff are doing online.**

Make sure they know how to stay safe and encourage them to report anything suspicious.

You can find plenty of information about how to use the Internet safely on the government Stay Smart Online website at www.staysmartonline.gov.au or www.netsafe.org.nz. You can also sign up for the government's plain language, free Cyber Security Alert Service that keeps you informed of new threats as they happen.

About AVG Australia & New Zealand

Based in Melbourne, AVG (AU/NZ) Pty Ltd, an Avalanche Technologies Group company, is a wholly owned Australian company that distributes the AVG Technologies' range of Anti-Virus and Internet Security products to the Australian, New Zealand and South Pacific markets. AVG provides outstanding technical solutions and exceptional value for consumers, small to medium business and enterprise clients. AVG delivers always-on, always up-to-date protection across desktop, and notebook PCs, plus file and email servers in the home and at work in SMBs, corporations, government agencies and educational institutions.

About AVG Technologies

Founded in 1991, AVG is a leading international developer of Internet threat protection solutions for businesses and consumers. AVG protects more than 110 million computer users around the world. The company has offices in Europe and North America and employs some of the world's leading experts in Internet security, specifically in the areas of threat research, analysis and detection.

Connect with us locally:



www.twitter.com/avgaunz
for local Australian, NZ and international updates & tips



www.facebook.com/avgaunz
for local news, tips, promotions and advice



www.youtube.com/avgaunz
for latest videos.

Connect with AVG Technologies internationally:



www.twitter.com/officialAVGnews



www.youtube.com/officialAVG



www.bit.ly/AVGSMB

For security tips and to learn more about how AVG can protect you online see <http://resources.avg.com.au/> or <http://resources.avg.co.nz/>

To gain specialist guidance on protecting your small business visit www.avgatwork.com.au

Contact us:

Australia: **1300 284 000** (local call within Australia)

New Zealand: **0800 284 000** (toll free within NZ)

International clients: **+61 3 9581 0800**

AVG (AU/NZ) operates a local support team to assist in ensuring you stay protected.

Or via email: info@avg.com.au



© 2011 AVG (AU/NZ) Pty Ltd and AVG Technologies CZ, s.r.o. All Rights Reserved.
AVG is a registered trademark of AVG Technologies CZ, s.r.o.
All other trademarks are the property of their respective owners.