

Small Business Security Guide

Five business
practices that can
open the door to
cyber criminals

Brought to you by AVG Australia and New Zealand



AVG. AT WORK

Shutting the door to cyber criminals

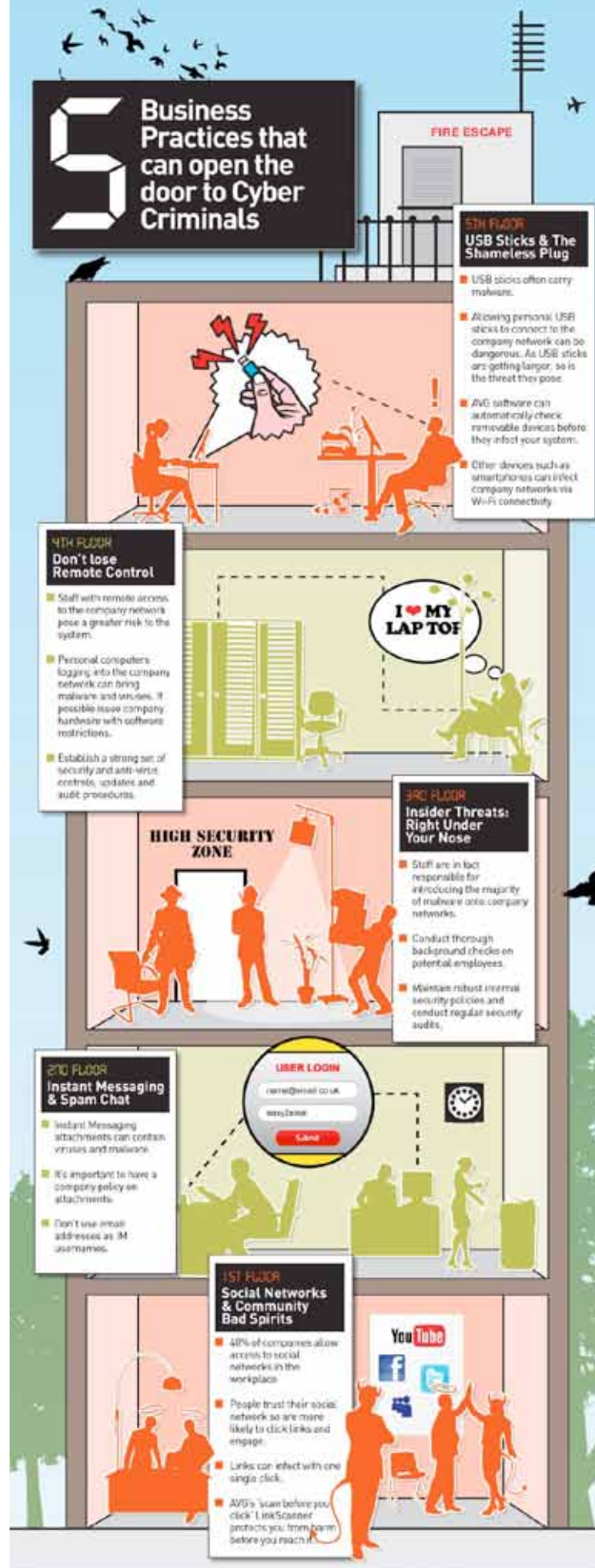
Small to medium-sized businesses are increasingly becoming targets for cyber criminals. Shutting the door on them is not enough - companies need to embrace and adopt a concrete lock-down process that constantly monitors for new and emerging threats from a variety of channels.

The journey toward success for any small business owner is usually a long one. By merely embarking on it, you open yourself up to attacks that fly in from all quarters. At least when it comes to competitors, you can be on the lookout, but what about cyber criminals? Do you know what's out there? Do you know how they can come at you? Will you be prepared when they do?

Cyber criminals will turn your most valuable assets against you. That same Internet connection you use to make financial transactions can let in a Trojan horse. The iPhone and Android smart phones your workers use to communicate with each other could be used to gain access to sensitive company documents. The social media channels you use to engage customers can be hijacked and used to harm your reputation. How can you arm yourself with the digital tools you and your workforce need to succeed without those very same tools being used against you?

Too many small business owners are letting their guard down. The very people we hire to help us succeed are very often the people that can cripple a network and bring down a business - all because they didn't know how to exercise proper caution in their use of the Web and mobile.

To help small to medium-sized businesses, this SMB Guide highlights five doorways through which cyber criminals can access company data.



Door #1 - Social Networks

The Danger: Trust

Most social networking activity revolves around community spirit and sharing a wide range of data including documents, music, video and links. People trust people they know. Users are more likely to click an infected link if it comes from a trusted colleague or friend.



The Solution

1. There are two ways to help protect against this.

Using AVG's free 'scan before you click' LinkScanner® technology will ensure shared links and files are checked and safe.

2. Beef up your security policy.

Recent AVG research suggests 40% of companies allow access to social networking technology, but only 23% of businesses say they have any appropriate security policies in place. Offer staff some guidelines to keep them and your business network safe.

For guidance on developing and implementing a security policy, see AVG AU/NZ's helpful **Small Business Guide: Securing your start-up or small business**. This is an 11-page action template covering the establishment of policies and processes to secure workplace practices and deliver governance over technology use. It may be downloaded [here](#).

Door #2 - Instant Messaging and Spam Chat

The Danger: Viruses and other malware

Viruses and other malware can be hidden in files sent via Instant Messaging (IM). Accordingly, you should introduce some policies to control the use of IM and educate users about its potential risks. Some IM services link your screen name to your email address when you register. Having your email address so readily available can result in an increased number of spam and phishing attacks.



The Solution

Don't use an email address that can be easily identified by your IM username. Some IM services link your screen name to your email address when you register. Having your email address so readily available is bound to increase the risk of spam and phishing attacks.

Door #3 - Insider threats right under your nose

The Danger

Although businesses might rightly be more concerned about shadowy cyber criminal outsiders, the reality is that employees are responsible for introducing the majority of malware onto company networks and thus pose a similar or even greater threat.

The Solution

Background checks on potential employees - especially IT and technical staff - are essential, and high-risk businesses should consider using advanced tools to conduct criminal history and social security searches to ensure their employees are totally trustworthy. The best advice is relatively basic - trust your gut feel, educate staff on keeping their data and network safe, and enforce a robust internal security policy combined with a security audit.



Door #4 - Don't lose remote control

The Danger:

While preventing staff from leaking malware into a business has its challenges, staff who are allowed to access the company network remotely are even harder to control. Allowing staff to use their own smartphones, tablets, and PCs for work increases the risk that malware may get inside the company network.



The Solution

An obvious way to close this security hole is to prevent staff from using their own machines. Businesses could use virtualisation technology to create a virtual safe-zone within your hardware - like an embassy does in a foreign country. Whatever your approach, it is essential to establish a strong set of security controls that ensure all staff only use hardware with appropriate Internet security software in place, with automatic updates working and subject to regular audit procedures.

Door #5 - USB Sticks and Smartphones

The Danger:

Plug-in memory USB sticks and portable drives are particularly good at spreading malware. They appear innocuous compared to a laptop or smartphone but can hold several gigabytes of code - some of which may be malicious. Allowing employees an unchecked option to insert these into company computers is an unnecessary risk.

Email-equipped smartphones pose similar risks to company networks as desktop computers.

Smartphones can help spread malware onto other susceptible devices on the network and hackers have been known to use text messages to guide unsuspecting users onto web sites containing infected code.



The Solution

Removable devices can be automatically checked using AVG's business security software, or users can choose to run a manual scan before accessing any of the files on the stick. Business owners should also create policies to keep personal and business drives separate on any machine.

Consider disabling your Windows Auto Run feature. The risk of a system being infected by an infected USB flash drive via the Autorun feature far outweighs the minimal benefits that this feature provides. To disable this feature Microsoft offers some useful guidance [here](#).

Summary

Make no mistake; your small to medium sized business is a target for a cyber criminal. Leaving any door open makes you a very attractive target indeed.



Security is a serious business. Shutting the door on cybercriminals is not enough; you need to embrace and adopt a concrete lock-down process that constantly monitors for new and emerging threats from a variety of channels.

The good news is you're not alone. The [AVG Small Business Security Guide: Securing your start-up or small business](#) provides some simple but effective steps you can take to secure your business. Also, [AVG's Business Resource Centre](#) has a library of guides and tools that can help you protect your business from identity theft, data breaches, online banking break-ins and other computer crimes.

AVG (AU/NZ) also has a comprehensive range of security tips on its web site at <http://www.avg.com.au/resources/security-tips/>

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

To learn more about how AVG can protect your small business visit www.avgatwork.com.au

For a confidential discussion on how AVG can protect your business, contact us on:

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

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

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

Lines are open from 8.00am to 6.00 pm, Melbourne time Monday to Friday.

Alternatively contact us at 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.