



10

**Top
tips to stay safe**

Protecting your business against the latest Web threats has become an incredibly complicated task. The consequences of external attacks, internal security breaches, and internet abuse have placed security high on the small business agenda – so what do you need to know about security and what are the key elements to address? Trend Micro sheds some light on this tricky subject.

Top Tip One: Close your doors to malware

In the same way that you wouldn't dream of leaving your back door unlocked at night, you wouldn't invite cyber criminals into your business. But by leaving your internet security wide open, and not having adequate firewalls and antivirus software, that could be exactly what you're doing.

In fact, according to the The Australian Business Assessment of Computer User Security: a national survey, from www.aic.gov.au, Australian small businesses lose on average \$2,431 per computer security incident. With more than 75% of small businesses admitting to being a victim in a 12 month period.

Malware is 'malicious software' designed to infiltrate or damage a PC or network without your knowledge or consent. A good Internet router will have an on-board firewall (so don't forget to turn it on), but this is not enough nowadays with the complexity of malware. The best security software will go beyond standard protection and will reside on the PC without hindering the performance of your PC, laptop or network.

Rather than relying on a pre-installed or consumer solution, choose a security solution such as Trend Micro's Worry-Free Business Security that protects against conventional threats like viruses, spyware, spam and phishing, but it also helps you to defend your business from the latest threats including identity theft, risky websites and hacker attacks. And best of all it does it without impacting your PC's resources which is common with conventional security solutions.

Top Tip TWO: Use security to make your business more mobile—not tie it down

The Internet is a fantastic business enabler, freeing your business to do business wherever is right for you and your customers. But it can also present a greater degree of risk – as connecting via public internet routes allows an increased opportunity of malware exposure and do not provide pro-active content scanning to track malware and alert you to the potential problems.



However, with the right security solution it is possible to protect your mobile devices and your business when out of the office – no matter how you connect. Good security software will have what's called location awareness that enables it to automatically change the security settings on laptops, selecting the best level of protection for employees as they move inside or outside the office.

This level of intelligence within the software protects your business without the need to rely on employees to think about security or restrict where and when they can access the network or Internet.

Top Tip Three: Embrace the Web

As we said before, the Web is a very powerful tool, and as consumers become more comfortable with buying products and services online, this is only set to continue. But a hacker can exploit vulnerabilities on legitimate websites, making your business an unknowing accomplice to spyware or even identity theft – putting your business, data and reputation at risk.

A solution such as Trend Micro's SecureSite will enable your business to test your website for vulnerabilities, dangerous content and links that expose your customers' computers and personal information to malicious use. Websites that meet the security policies can display a new Trend Micro SecureSite trust mark to identify their security reliability and diligence.

Top Tip Four: Get a policy

Think your business is too small for hackers to worry about? Think again. Size is really irrelevant when it comes to online crime and fraud. So it's important that your business takes security seriously, and one way to do this is to create an Information Security Policy.

- First step is to talk to your employees and help them to understand the importance of good security practices – such as not opening email attachments from unknown senders.
- Secondly, create an acceptable usage policy – this lets your employees know what they can and cannot do on their PC. Put down in writing what you expect – covering from passwords to downloading files or music etc. from the Internet. It might also include prohibitions against installing unauthorised software or visiting specific websites, such as Web 2.0 or social networking sites – whatever it includes, it should state the penalty for violating the policy



and be signed by each employee (and you too).

- In addition to your acceptable use policy, consider creating a handout on how sensitive information is handled. This should cover what type of email or documents employees can send to others outside the company, how to handle copyrighted materials and what type of customer information can be shared. Again, circulate the policy among your employees and have them read and sign a copy.
- Lastly, it's a good idea to appoint someone in your business as your 'security expert' and make it known to everyone that this person is available to find answers to – or respond to – security questions.

Top Tip Five: Get a relationship with your reseller

Having a good relationship with your IT reseller will mean that you always have a trusted advisor to turn to when it comes to IT issues. And rather than you just responding to the latest deal or best price ad you've seen, they will also be able to help you select the right solution for your business that will grow with your needs and protect your IT investment.

And who knows, if they like you enough they might even offer to remotely manage your security solution for you – meaning less hassle and even greater protection for you and your business.

Top Tip Six: Get help from your employees

We've all seen the headlines that high profile data loss cases cause, but did you know that up to 80% of all data loss is caused by human error – either sending out confidential or sensitive information to the wrong people or in an unsecured way?

The implications for this are becoming even greater with increasing compliance regulations. So if your business employs more than one person, look to educate them about the risks their actions can present.

Alongside this you can implement effective company-wide security policies that everyone knows and understands, and if needs be, look at an email encryption solution that can help prevent your sensitive information being wrongly handled.

These solutions can automatically identify particular types of content, depending on the policies that you set up, and encrypt the emails when the rules are triggered. This means that you don't have to rely on your employees to keep important



content secure – it's done automatically for you.

Some hosted email security solutions, such as Trend Micro InterScan Messaging Hosted Security, can integrate this as part of the overall offering – and because they're hosted, they take away the worry while freeing up your time to do other things.

Top Tip Seven: Stop spam in its tracks

Spam is an ongoing headache for most businesses, causing problems such as network slowdown and delayed communication. It affects productivity and often delivers offensive or malicious content.

To cap this off, spammers are continuously deploying changing techniques to get around conventional filters. Botnets, dictionary attacks, hijacked PCs and image spam are being used to deliver increasing levels of stock pharmacy and mortgage spam into your mailboxes.

However, today's security technologies are using even more unique ways of dealing with this unwanted traffic – using online or 'in-the-cloud' resources to block it before it even reaches your email server – this delivers better protection with less impact on your network and employees' performance. Also look for a solution that offers multiple layers of spam protection to help ensure complete protection.

Top Tip Eight: Use a filter, not blinkers — Gain back your productivity

According to IDC, 30 – 40% of Internet use in the workplace is not work related. This is backed up by Trend Micro research which found 51% of employees within small businesses admit to surfing non-work related websites during work hours. In addition to surfing the Web, employees increasingly use streaming media, peer to peer (P2P), Internet radio, and other bandwidth-intensive protocols.

Aside from using up valuable resources, this can have a significant impact on your company's reputation – especially if your employees are downloading inappropriate content – as this not only exposes your business to threats, but



potential prosecution as well.

By using URL filtering software, you can control access to the types of websites you deem appropriate for viewing during work hours. This enables you to ensure that your employees are able to visit sites required for their roles without getting distracted; keeping them and your organisation safe and more productive.

Top Tip Nine: Think about the consequences

How many times have you seen 'funny' emails being circulated around the office? But have you thought about the consequences of those emails if they fell into the wrong hands?

A rising number of employees are taking legal action against their employers because they've been exposed to offensive or inappropriate content at work, and winning large settlements because their employer is held responsible for the content of their network.

From racial to sexual harassment, through to the spreading of extreme political views, it all has financial, reputational and demoralising consequences for the business as a whole. But if you can stop offensive content coming into the network then you've already won half the battle. So make sure you have an appropriate content filtering solution as well as a well enforced suitable security policy to reduce your legal liability should anything unforeseen happen.

Top Tip Ten: Stay up to date

The majority of threats exploit weaknesses within existing operating systems and applications. So it's very important to ensure that you have the latest protection.

Traditional security solutions rely on pattern matching and signatures; however, constant changes in the threat landscape have caused massive growth in complex types of threats. This means that security vendors are reacting by issuing more frequent pattern updates – which as you can imagine, has a significant impact on system performance.

Trend Micro's Smart Protection Network uses an innovative architecture that provides faster PC and server protection. A light-weight client uses in-the-cloud technologies to reduce the burden on the PC, while providing immediate access to the latest threat intelligence. This unique approach correlates in-the-cloud web, email, and file reputation databases, to provide real time protection at all points of an attack, and stop threats from impacting your business.



At Trend Micro we understand that as a small business owner, you have enough to do running your business – so that is why our solutions address threats in a way that reduces the burden on small businesses. Our unique solutions gather knowledge and rapidly deploy it to defend our customers. Giving you the easy-to-use, simple, hands-off protection that you and your business needs.

Find out how Trend Micro can help protect your business today, visit www.trendmicro.com.au for more information.