

## *If you're worried about security on the Net, here are a few hints.*

The World Wide Web opens up many new opportunities for small businesses, but exposes you to new risks. Before embarking on eCommerce ventures, take time to understand the risks and protect your business.

Common risks include viruses, hackers, security for online banking and credit card fraud. This eNote outlines methods you can use to protect yourself and your business online:

- **Internet Security Software** – software which combines antivirus and firewall software (see below) and often includes anti-spam and other security and productivity features.
- The Internet Industry Association provides a list of free trials for security software at [www.iiia.net.au/novirus](http://www.iiia.net.au/novirus)



- **Antivirus software** — software which detects and removes known computer viruses.
- **Firewall software** — software which acts as an intelligent gateway between your computer and the rest of the Internet. It monitors the traffic flowing in and out of your system and checks if it's authorised to do so. If there is no authorisation, that communication is blocked and you remain protected.
- **Online banking security features** — features that banks include in their online

banking service offerings to protect their customers, and themselves, during online banking transactions.

- **Online transaction (buying and selling) security features** — features such as encryption used on websites to protect customer details during transactions. These are often part of the Internet Service Provider package, so ask your ISP.

## The Starting Point for Security

Some basic procedures can reduce your risks significantly:

- Install a reputable Internet Security package (or separate antivirus and firewall) and set it to stay updated automatically. Ensure you update all other software as well.
- Use different passwords for different programs and websites. Change passwords regularly for increased security.
- Be careful replying to email from unknown sources and spam (junk email). Talk to your Internet Service Provider (ISP) if spam becomes a problem and use the anti-spam features of your existing email software or if not available, use third party anti-spam software to effectively deal with spam.
- Be careful opening email attachments or downloading Internet files from unfamiliar sources. Run a virus check on those files.

## Firewalls

- Firewalls can provide varying levels of security to a business accessing the Internet.
- Use of firewalls does require some skill, so seek technical advice to set up your firewall to suit your needs — see your ISP or computer retailer.
- Some firewall software comes in 'shrink-wrapped boxes' and can be purchased from a computer retailer or software dealer. Other firewall software can be directly downloaded from the World Wide Web.

## Antivirus Software

- A virus is any computer program written to damage computer systems. This involves attaching viruses to outgoing emails sent to using your computer as a server).
- Viruses may be sent deliberately or accidentally, within email or email file attachments.
- Viruses can be detected by antivirus software, which must be kept up-to-date. Ensure your software is set to update itself automatically.

## Online Banking Security Features

- During online banking, the connections to your bank's website will encrypt or encode customer information. Look out for a **gold padlock** at the bottom of your browser window — it indicates your information is being encrypted using the Secure Socket Layer protocol (denoted by https://) before it is transmitted to the bank.



## Security for Online Transactions

- Web merchants often use encryption to protect credit card numbers and other customer personal details. Again, the **closed padlock** indicates that the data transfer is being encrypted using the Secure Socket Layer protocol (denoted by https://).
- Banks and payment gateways are normally intermediaries during the buying and selling process. During this process, the bank also ensures information security.

## Where to Get More Information

- W3C (World Wide Web Consortium) Security Resources are available at [www.w3.org/security](http://www.w3.org/security)
- The *Trusting the Internet: A Small Business Guide to E-security*, which can help you understand the key issues of Internet security is available from the website: [http://www2.dcita.gov.au/ie/publications/2002/07/trusting\\_the\\_net](http://www2.dcita.gov.au/ie/publications/2002/07/trusting_the_net)

- The Department of Communications, Information Technology and the Arts has further information about Security at <http://www2.dcita.gov.au/ie/trust/protecting/e-security>

## Internet Security: Antivirus & Firewall

- Ask your ISP about Internet Security, firewall and antivirus software when you set up your Internet access.
- Visit the Internet Industry Association's National Antivirus Initiative at [www.iaa.net.au/novirus](http://www.iaa.net.au/novirus)

## Online Banking Security Features

- Contact your bank. For contact details try the Australian Bankers' Association — [www.bankers.asn.au](http://www.bankers.asn.au).

### Disclaimer

These materials are provided for general assistance and information only. Neither APT Strategies Pty. Ltd nor the State of Victoria makes any representations or warranties (express or implied) as to the accuracy or currency of the information contained in the materials nor endorses any company or organisation or other web-sites or materials referred to. The State of Victoria does not accept any liability for any reliance placed on this material, including any liability in negligence for relying on any information in these materials or any products, services or information which may be provided by the companies and organisations referred to. Copyright State of Victoria 2004.