

Learning Outcomes

The training objectives of this module are to provide information on:

- eSecurity
- Benefits of eSecurity
- Types of eSecurity technologies
- What sort of eSecurity does your business need?
- What questions to ask when purchasing eSecurity software?
- eSecurity Resources

Workshop Notes:

What is eSecurity?

The World Wide Web opens up many new opportunities for 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. In this training module, we shall touch on methods you can use to protect yourself and your business online:

- **Internet Security Software** – software which combines antivirus and firewall software and often includes anti-spam and other security and productivity features.
- **Antivirus software** — software which detects and removes known computer viruses. Quite often, viruses arrive onto your computer network through email. Antivirus software ensures that all emails arriving in your Inbox are “clean” and quarantines those emails it detects as being infected.
- **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 remember to ask your ISP.



What are the eSecurity business benefits?

The key business gain in establishing a robust eSecurity program in your business is that it allows you to operate without interruption. Imagine the disruption caused to your operations if your system was infected by a virus and shut down, your business was hacked into and your confidential material was accessed or your customers were defrauded.

These things can take an hour or weeks to fix so in the case of eSecurity, prevention is better than finding a cure.

Specifically, the benefits (often referred to as the 'Four Pillars of Trust') of applying eSecurity technologies include:

- **Privacy and confidentiality** – To ensure that customer data remains private and users have control over how information is used
- **Authenticity** – For businesses to know exactly who they are dealing with
- **Integrity**– Transaction details and other valuable commercial information will not be accessible to anyone other than those involved in the transaction
- **Non-repudiation of payments and transactions** – businesses must have confidence that a payment made over the Internet is irrevocable. A contract formed over the Internet must be binding and capable of enforcement against a defaulting party.

Workshop Notes:

How does eSecurity work?

eSecurity works by utilising various authentication technologies to ensure protection for business. These include:

- **Secure access (password authentication)** - A username and password is assigned to each user to allow access to a website. Used: when a low security level is required.
 - **Reference Websites** www.hotmail.com
www.pureprofile.com.au
- **Secure connections (SSL)** – Secure Socket Layer (SSL) combines a basic password system with protocols that encrypt data transmissions. Used: for websites that sell products and services
 - **Reference Websites** www.chaosmusic.com
www.rosesonly.com.au
- **Secure interconnection (PKI)** – Public Key Infrastructure (PKI) uses keys to scramble and decipher messages. Used: for high value business, government and military transactions
 - **Reference Websites** www.verisign.com.au/managedpki/



www.thawte.com/spki/

- **Secure personal connection (PGP)** – Pretty Good Privacy (PGP) uses public key encryption. Used: as a popular security option for individuals
 - **Reference Websites** www.pgpi.org
- **Secure networking (VPN)** – Virtual Private Networks offer one of the highest levels of security using advanced encryption and tunnelling technologies. Used: by business with multiple office locations
 - **Reference Websites** computer.howstuffworks.com/vpn.htm
- **Email security** – Where similar software is used to send and receive encrypted email messages so only the intended recipient can read it. Email software includes:
 - Dedicated email encryption- Uses same technology as PKI/PGP and can plug-in to existing email software (e.g. Microsoft Outlook, Eudora)
 - Secure email gateways – For businesses that do not require email security within their own office environment yet do outside the internal mail gateway
 - **Reference Websites** www.pcguardiantechologies.com
- **Anti-virus software** – Installed on a computer to protect and eliminate incoming viruses
 - **Reference Websites** www.symantec.com
www.mcafee.com
www.iaa.net.au/novirus
- **Firewall** – A firewall is software that separates a public business Web server from its internal network and provides the first layer of security for your computer when you connect to the Internet.
 - **Reference Websites** www.symantec.com
www.mcafee.com

Be vigilant against viruses!

Quite often, you can stop viruses even before your anti-virus software detects them. By following the steps below, you can ensure protection against virus attacks:

- Be cautious about opening unsolicited emails, especially if they contain attachments
- Only download software from trusted websites
- Disconnect your PC from the Internet when not in use

Workshop Notes:



What does eSecurity Cost for my business?

Small business:

- **Antivirus:** Individual or multi-user packs are approximately \$100 to \$400
- **Firewalls:** Approximately \$400
- **Integrated anti-virus and firewall protection:** Approximately \$500+

Medium business:

- **Antivirus:** Approximately \$1600
- **Integrated anti-virus and firewall protection:** Approximately \$2500+

Secure eCommerce Payment solutions

A secure, real-time payment facility including on-line reporting, SSL encryption, GST features and currency conversion start at around \$400 (some gateways may ask for a fee per transaction as well)

On top of your eCommerce payment solution a "Bank Merchant Facility" is required to process credit card payments. This includes a fee of approximately 1% of each total transaction value.

For more information on Secure eCommerce see:

- www.verisign.com.au/guide/
- *Trusting the Internet* publication at www.dcita.gov.au

Workshop Notes:



Questions to ask when purchasing eSecurity software?

Firewalls

What sort of Firewall do I need for my business?

- Firewalls can provide many levels of security. As firewalls require some skills to set up, it is advisable to seek technical advice to set up your firewall to suit your needs — see your ISP or computer retailer.

Where can I purchase Firewall software?

- Some firewall software comes in shrink-wrapped boxes and can be purchased from a computer retailer, software dealer or can be directly downloaded from the World Wide Web.

How can I ensure that my Firewall remains secure and up to date?

- Set your firewall to update itself automatically. Most update when you are connected to the web.

Antivirus Software

What sort of anti-virus software do I need for my business?

- The decision revolves around how many individual computers your business has that require protection. Like firewall software, it can be purchased by traditional retail means or downloaded across the Internet. Also like firewalls, antivirus software must be kept up-to-date and can be updated automatically when you are connected to the Internet.

Security for Online Transactions

What type of secure online payment solution do I need for my business?

- Secure online payment solution costs are based on the volume of transactions. The more you do, the cheaper it gets – a bit like mobile phone plans. Try and estimate how many transactions you will be doing across your website and use this number to make your decision.

Workshop Notes:



eSecurity References

Case Studies

- The Coffee Company - www.coffeecompany.com.au
- Clearstream Olive Farm - www.clearstreamolives.com.au
- Further case studies are available at www.mmv.vic.gov.au/casestudies

eNotes

- eNote 12: Selling Online
- eNote 14: Online Credit Card Facilities - FAQs
- eNote 16: Security

Websites

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

Activities

Time allocation: 10 to 15 minutes per group

1. Explain how your business is adopting or implementing eSecurity policies and practices?
2. Using an example, how would you implement or improve the existing eSecurity measures within your business?

Workshop Notes:

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.