## LEARNING OUTCOMES

Recognise that there are serious security issues associated with the online world.
Recognise that there are strategies for being secure and responsible online, just as there are for being safe and secure offline.
Recognise that cybersecurity is the responsibility of every ICT user.
Identify four basic cybersecurity strategies: a firewall, anti-virus software, keeping security software up-to-date, and email filtering.

## INTRODUCTION

There are serious security issues associated with the online world. Cybercrime is a widespread and growing phenomenon. Cybercrime is a threat to critical infrastructure, and the digital economy. It is also a real threat to individual users. The consequence of not adopting cybersecurity strategies can be very costly, and may include the loss of personal identity, privacy, data, and devices.

Unsecured home-based computer systems are the frontline of attack for many cyber criminals.
There are simple steps that every computer user needs to take to secure their home-based system.
It is the responsibility of every user to secure their computers and internet devices.

## AT THE COMPUTER

In this activity, the student is presented with a selection of ‘enhancements’ for their internet device that are represented by graphics. These enhancements include cybersecurity fundamentals (firewall, email filtering, anti-virus software, and security updates) as well as things that are nice to have—graphics, music, games and movies.

The student is prompted with feedback to sort the things they ‘need’ to secure their device, from the things that are ‘nice’ to have. They also need to match the graphic depiction of these cybersecurity essentials to their definitions. In this way, the learner discovers the importance of cybersecurity fundamentals.

## FOLLOW UP

Whole-class discussion to review learning objectives.
Brainstorm why there are cyber criminals and what they are after.
Brainstorm the sorts of data that people keep on computers, and make a list of good things that may be lost if a computer is corrupted.
Brainstorm ways we keep ourselves safe and secure in the offline world. Compare these strategies to safety and security strategies for the online world.
Discuss other cybersecurity measures like backing up data, and securing wireless networks.
Discuss why it’s important to report (to teachers, parents or carers) anything bad that happens online: that it helps to make the web safer and more secure for everyone.

## RESOURCES

- Stay Smart Online at www.staysmartonline.gov.au
- SCAMwatch at www.SCAMwatch.gov.au
- ThinkUKnow at www.thinkuknow.org.au
- Cybersmart at www.cybersmart.gov.au

## UNIT VOCAB

- Anti-virus software
- Computer
- Cybercrime
- Cybersecurity
- Data
- Email
- Filtering
- Firewall
- Internet
- Internet-enabled device
- Malware
- Online
- Report
- Security updates
- Site
- Software
- Wireless

---

© Commonwealth of Australia 2011
Creative Commons Attribution Non-commercial 3.0 Australia licence