PC and me

LEARNING OUTCOMES:

Members will be able to:

- correctly connect a computer system including additional hardware;
- demonstrate proper cleaning and maintenance procedures;
- demonstrate skills in the use of word processing, Internet and e-mail software;
- demonstrate knowledge about PC security.

BADGE REQUIREMENTS:

1. With your group set up a stand-alone computer system.
2. Demonstrate basic care and maintenance of a computer and printer.
3. Use a basic word processing program to produce a letter or document.
4. Explain potential hazards and how to protect your computer.
5. Know how to protect personal information when using a computer.
6. Use an e-mail program to send and receive an e-mail.
7. Know how to use a 'search engine'.

GUARDS
RANGERS

CATEGORY

Skills

TIME FRAME

Three weeks

AIM

To develop members' basic computer skills and care of computer equipment.

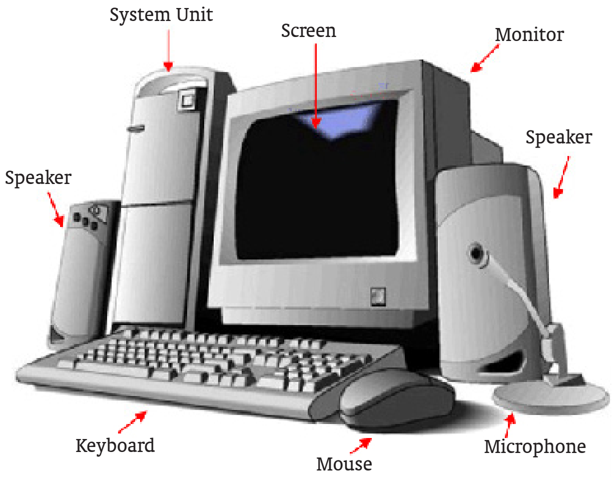
Teaching Ideas

Although there are a lot of 'self-trained' computer specialists around, you should ensure that the presenter is sufficiently experienced in the content of this badge. Knowing how to send an e-mail may be familiar to most people and is easily demonstrated, but knowledge about computer security will require a person with greater skill and understanding. A guest presenter could be identified in the corps or community, e.g. the local computer store owner, an IT employee.

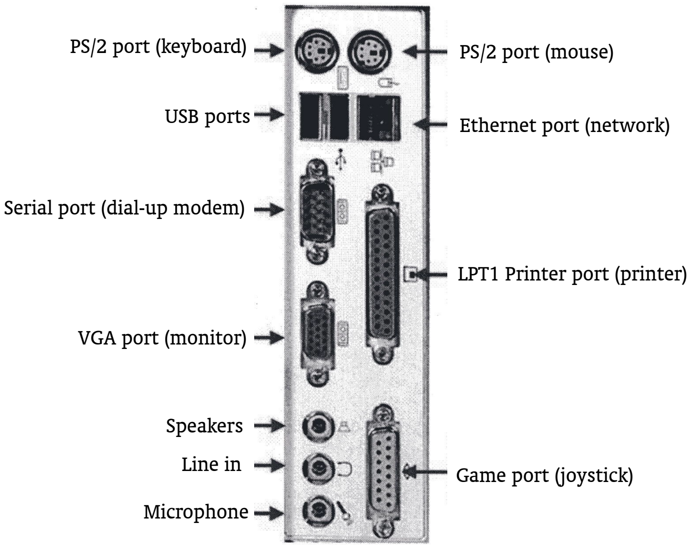
Providing equipment for members to use may be the first challenge of this badge. Some suggested sources of computer equipment include the corps computer, The Salvation Army's IT department, local computer store, or members'/leaders' personal computers.

1. With your group set up a stand-alone computer system.

The system to be set up should include at least a CPU (Central Processing Unit or System Unit), monitor, mouse, keyboard, speakers and a printer. Set up should include the installation of software drivers for one device, e.g. the printer driver software.



Explain each component as they are connected. Explanation should include the various cables and ports associated with the equipment. **Handout 1** could be used to help members identify the components and ports on a typical PC.



Members might be eager to discuss their own computer which may include additional components and ports. Allow them to talk about their computer with the group, e.g. they may have a 'Fire-Wire' port for more high speed applications such as digital video download.

Allow members to help connect the main computer components, without the printer. Then start the computer and confirm its operation. The computer could then be shut down and the printer connected and the computer restarted. When the computer has restarted it should then prompt that it has found new hardware. Members could then follow the steps to install the software drivers for the printer. (You need to ensure the printer drivers were not already installed.)

If you are finding it difficult sourcing hardware members could video themselves assembling their own PC. They could start with the basic components separated and then assemble and start up their computer.

2. Demonstrate basic care and maintenance of a computer and printer.

Commercially designed computer-cleaning kits can be purchased from a variety of retailers. They would generally include products such as cleaning wipes, air duster spray cans *(an air duster spray can is basically an aerosol can of 'clean air')*, soft brushes and cotton buds. Often these can be substituted with a clean dry cloth.

The computer itself will require limited maintenance – the biggest issue is dust. Dust is easily removed from the monitor and CPU by wiping with a dry cloth. To remove dust from the keyboard an air duster spray can be used or a soft haired brush. Another common issue is with the 'ball' mouse. Over time movement becomes 'jerky' due to the build up of grime on the mouse's rollers, ball or exterior pads. Cleaning wipes or a dry cloth can be used to remove the grime.

Over time dust will build up inside the CPU. You might show members how to open the box to remove dust by using an air duster spray can. Extreme care must be taken when doing this so as not to touch, damage or knock components. **Note: members should be warned that opening a computer may invalidate the warranty. Computers under warranty should only be opened by the computer's authorised repairer.**

Food and drink products should be kept away from the computer because they can short circuit the equipment resulting in irreparable damage.

There are a number of printer types and brands on the market. However, all of them require the replacement of ink. Discuss the different types of printers, e.g. Ink Jet, Bubble Jet, Laser, and how the cartridges are replaced. Demonstrate how to replace the ink as required. Most printers run maintenance software to assist in loading new ink cartridges or to complete a 'test' print when it has been replaced. Members could demonstrate how to use these options.

3. Use a basic word processing program to produce a letter or document.

The letter or document produced should include at least two fonts and one graphic.

Most Windows-based operating systems come with a basic word processing program. Members may use another program such as

'Microsoft Word™', 'WordPerfect™' or 'Lotus WordPad™'. Demonstrate how to choose a font, font size, paper size and orientation and to set margins. In addition to this they should know how to add bold, underline and italics to the text. Don't focus on typing skills but rather the member's ability to open and use the program, including formatting the page and the text, inserting a graphic, and printing the completed document.

Option 1: create a 'personal profile' sheet outlining name, age, interests and hobbies. Do not include addresses, telephone numbers or schools. This could be used at a Church Parade to encourage prayer partnership with corps members. A digital camera could be used to take the members' photos* for their page. This would have the added advantage of showing how to connect the camera and download the photos.

***Note:** *Remember to obtain parental permission for members to be photographed and used in a publication. See Caring for Kids 'Individual Record/Permission Form'.*

Option 2: a report based on an activity, e.g. expedition report, other group outing or activity.

Option 3: a document based on a topic chosen by members.

Option 4: write a letter.

4. Explain potential hazards and how to protect your computer.

Computers are vulnerable to computer worms, viruses and other damaging programs that access computers through Internet websites and infect files and disks. Members should have an understanding of these harmful programs and know how to protect a computer against them. Various security methods are available for home computers, e.g. virus softwares, firewalls, software updating, and password protection (see requirement 5).

The information on security could be taught using an open-style quiz or brainstorming activity. Ask open questions and invite responses. Accept all answers without judgement but direct members' thinking to the correct answer as you teach. This teaching style encourages participation. You may use the questions on **Handout 2**.

The local library may have videos/DVDs that teach information about computer viruses, spyware, SPAM and computer security. Use these tools to teach members. Alternatively present the following information on *PowerPoint,* displayed on charts around the room, or your own method.

Computer Worms

A computer worm is a self-reproducing computer program. It uses a network to send copies of itself to other systems and it may do so without the user doing anything. A worm will always harm a network unlike viruses which attack a targeted computer. It does not need to attach itself to an existing program.

Viruses

Computer viruses are software programs deliberately designed to interfere with computer operation, record, corrupt, or delete data, or

spread themselves to other computers and throughout the Internet, often slowing things down and causing other problems in the process. Some viruses such as "Trojans" often appear as a beneficial program to coax the user into downloading them, even providing the expected result whilst quietly causing damage in the background.

Spyware

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. Other kinds of spyware make changes to your computer that can be annoying and can cause your computer to slow down or crash. There are a number of ways spyware or other unwanted software can get on a computer. A common trick is to install the software covertly during the installation of other software such as a music or video file sharing program.

Spam

Spam is generally an unwelcome/unwanted commercial e-mail.

Firewalls

A Firewall is an 'electronic door' to stop people gaining access to your computer. When the door is left open hackers or malicious software can find its way into your computer. A firewall can either be a software application or a hardware device.

It is important to install, and keep up-to-date, anti-virus, anti-spyware and anti-spam software.

This topic should also include discussion on Internet predators and moral issues (e.g. pornography). When programs such as e-mail or chat rooms are used we are not face to face with the person we are talking to. This presents a danger because there are people who 'prey' on innocent people, seeking contact or to scam them. In presenting this you may be able to include some examples of where this has happened, e.g. from a news clipping/article. Care should be taken not to "scare" members but rather to educate and make them aware. For access to material on computer safety issues, open the Internet Explorer icon, request a 'search engine' e.g. google.com and type in 'Internet safety for teenagers'. This should reveal many websites with varying topics that confront teenagers using computers. The need to reinforce Internet user's own moral obligations when faced with explicit, questionable or unacceptable material is important. This could be best brought into discussion in devotions. See devotional pages.

Use **Handout 2** as a quiz to reinforce learning.

Solutions to Questionnaire on **Handout 2**
1 = Through giving your personal information to a Web site that is not secure, 2 = False, 3 = Software or hardware that helps protect your computer against malicious attacks, such as computer viruses, 4 = Downloading media or software files from the Internet, 5 = Unwelcome/Unwanted commercial e-mail, 6 = Delete it without opening it or clicking any links in it, 7 = All of the above, 8 = All of the above

Teaching ideas

5. Know how to protect personal information when using a computer.

Although there are no guarantees of 100% security when it comes to using computers, there are a number of steps we should take to ensure we have the strongest possible protection against malicious software and hackers.

Members should be able to explain the importance of computer security.

Various security methods are available for home computers, e.g. virus software, firewalls, software updating, password protection. Members should also be able to explain good security practices, e.g. not giving out email address to unknown sources and keeping passwords secure, strong, complex and regularly changed. Other good practices include not downloading software from questionable or unknown websites or sending personal or financial information to unsecured or unknown sites.

Creating a ‘complex’ password is another way to protect against unwanted computer attacks when transferring information over the Internet or using online shopping or banking systems.

Passwords are part of the guarantee that others are not infiltrating personal details. When a password is requested ensure it is an authorised site. If you believe your password has been compromised you should change it immediately.

‘Hackers’ and ‘crackers’ use automated software systems capable of attempting many thousands of passwords in a short period of time. If a complex password is not used, then those trying such ‘brute force’ methods can break a password fairly easily.

A complex password incorporates a combination of the following ideas:

- lower case letters
- upper case letters
- numbers (for instance, 1, 2, 3)
- symbols (for instance, @, =, -, and so on)
- at least 7 characters in length, but more is even better.

An example of a complex password would be mY$doG_3

Password cracking software often uses substitution, i.e. your password may be J0hn where you have substituted the o for a 0 (zero). Password cracking software that is trialling many variations a second may work along John, john, J0hn substituting combinations with likely possibilities. In this case it would be stronger to have used J()hn, a less likely substitution combination.

There are a number of ways you can test the strength of a password. Microsoft provide a website to check your password http://www.microsoft.com/athome/security/privacy/password_checker.mspx

Members could visit the above site and test the strength of various password combinations. Alternatively members could write out possible passwords and as a group discuss their strengths and weaknesses.

Teaching ideas

☺ 6. Use an e-mail program to send and receive an e-mail.

To complete this component you will need access to the Internet and an e-mail address.

Options for accessing the Internet include a booking at the local library for use of their computers and the Internet, visit an Internet café or the Corps may have Internet access. Members may already have a family email address or their own email address in which case they can send an email to a nominated person, e.g. the CO, or someone who is willing to reply immediately.

As for most badge work the requirement must be completed during SAGALA and not done at home or school.

NOTE: *If members do not have their own email account they may need to use the address of someone else or have parental permission to create their own account.*

☺ 7. Know how to use a 'search engine'.

Search engines are used to locate all available sites or web pages on a given topic. Users click on each site to access the information about the topic.

There are a number of search engines available when searching the Web, such as:
www.google.com
www.yahoo.com
www.anzwers.com.au

Members should use one of the above or a search engine of their choice to find information regarding a particular topic. Suggested topics for a search include computer safety for teenagers, viruses, spyware, SAGALA, school projects, hobbies, interests, sports, news items.

Draw members attention to interesting things related to search engines, e.g. the number of sites available or possible related link sites.

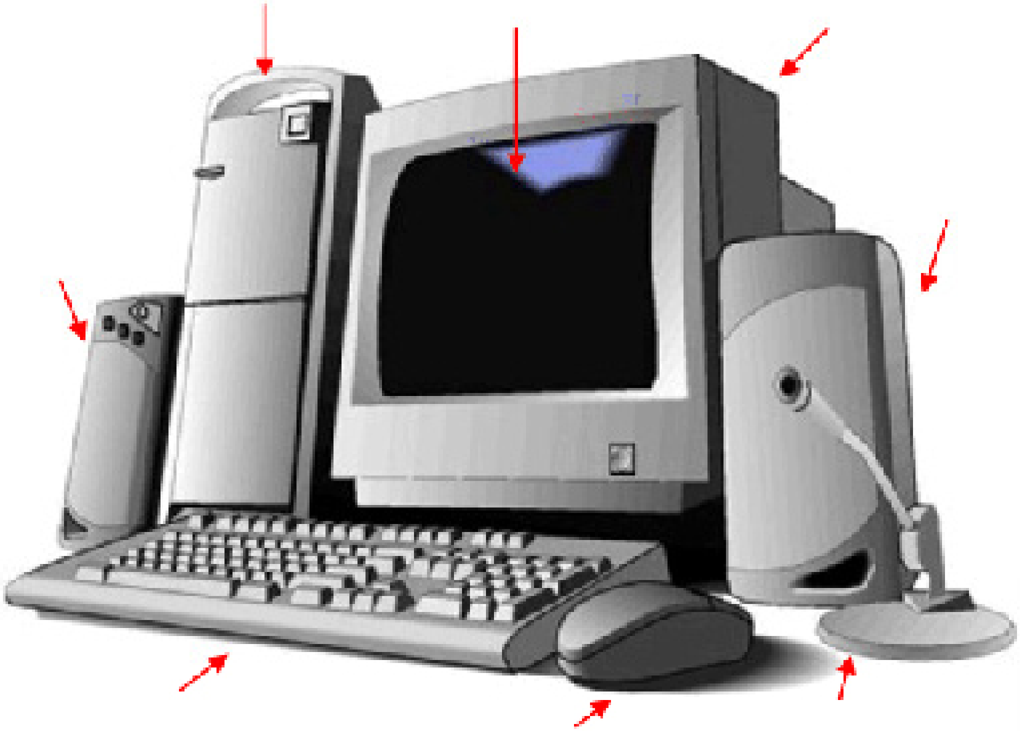
Allow the members to search for several topics but they are not expected to open sites to obtain any information other than sites containing information about computer safety.

The badge requirement simply requires members to know how to use a search engine. The leader may determine whether web pages are opened.

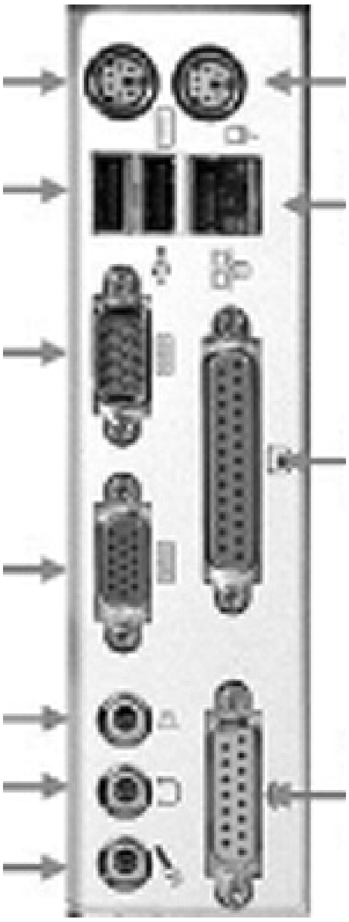
Important Note: *It is often during searching that undesirable "hits" or "links" to web pages come up. This activity should be monitored closely to avoid any explicit or potentially harmful material.*

Handout 1 - Guards/Rangers

Identify the components of the computer.



Identify the typical ports



Handout 2 - Guards/Rangers

QUIZ

1. Which of the following is *not a typical way* for worms and other computer viruses to spread?
- □ Through e-mail attachments.
- □ Through programs you download from the Internet.
- □ Through pirated software.
- □ Through giving your personal information to a Web site that is not secure.

2. After you install antivirus software, your computer is completely protected
- □ True.
- □ False.

3. What is an Internet firewall?
- □ Asbestos cloth that protects your computer from open flames.
- □ A strong password.
- □ Software or hardware that helps protect your computer against malicious attacks, such as computer viruses.
- □ A lock you can place on your computer to prevent unauthorized people from using it.

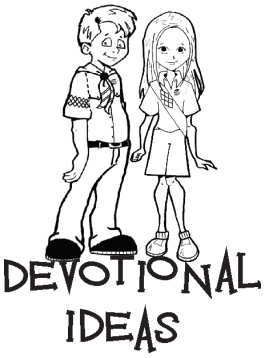
4. Which activity poses the highest risk of exposing your computer to a virus?
- □ Visiting Web sites that are not secure.
- □ Downloading media or software files from the Internet.
- □ Entering personal information or making purchases online.
- □ Allowing friends and family members to use your computer.

5. What is e-mail spam?
- □ E-mail that comes from mailing lists you've subscribed to.
- □ E-mail from your friends.
- □ Unwelcome/unwanted commercial e-mail.

6. What should you do if you receive an e-mail message that seems to be spam?
- □ Reply to it.
- □ Delete it without opening it or clicking any links in it.
- □ Click a link in the message to see who sent it so you can report them.
- □ Forward it to a friend to see what they think.

7. Why is e-mail spam destructive?
- □ It distracts you from your work.
- □ It may contain false information or attempt to scam you.
- □ It may contain a virus or other malicious software.
- □ All of the above.

8. What are some steps you can take to help protect yourself against spam?
- □ Don't give your e-mail address out to just anyone.
- □ Use up-to-date e-mail filters.
- □ Never open e-mail attachments unless you know what they are.
- □ Report spammers and scammers to authorities.
- □ All of the above



Devotional ideas

1. **Title:** The World Wide Web of Danger
Bible: Ephesians 6:11 - 18
Thought: God provides a security package for our lives
Supplies: Bible

Introduction: Ask members to think about the way computers can be attacked (e.g. worms, viruses, spam, decoded passwords, spyware). Have the members ever though that in a similar way we are open to dangers and attacks of a spiritual kind?

Explain how Satan's attacks and temptations come in many forms and from many directions. They are like 'worms' that sneak around unknown to us and cause problems, they replicate themselves without us even realising what is happening. Be aware of the 'worms' of life, those things that not only cause us to do wrong, but through us cause others to do wrong. Temptations and trials don't always come from our earthly enemies they also come from those who we consider friends like 'Trojans'. The word 'Trojan' comes from an event in ancient Greece. The people of Troy sent the Greeks a gift – a large wooden horse. What the Greeks didn't know was that the horse was full of Trojan soldiers. When the Greeks went to sleep the Trojans exited the horse and killed the Greeks as they slept. Whilst the Greeks thought the horse was a gift from friends, it turned out to be a bad experience.

'Trojans' are software programs that sneak in and cause unexpected programs or events to occur. We must guard ourselves at all times that the 'Trojans' of life don't enter in and program us to do things we wouldn't normally do.

Just as your computer needs a full security package, God has provided a security package for our lives. Read Ephesians 6:11 - 18.

- 'Truth' means that you know you are on solid ground – nothing false.
- 'Righteousness' is to reflect God's goodness and not hurt others.
- 'Readiness' is about telling others the true message of God's purpose for life.
- 'Faith' is knowing that we can trust God without hesitation.
- 'Salvation' stops us from being separated from God.
- The 'Sword' is the very truth we must share to put a stop to the falseness that is spread so quickly because it is a virus.

To be protected in life make sure you have put on the full Armour of God.

Devotional ideas

2. **Title:** Moral Dilemmas
Bible: Colossians 3:8 - 9
Thought: Living a clean life

Discuss some of the moral dangers members may face when surfing the web, e.g.

- Material that ‘pops up’ accidentally, or is an unintended result of a search request.
- Material that is intentionally searched for when no-one is looking.

Talk about what God expects us to do. In life we are faced with many decisions and we cannot always be sure we are going the best way.

It’s not our fault if we have an unexpected site turn up when we are trying to do a legitimate ‘search’. How do we overcome this? We DO NOT need to sit and read it through. We should exit the site immediately.

But what if a friend tells us about a pornographic web-site and we open it? How do you think that makes God feel?

We’ve really made a bad choice and once our eyes take something into our mind it is hard to get it out again - like a computer worm or virus. Don’t get hooked into looking at bad sites.

Here is what God says about bad habits. Read Colossians 3:8 - 9.

Remember – you might be able to fool others but you can’t fool God.