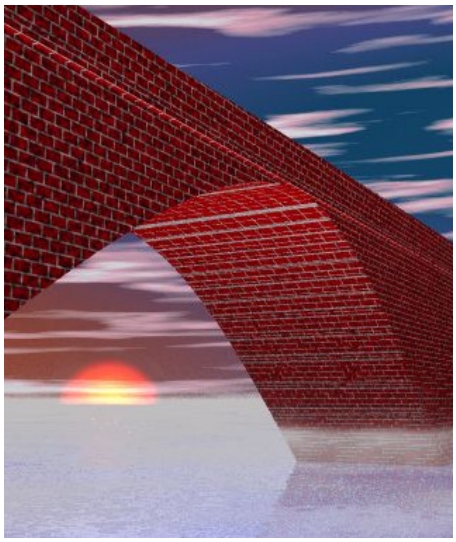
Bridging the Digital Divide

Issues in Achieving Universal Computer Literacy

Lamaan Whyte, B.A. Hons[1]

November 2007



As computers and the Internet become ever more central to our lives, a new and increasingly urgent problem is emerging – digital poverty.

Digital poverty is what happens when people in our community fail to gain – or maintain - access to computer and Internet technologies.

For most people, of course, there is no difficulty getting connected to the Internet. For students, and for most people in the workforce, the problem often seems more the other way – how to stop the Internet taking over their lives. For such people, using the Internet often seems as natural as breathing. But for others – especially seniors, people with disabilities, and for the long-term unemployed – lack of Internet access can be a particularly unpleasant form of poverty.

Without access to computers and the Internet, many people are finding themselves increasingly socially isolated, increasingly information poor, and increasingly cut off from many forms of shopping, banking and dealing with Government.

The plight of seniors is typical of the Digital Poor. Around eight out of every ten senior Territorians do not know how to use computers or the Internet[2]. Many lack the money to either buy a computer or to connect to the Internet. Of those who can afford to buy, few know how to keep themselves safe on the Internet, or how to do basic maintenance on their computers. Finally, as if none of this were bad enough, even those who learn to use computers have trouble keeping up to date with the rapid changes in technology, and often steadily fall behind.

In this paper, we look at the factors that produce the Digital Divide, and useful steps that may be taken to minimize its adverse effects.

---

[1] The author holds an honours degree from the University of Wollongong (majors in sociology and psychology, a minor in history and philosophy of science, honours in psychology, other studies in computer programming and economics). He also holds a certificate in adult education (NSW TAFE). Other training includes: accountancy, advertising, computer programming, law, management, marketing, organizational development, psychological counselling, sales and sales management, and vocational counselling. Professional experience includes about 30 years of social research, both quantitative and qualitative. Computer-specific experience includes system analysis and user- training. Volunteer teacher at Darwin Seniors Computer Club since 2003, and President since 2004.

[2] Derived from research undertaken by Council of the Ageing, Darwin, 2007.

Table of Contents

1 Executive Summary

In this paper, the term 'computer' is used quite broadly to include all information and computer technologies (ICTs), which generally includes all forms of desktop computers, laptops, Blackberries and other handhelds, and Internet-capable mobile phones.

The Digital Divide refers to the gap between those with, and those without, access to ICTs. According to the 2006 Australian Census, nearly 40% of Australian households do not have an Internet connection, with seniors, people with disabilities and people of Indigenous status[3] being particularly affected. For instance, there is evidence to suggest that as many as 80% of seniors[4] and 70% of Aboriginals[5] within the Northern Territory may be on the wrong side of the Digital Divide.

The Causes of the Digital Divide

There are many reasons why people find themselves on the wrong side of the Digital Divide. Four major reasons emerge as critical -

- The technology is expensive to buy.

  For a beginner, a new desktop computer can costs upwards of $800, while an ordinary broadband connection such as most households have[6] can cost a further $300 or more per year. For many people, especially those living on the dole or a pension, this can be a large financial hurdle to cross;

- The technology is reasonably easy to learn, but difficult to master.

  In this respect, ICT is very similar to automotive technology. Thus, while it is easy to learn to become a passenger in a car, it is very much harder to become a competant motorist, and it is very much harder again to become a good mechanic or racing driver. The practical effect of this is as follows: To use the Internet, one has to have access to a working computer. To keep a computer working involves a wide arrange of tasks, including constantly choosing and installing new hardware and software. To do this requires high levels of skills that, within workplaces, are provided by paid technicians. Home users, however, generally do not have either such skills or a resident technician, and so are often unable to keep their computers functioning;

- The Internet is a dangerous place, and it takes a lot of skill to stay safe.

  To combat the dangers of hackers, phishers and malware, computers have an ever-increasing complexity of security features, which can make even routine tasks like browsing or emailing a challenge. For many people, these challenges can become overwhelming, and beyond their capacity to handle;

- The technology keeps changing, so the need for new learning is constant.

  Using a computer is *not* like learning to ride a bike; they keep changing the bike! Even computer professionals can end up on the wrong side of the Divide within a decade or so if they stop practicing.

In combination, then, these four factors are often sufficient to keep computer and Internet technologies beyond the reach of most people outside schools and the workforce.

---

[3] Derived from a combination of 2006 Australian Census figures, and Council of the Ageing NT research.

[4] Council of the Ageing, 2007

[5] 2006 Australian Census

[6] 2006 Australian Census

The Consequences of the Digital Divide

There are two major sets of consequences -

- Digital Poverty for those on the wrong side of the Divide.

  For most people without ICT access, Digital Poverty means:

  - Reduced opportunities for communicating with their family and friends;
  - Reduced opportunities for participating in the social life of their peers;
  - Being blocked off from many otherwise convenient and advantageous ways of shopping, banking and dealing with Government;
  - Inability to access the information sources of the Web;
  - Lack of access to a wide variety of jobs and sources of self-employment.

- Losses for everyone else.

  Digital Poverty affects everyone:

  - If grandparents cannot contact their grandchildren for lack of Internet access, then the family loses;
  - If parents cannot get a job because they cannot use the Internet, then their children suffer;
  - If children cannot access a computer because their parents cannot keep it working properly, then the children's schoolwork suffers;
  - If people cannot access a computer, then businesses lose customers, and companies and Government alike are forced to spend more to communicate with them. Thus Digital Poverty hurts organizational bottom-lines.

Challenges of the Digital Divide

Just as there is no single cause, there is no single cure for the Digital Divide. What we have instead are a number of challenges, some of which can help reduce the extent of the Divide, others of which will alleviate the pain it creates. These challenges, and associated recommendations, are as follows -

- Challenge: To enable non-users to cross the Digital Divide.

  Before people will even attempt to cross the Digital Divide, first they need to know why they should try, whether it is achievable, and (finally) how to do it.

  - Recommendation 8.1.1: Create and distribute a multimedia presentation (e.g. video) outlining the issues to be considered by a person thinking of learning about computers.
  - Recommendation 8.1.2: Create a telephone Hotline, to provide basic information relevant to the caller's location – e.g. if the caller is in Jabiru, information would be specific to Jabiru residents.

- Challenge: To provide low-cost computers.

  People on low incomes need Internet-safe, low-cost computers.

  - Recommendation 8.2.1: Consideration be given to setting up an organization in the Northern Territory to refurbish computers, for supply to low-income people.
  - Recommendation 8.2.2: Consideration be given to subsidizing Internet connections for low-income people.
  - Recommendation 8.2.3: Research be undertaken to determine the evidence-based risk of malware infection and damage in home computers.
  - Recommendation 8.2.4: Formal standards be set regarding the protection needed in home computers against malware before manufacturers or retailers can claim their computers to be Internet-safe.
  - Recommendation 8.2.5: Manufacturers and retailers to be prohibited from claiming their computers to be Internet-safe if their only protection is time-limited (that is, expires after a limited time).
  - Recommendation 8.2.6: Research to be undertaken to determine the most effective form of training for home users in how to keep their computers safe on the Internet.
  - Recommendation 8.2.7: Retailers who claim their computers to be Internet-safe to be required to provide training, either by DVD, or personal training through their own organization or some other suitable organization.
  - Recommendation 8.2.8: Consideration be given to establishing a volunteer-based service helping people with disabilities install and move computers.

- Challenge: To provide appropriate training.

  Having acquired their computer, people need suitable training, especially in looking after their computers.

  People on low incomes cannot afford to hire technicians to look after their computers. Accordingly, they need access to low-cost training in computer care ('system administration' or 'sysad'). This includes customizing the operating system and software, routine maintenance, and file backup.

  - Recommendation 8.3.1: Government to establish training programs in home computer maintenance and security.
  - Recommendation 8.3.2: Consideration be given to establishing a central body to coordinate standards for home computer security and training.
  - Recommendation 8.3.3: Government to work with industry and computer clubs to identify suitable training methods and standards for home users in home computer security.

- Challenge: To provide low-cost Technical Support.

  People on low incomes need in looking after their Internet-connected computers.

- Recommendation 8.4.1: A directory to be prepared of technicians within each local area willing and able to help home users.
- Recommendation 8.4.2: A support service to be established for home users with disabilities or other special needs. This service to undertake routine maintenance and other low-level technical services.

- Challenge: To help home users stay up-to-date and enthusiastic.

  Finally, home users need to stay focused and enthusiastic even through the worst of their learning curve. In addition, they need to be able to keep up to date with computer technologies.

  - Recommendation 8.5.1.1: Public libraries and other community venues to be made available for 'social surfing' – allowing community groups such as computer clubs to surf with relaxed noise and time limits.
  - Recommendation 8.5.3.1: Community venues to be equipped with computer, projector and screen to encourage use of the facilities for 'Computer Update' meetings.
  - Recommendation 8.5.3.2: A journalist to be funded to prepare regular news bulletins for presentation at 'Computer Update' meetings.

2 Introduction

Within the Australian society, some people do not, or cannot, access computer technology. This fact is often referred to as a 'Digital Divide' – a divide or chasm between those who can access the technology, and those who can't. This paper explores the Digital Divide with reference to the Australian community in general, and the people of the Northern Territory in particular. It focuses on the general causes of the Divide, and on remedies that might reasonably be undertaken by organizations within our community .

As we shall see, the Divide is both wide and unfortunate. It is wide, in the sense that very many people within our society find themselves on its wrong side; and it is unfortunate in the sense that the people without access to computer technology are often at severe social disadvantage to everyone else. Helping people to cross the Divide is therefore a critically important social objective.

In discussing the nature of the Divide, we are confronted by many diverse problems. For a start, computer technology is wrapped in a shroud of jargon, on which there is sometimes little or no consensus as to the meaning of particular words or phrases. To avoid misunderstandings, a short glossary of frequently used terms is included in the next section.

A second problem revolves around the fact that, while it may be said that we have only one society, we have 20 million individuals, each unique, who between them face an often-bewildering multitude of problems in crossing the Divide. To a casual observer, these people may appear to coalesce into a number of apparently discrete social groups, such as 'seniors', 'people with disabilities', 'unemployed', Aboriginals', and so on. Whether the members of these nominal groups actually have very much in common so far as is the Digital Divide is concerned is an open question – one which this paper largely ignores. In this paper, our focus will be mainly on universal issues, leaving group-specific issues for exploration at some later time.

A third problem is that many of the possible solutions to the Digital Divide are beyond the reach of the non-profit sector; some solutions are in the hands of the corporate and government sectors, and sometimes even of the international community. While some of these issues will be mentioned, they are in the main beyond our purview.

Finally, there is the problem of individual ability and motivation. As we shall see, there are some people who seem to lack either the physical or mental ability to cross the Divide, and others who lack – or claim to lack – the motivation. What we do not always know, and what can sometimes be very hard to discover, is whether these 'lacks' are real – that is, inherent in the person – or some type of 'sour grapes'. For example, if a man claims to have no desire to learn about computers, is this because he has better, more interesting things to do, or is it, for example, because he realizes that he lacks ability ever to learn to use one? Such questions are largely ignored in this paper. Our major focus will be on those who are both willing and able to cross the Divide.

In short, then, the aim of this paper is to explore the general issues that create the Digital Divide, and then to identify the necessary and sufficient[7] conditions for helping those people of ability and enthusiasm to bridge it.

[7] The concept of 'necessary and sufficient' means 'doing all that is necessary, neither more nor less'. For example, suppose you wanted to walk from A to B, a distance of 10 paces. 'Sufficient' means taking each of those 10 paces; taking fewer will mean that you never get there. 'Necessary' means only doing what is needed, that is, taking the necessary 10 paces, but avoiding unnecessary actions such as flapping your arms or muttering magical incantations.

3 Terminology

The Computer Age, in which we are living, has thrown up many new words and phrases, and added new meanings to old ones. The result has been a kind of linguistic thicket through which novices must wade, and which can seem intimidating, if not indeed deeply threatening, to those unfamiliar with the field. To avoid confusion, certain terms used in this paper are now defined.

3.1 Computer

A computer may be said to be a machine or device for manipulating data according to a list of instructions[8].

Most people in Australia think of the term 'computer' as meaning either a desktop or laptop computer. In fact, however, there are many hand-held computers – examples being the BlackBerry, Apple iPhone, and many of Nokia's mobile phones. Such hand-held computers usually double as mobile phones, which means that it is a matter of personal choice whether one regards them as computers or phones; they are, in fact, both. As computers, they are entirely Internet-capable, handling emails and surfing the Internet. As compared to their big brothers, the desktops and laptops, they may have their limitations (keyboard and screen too small; lack of expansion slots), but then again, so too do their big brothers have limitations. Putting a desktop or laptop to your ear to make a phone call is not so easy, and fitting either into your pocket impossible.

For the purposes of this paper, a computer will generally be defined as any device that can be connected to the Internet for emailing and browsing the Net. This recognizes that a computer unconnected to the Internet can also be useful – but also focuses on the inescapable fact that it is the Internet that makes the Digital Divide such an important issue. To make this matter plain, we can note that people have been using computers in Australia for nearly 50 years[9], but the issue of a Digital Divide only emerged with the advent of the Internet. Hence the focus on Internet access as the critical issue.

Having said that, however, it may be noted that, while hand-held phone/computers have their place in the computer family, for most people, this place is at present very limited. For now at least, hand-helds are both too expensive and too limited in usefulness to be universally satisfactory substitutes for laptops and desk-tops. Accordingly, while recognizing that some people might choose hand-held devices, we assume that most people will choose to use either a desktop or laptop computer when attempting to bridge the Digital Divide.

3.2 Digital Divide

The term 'Digital Divide' refers to the gap between those who have access to digital technology[10] and those who do not. According to the Wikipedia[11], this term was coined sometime around 1995, and is now used to refer to either (or both) the divide between the people of different countries or to the divide within a single country. This paper focuses exclusively on the Digital Divide within a single country, Australia, with particular reference to the Northern Territory.

---

[8] For example, Wikipedia.org, dictionary.com.

[9] The first computers came to Australia in about 1960; the author worked with one of them at the time.

[10] The term 'digital technology' refers to the way that computers function, namely, by converting all data into digits of 0 and 1.

[11] http://www.wikipedia.org

3.3 Information and Communication Technology

Until recently, computers were regarded as having a single purpose: the processing of data, also called 'information'. For this reason, the technology was often referred to as 'Information Technology' (IT). With the advent of the Internet, however, people began to use computers to aid interpersonal communication, and lately the term has been expanded to 'Information and Communication Technology' (ICT).

In this paper, the terms ICT and computer technology are used interchangeably.

3.4 Home User

For the purposes of this paper, the term 'home user' refers exclusively to any computer user – effectively, any adult – who relies largely on their own resources when using computer technology. Effectively, this excludes all students at school, college or university, and many if not most people within workplaces.

4 Measuring the Digital Divide

In this section, we attempt to gain an idea of the width of the Digital Divide, namely, how many people have succeeded in crossing it, and how many have yet to make this journey. As we shall see, both sets of figures are important.

There are no reliable statistics available as to the exact number of people who have crossed the Digital Divide. We do not know, for instance, exactly how many people have sufficient skills to use a modern computer, nor how many of these can also use the Internet. The very best we can do is to make some guesses based on other statistics, such as home Internet connection.

In 2006, the Australian Bureau of Statistics included a question in the Australian Census on home Internet connection. A summary of responses to this question is given in Table 4.1. From this, we may see that most (61%) homes in Australia have access to the Internet. Within the Northern Territory and Darwin, the figures are similar: 57% for the Territory, and 63% for Darwin.

TABLE 4.1. INTERNET ACCESS IN AUSTRALIAN HOUSEHOLDS IN 2006[12]

	Australia-wide		Northern Territory		Darwin Stat Div	
Internet?	N	%	N	%	N	%
Yes	4,379,941	61%	32,103	57%	22,248	63%
No	2,530,999	35%	21,266	38%	11,474	33%
Non-response	233,156	3%	2,554	5%	1,454	4%
Total	7,144,096	100%	55,923	100%	35,176	100%

How many adults live in these households? Table 4.2 shows the number of people aged 20 years or more living in households with and without Internet access. It will be seen that 70% of people Australia-wide have Internet access at home, as compared with 58% in the Northern Territory and 68% in Darwin[13].

TABLE 4.2. ADULTS WITH HOME INTERNET ACCESS IN 2006[14]

	Australia-wide		Northern Territory		Darwin Stat Div	
Internet?	N	%	N	%	N	%
Yes	12,745,366	70%	90,360	58%	44,731	68%
No	5,071,072	28%	59,351	34%	18,698	29%
Non-response	477,074	3%	5,707	4%	2,119	3%
Total	18,293,512	100%	155,418	100%	65,548	100%

So what do such figures tell us? At first glance, not very much at all. They tell us that more two out of three Australians have access to the Internet, but they tell us nothing at all about whether any of those people have the skills, inclination or opportunity to take advantage of their access.

[12] Source: 2006 Australian Census. It will be noted that figures for Darwin refer to the Darwin Statistical Division, which includes Darwin and the Northern Suburbs, but not Palmerston.

[13] A close examination of the figures shows that differences between Australia as a whole (70%), the Northern Territory (58%), and Darwin (68%) can be largely attributed to a comparatively low level of Internet access by the Indigenous population. Exploring this issue is, however, beyond the scope of this paper.

[14] Source: 2006 Australian Census.

Perhaps, if we could only look more deeply, we might find that many – perhaps even a majority - of these people do not or cannot use their Internet connection at all.

The figures also tell us little about the remainder – the ones without Internet access. For instance, they do not tell us how many of these people make up for their lack of home Internet access by using Internet facilities at their local libraries, at their workplaces, at Internet cafes, or even at friends' homes. For all we know, many – once again, maybe even a majority – of these people use the Internet regularly, but only when away from their home.

In the end, then, these figures tell us little besides the bald fact that most people have an Internet connection at home, but that some don't.

But that is only at first glance.

At second glance, however, the figures tell us that most people either have already bridged the Digital Divide, or have convenient opportunity to bridge it any time they choose. Without spoiling the plot in the pages ahead, it will be obvious that, if people are to bridge the Divide, they will need ready access to the Internet – and a home computer is usually as 'ready' as it gets. So these figures tell us that a major portion of households have declared themselves as ready and willing to cross the Divide, whether or not they have actually done so.

A second lesson from these figures is that there will be many people in the Australian community whose need is not so much to get to the 'right' side of the Divide, as to stay there. That is, they have indeed already crossed the Divide, but now face the challenge of staying there. Learning to use a computer is not at all like learning to ride a bicycle. It is said about bicycles that once you have learned to ride them, you never forget. In the case of computer, however, the only constant is change, such that every day you have to start learning all over again[15]. So these figures tell us that there will be a large pool of people facing the challenge of constantly re-learning their computer skills.

[15] To illustrate this point, in 1961, at the time of the author's first encounter with a computer, punched cards were a common method of storing data. Since then, many different other methods of data storage have come and gone (or almost gone), including magnetic tapes, 5 ¼ inch floppies, 3 ½ inch floppies and zip drives. This rate of technological turnover – roughly one new technology every 10-12 years – has been repeated in almost every aspect of computer, and may be increasing. Accordingly, it is reasonable to assume that everybody who is using a computer today will need to do the equivalent of entirely replacing their computer skills within the next 10 years – and possibly sooner!

5 Pressures to Cross the Divide

In recent years, people without access to ICT skills have experienced ever-increasing pressures to acquire them.

5.1 Peer Pressures

One form of pressure comes from social peers such as friends at school or work, who encourage each other to start using some preferred method of communication such as chat rooms, email, VOIP, messenger services or text messages. In addition, they encourage each other to use search engines to find information – to 'google it'. In all cases, there are 'social sanctions' (penalties) for not doing complying with this pressure, namely, the threat of being excluded from the group by being unable to participate in its favourite activities.

5.2 Family Pressures

Another form of pressure comes from family members, who wish to be able to communicate with each other by their favourite communication method – once again, chat rooms, email, etc. This form of pressure is widely experienced by seniors, who often find themselves under pressure from their children and grandchildren to adopt ICT technologies.

5.3 Job Pressures

Not all jobs require ICT skills, but many do, especially amongst the 'better' (that is, higher prestige, higher pay and/or more popular) kind. Thus people without ICT skills, or with inadequate ICT skills, can either find themselves unable to get a 'better' job, or even unable to get themselves a job at all.

It might be noted that many corporations now accept job applications only online; even jobs with no ICT component (such as cleaning jobs, or supermarket shelf-filling jobs) have to be applied for online.

5.4 Work-at-Home Pressures

Many people prefer to work at home, either in a home-based job, or in some form of self-employment. Examples are: parents who have to look after children; people with mobility disabilities such that they are unable to attend a normal workplace; people in remote locations. While there are work-at-home jobs that do not require ICT skills, they are few and far between, and are generally poorly paying. By contrast, there are many well-paying opportunities for people with adequate ICT skills.

5.5 Corporate Pressures

Companies provide a variety of pressures on consumers to acquire ICT skills, such as:

- Since the mid-1990's, banks have shifted many of their services online (that is, on the Internet), with the result that many of their services are now *only* available to people who can use the Internet;
- Airlines routinely offer lower airfares to people who book their tickets online;
- Many retailers offer lower prices and sometimes larger ranges to their online customers.

In short, people without access to the Internet have restricted access to goods and services, and often pay more for what they buy.

It might be noted that offline retail sales have been largely static since 1990, while online retail sales have been growing at a steady 30-35% per annum.

5.6 Government Pressures

Governmental departments and agencies are using the Internet to communicate with their public. The Tax Office invites people to submit their tax returns electronically (i.e. via the Internet); Centrelink encourages people to lodge their forms online; and Government departments and politicians of all persuasions use websites as a means of helping to answer people's questions. The incentive for them to do this is simple: it is cheaper for Government than traditional communication methods. Put simply, using ICT allows Government to drive the tax dollar further.

5.7 Medical Pressures

Further pressure comes from health professionals. This concerns the use of computers for entertainment purposes, especially for playing games, playing music, and looking at photos. This comes from the fact that there seems to be causal links between these activities and individual health and well-being[16] – though the exact nature of these links is at present poorly understood.

At first glance, one might wonder whether computer games are all that important; after all, human beings have managed to survive as a species for quite a few years now without them. Evidence is mounting, however, that playing computer games can have positive health consequences. For instance, regular playing of certain kinds of computer games has shown to be associated with delaying the onset and severity of degenerative mental diseases such as Alzheimer. While there are undoubtedly alternatives to playing computer games in delaying the onset of such diseases, these alternatives are often more costly to provide, and often less convenient.

5.8 Affective Pressures

The pressures described above – from other people and from circumstances – can be severe enough, but to these can be added a further pressure, that from within. These we may call emotional or affective pressures. These are the pressures that can make a person feel deprived or inadequate if they find themselves on the wrong side of the Digital Divide.

All of us are, at one level or another, deprived or inadequate. Most of us, for instance, have been deprived of the chance to climb Mount Everest, or to dive in a bathysphere into the ocean depths, or to walk on the Moon – and most of us are quite content with such deprivation. Most of us consider such things to be too scary, or an unwanted distraction from doing other more enjoyable things.

For many people, however, being on the wrong side of the Digital Divide is a highly uncomfortable experience, leading not only to real economical and social losses, but also to loss of self-confidence, feelings of relative deprivation, and a sense of lack of social and economic opportunities.

[16] This topic is reported on regularly by NewScientist.com.

6 Causes of the Digital Divide

There are many reasons why some people find themselves on the wrong side of the Digital Divide. These are a few of them:

6.1 Lack of Motivation

Crossing the Digital Divide is not easy. For most people, it involves both financial expense, and significant effort at learning. Without a good reason for making the journey, few people take it[17].

There are two aspects to lack of motivation. The first is a general disinclination to involve oneself with computers in any shape or form. People who feel this way are often 'hands on' and 'out-of-doors', and ICT technology represents an aspect of the world that they dislike, and will ignore completely if given their druthers.

The second aspect of lack of motivation can be described as, "I haven't found a use for ICT … yet". People lacking this type of motivation are not actually hostile to the technology; they just haven't found a major use for it so far. In the jargon, they haven't yet found their 'killer app' – this being an 'app' (that is, 'application' or computer program) that 'they would kill for'.

Either way, people with a lack of motivation see no personal benefit in crossing to the other side of the Divide.

6.2 Lack of Sufficient Intelligence

To learn ICT skills not only requires a teacher, but also sufficient intelligence on the part of the student. Not all people have sufficient intelligence[18].

Intelligence has been defined as an individual's ability "act purposefully, to think rationally, and to deal effectively with his environment[19]". When it comes to using computers, intelligence is clearly an important issue with determines, first of all as to whether an individual can use one at all, and secondly, as to the level of sophistication the individual can bring to that usage.

In the most basic level, learning to use a computer requires only a very few skills, such as knowing how to: switch the computer on; recognize when the operating system has loaded; find the icon for one's email program; and read and write emails. None of this is particularly intellectually demanding. Based on the writer's observations, it is reasonable to assume that somewhere around 85% of people could handle tasks such as these.

The situation changes, however, when it comes to more advanced skills. In addition to knowing how to handle emails, home users generally also need to know how to look after their computers, and to do this in an effective and efficient manner. Such skills include: being able to locate, evaluate and install software; being able to customize the operating system; being able to plan and undertake routine maintenance; and being able to back up files and drives. All of these tasks are essential to maintaining computers in good working order; all are essential for helping keep people on the 'right' side of the Digital Divide; and all are intellectually challenging. While the writer knows of no adequate research into this field, his experience suggests that it is possible that as many as three out of four people would have great difficulty in mastering them adequately without great personal effort (which brings us back to the earlier topic of

[17] This can be seen in the very low percentages of homes that owned a computer in pre-Internet days, or even in the early days of the Internet.

[18] The following website offers a quick guide to the issues discussed, and terminology used, in this section: http://wilderdom.com/intelligence/IQWhatScoresMean.html

[19] David Weschler, cited in http://en.wikipedia.org/wiki/Intelligence.

motivation). In other words, it is this writer's working hypothesis that only 25% of people have the intellectual capacity to keep themselves on the 'right' side of the Digital Divide without either extraordinary dedication, or substantial help from technicians or other highly skilled people.

6.3 Lack of Hardware

In order to be on the right side of the Divide, one needs suitable hardware – a personal computer (PC) for instance. In Australia, new PCs suitable for normal home use can be purchased for well under $1,000. Low-income people can buy refurbished PCs for as little as $200 or $300. Thus hardware is somewhat affordable to most people within Australia – provided that they are motivated to budget for it.

6.4 Lack of Internet Access

Having acquired suitable hardware, the next challenge is to connect it to the Internet. In the major cities, Internet connections are readily available, with a choice of dial-up, ADSL, wireless or satellite. Of these, dial-up is the cheapest option, while satellite is by far the most expensive. In more remote areas, the choice may be limited to satellite. Thus, Internet access can be regarded as available almost everywhere within Australia.

Whether it is affordable by people on low incomes, however, is an entirely different matter.

There are many different ways to connect to the Internet, each with its own associated costs. All are expensive for people on low incomes. A person connecting for up to five hours each day using a Telstra dial-up service, for example, would pay at least $40 per month (including land-line connection), a great sum of money for an unemployed person or a pensioner.

There is one non-profit organization that tries to keep connection costs down, TadAustConnect.org.au. This organization offers dial-up and broadband services to 'people with disabilities, the elderly and veterans'. Their dial-up service is, for the first year, marginally cheaper than Telstra (though their terms of service are more generous), and significantly cheaper thereafter. Their broadband service, though generous in its download limit, is much the same price. In the end, therefore, this organization makes very little difference to the cost of Internet access.

6.5 Lack of Internet Security

Having bought one's PC and signed up with an ISP, the next hurdle for a home user is to make it and its users safe against Internet viruses and other malware[20]. This subject is called 'Internet security'.

The issue of Internet security is of enormous complexity, and almost intractable difficulty. Indeed, it is the notional 800 kg gorilla on the bridge across the Digital Divide. It is a gorilla so large and so ferocious-looking that it has cowed many would-be users into abandoning the Internet, and seems to have reduced the Australian Government almost to a quivering wreck. Accordingly, it is most important that we examine it most carefully to understand why it is so difficult, and what can – and should – be done about it.

The Situation is Serious

The first thing to understand about Internet security is that it is indeed serious.

About 60% of home users suffer damage to their computer files from malware[21] such as viruses and spyware, with some suffering damage so severe that they find themselves obliged to rebuild

[20] Malware is a term used to encompass all forms of harmful software to be found on the Internet, such as viruses, spyware, trojans and worms.

their operating system, or even to replace their computers. These losses can involve more than mere passing inconveniences. Users often suffer financial losses: from disruption to home-based businesses, and/or from hiring technicians or buying new computers. Sometimes they also suffer emotionally, such as from depression at loss of irreplaceable family photos or from the stress of their financial losses. In one extreme case, the author has sat next to a person as they had a stroke brought on by the emotional stresses of a malware attack.

Finding suitable statistics for calculating a reliable risk assessment seems to be quite impossible; whether deliberately or otherwise, research organizations seem reluctant to publish them. From such information as is available, however, the author calculates as follows: 60% of home users (as compared to 60% of government users and 40% of business users) are inherently vulnerable to malware, having a 50% chance of being infected within any given year. If a home user is infected, that user has an 80% chance of sustaining damage to their computer or software which they cannot easily fix (which in turn can lead to expensive technician's bills, or even the need for a new computer), plus a further 10% to 20% chance of sustaining some other major loss or inconvenience (e.g. having the money taken out of their bank account, and/or losing their credit rating)[22].

Not all damage comes from malware. Some comes from what is sometimes called 'Code-18' problems[23]: problems created by users who do silly things such as replying to spam emails. Avoiding malware, for home users, usually involves installing a suitable range of security software (firewalls, antivirus programs and such like); avoiding Code 18 problems means learning 'NetSmarts', the rat-cunning skills of survival on the Internet.

The Consequences of Malware Infection

We have seen some of the consequences of malware infection: file loss, financial loss, emotional stress, and physical illness. What else happens when computers become infected?

When a computer becomes infected with malware, the usual result is that it will slow down (sometimes dramatically) and begin to behave erratically. At this point, computer owners will face a cascade of decisions:

1. They may attempt to clean out the infection themselves, personally. In order to be able to do this, they will have to have, or to acquire, a huge array of skills, almost equivalent to that of a professional computer technician, which will involve the equivalent of one or two years full time study. Many owners will decide that this effort is out of proportion to the benefit they get from their computer, so they will move to their next option -
2. Having decided not to fix the problem themselves, they consider hiring a technician. Businesses and governments do this as a matter of course, but for home users, this may not be so easy. People on low incomes may decide a technician to be unaffordable, while people in remote locations may find themselves unable to find one at all; either way, they choose the next option -

[21] E.g. http://tinyurl.com/2ba5jq. Very many surveys, using a variety of measures and criteria, have reported that approximately 60% of home user and Government computers are infected with malware at any given time.

[22] This assessment is the author's. It is based on a study of statistics published on the Internet and experience in helping members of the computer club deal with infections.

[23] Code-18: a computer glitch originating 18 cm in front of the monitor (i.e. in the user's head).

3. Unable or unwilling to get a technician, many people choose to buy a new computer, and to throw the old one away[24]. People on low incomes, however, may decide that this is unaffordable, and so they move on yet again –
4. Unable to buy a new computer, they decide that computing is too expensive, and shift themselves back over to the wrong side of the Digital Divide. In other words, despite all the good work of social welfare agencies and benevolent organizations such as GreenPC[25] to make computers available to low income people, lack of security support can render their efforts useless.

In short, lack of inadequate security protection on individual computers provide common reasons for keeping people remaining on, or returning to, the wrong side of the Digital Divide. There is no clear evidence as to how often this happens. Two or three years ago, however, the author saw a report of some research undertaken a few years ago in the USA which indicated that about 40% of low-income users abandoned use of the Internet following malware damage to their computers. Whether that was a statistical anomaly, a one-off event, or part of a continuing trend is not known.

(In major towns and cities, some people deal with their inability to keep their computer suitably protected on the Internet by using computers at Internet cafes or public libraries, trusting - probably naively[26] - that these computers are safe.)

Sourcing Advice on Home Security

One of the most serious and potentially disastrous problem facing home users as they cross the Digital Divide is to find reliable, understandable advice about Internet security in general, and security software in particular.

There is, of course, an endless supply of people willing to provide advice to the novice user – computer salespeople, computer technicians, and relatives, friends and acquaintances by the score. Rarely do any of these people have any particular expertise in Internet security for home computers. Not even technicians necessarily have expertise in this area. Charles Darwin University's certificate and diploma courses in information technology offer no subjects at all in home computer security. Indeed, it seems that there are very few if any courses in this subject offered anywhere in Australia.

There is also an endless supply of security advice available on the Internet. The quality of this advice, however, varies from excellent to dreadful, with home users facing a huge challenge in separating out the good from the bad. One of the major problems facing the home user is that many of these advisory sites have financial axes to grind, such as selling products, or committing scams. Indeed, scams are a major source of concern here. Spywarewarrior.com lists just twelve 'good' antispyware programs, but over 200 'bad' ones.

So where are the genuine security experts?

The place where Internet security experts gather is, of course, the Internet. They are found in countless websites, forums and discussion groups. Some can be found at university websites,

---

[24] As Greenpeace has pointed out, computers are filled with a lethal mix of heavy metals and other toxic substances. Unless it is put into the hands of a competent recycling company (none of which exists in the Northern Territory), throwing a computer away creates an environmental disaster. The fact that computers are sold in a condition that makes them liable to be thrown away unnecessarily could be seen as placing a measure of irresponsibility on the retailers that sell them, and on Governments that do not regulate the retailers.

[25] www.greenpc.net.au

[26] Given that 60% of public sector computers are known to be infected at any given time, and that public libraries are by definition part of the public sector, it is reasonable to assume that 60% of city councils are offering their clients unsafe computers on which to do their banking and their shopping.

offering advice to their students and to the public. When many university websites recommend particular websites as good sources of information, such sites can be regarded as expert sites. If these expert sites then say something about home computer security – and all agree - then what they say can be taken as authoritative, even definitive.

Finding these expert sites is, of course, a huge task, which few home users are willing to tackle. Making sense of the advice given by these experts is an equally hard task, sometimes requiring the home user to be even more of an expert than the experts.

One of the most highly regarded security websites relevant to home users is Spywarewarrior.com[27]. This site shortlists eight different antispyware programs from which the user is instructed to choose at least two. It warns, however, "you should not rely exclusively on this short list … [but] investigate and test a range of reputable anti-spyware programs to find the programs that are best suited to your own privacy and security needs." Exactly how a home user is to do this is not discussed. The site seems to assume that its readers are at least as expert in Internet security as the site's writers – if indeed not more so!

Thus we are lead to consideration of the proper role of experts in helping people secure their computers.

There seem to be two opinions as to how experts should share their expertise. The first point of view is that demonstrated by one of the Australian Government's websites[28], StaySmartOnline.gov.au, which is to provide no practical information at all. The site does not actually say so, but its rationale seems to be that home users are to be discouraged from learning anything about securing their computers except how to buy the necessary software from members of the Internet Industry Association (that is, from commercial software manufacturers).

The second view is that demonstrated by Spywarewarrior.com. Sites such as this seem to believe that the role of the expert is to provide lots of facts and statistics in the expectation that possession of these will somehow turn home users into security experts. Then, or so the theory goes, the home user can make expert decisions and perform expert actions.

Are these reasonable opinions? As the reader may guess, this paper argues that neither of these sites offers any practical help to people struggling to cross the Digital Divide[29].

Consider how it would be if each of these sites were a public hospital, and a sick person were to arrive at Casualty. The Government site would say, "I'm sorry; we don't fix sick people. You'll have to go to a private hospital." By contrast, Spywarewarrior would say, "Welcome! Here are eight prescriptions and a list of all available medicines. Take any two, and then join me in the lecture theatre if you survive."

In effect, we see here one of the two major besetting weaknesses of most expert advisors online: an implicit belief that home users have unlimited time, motivation, experience and intellectual brilliance, and need only a little more knowledge to be better able than security experts to distinguish between nearly identical security programs. As we have seen earlier, absolutely none of these assumptions are valid.

---

[27] It may be noted that Spywarewarrior.com deals specifically with software suitable for home users, and makes no mention of software intended exclusively for corporate networks or other non-home computers. Accordingly, it is reasonable to examine this site as a typical example of a well-regarded home user site.

[28] At least as demonstrated by StaySmartOnline.gov.au. See Appendix A for a detailed discussion of this and other Government sites.

[29] To give credit where credit is due, the Spywarewarrior.com site does do one thing well, and this it does extremely well; it provides a source of expert advice for budding and current security experts.

They also seem to have very limited understanding of how their advice might be taken. For instance, after committing itself to a short-list of eight antispyware programs, Spywarewarrior.com then undoes all its good efforts by inviting readers to examine other 'reputable' programs. What exactly does it mean by 'reputable'? It does not say. Ordinary home users, however, know exactly how to identify 'reputable' software, but it leads to results that can be the exact opposite of what Spywarewarrior.com intends!

People tend to have an implicit theory of merchandise in their head, in which quality and reputation are judged largely by weight of advertising. That is, they judge both the quality and the reputation of products that they normally buy by the number and size or impressiveness of its advertising. They do this with all the products they buy – soap powder, cars, breakfast cereal – and they do it too with Internet security software. So if they see a security product well advertised – say, by a nice big colourful webpage – they automatically rank it as reputable[30].

All of this is entirely natural and proper. It is what they learned to do as small children, and it is a strategy that has stood them in good stead throughout their life. Why should they change now? Thus any scam software program that can afford to buy itself a nice big colourful webpage can instantly acquire reputability. By recommending the use of 'reputable' programs, security websites effectively recommend the use of scam software.

In the end, these websites, and others like them, are suitable for very few home users. As discussed above, very few home users have time, inclination or (in most cases) the intellectual wherewithal to become security experts. In addition, many lack the financial resources to be able to rely on commercial software.

NetSmarts

Even with all necessary security features for their computer, users are still not safe.

In order to be safe on the Internet, people have to learn, and then apply, a whole battery of skills, plus a range of 'does and don'ts' sometimes called 'Net Smarts' (in analogy to 'street smarts'). For instance -

- How to use all the security devices and software installed on their computer. To work properly, these devices require the user to take appropriate actions almost continuously during the times when connected to the Internet. In addition, usually once a week, users have to spend an hour or so updating their software and scanning their computers. Then, once every few months, further maintenance activities are required. Users have to know how to do all of this, and then actually organize themselves so that they actually do it. For all but the most enthusiastic of users, this is a very big ask!
- Even when the security devices are all purring contentedly, still users cannot relax. The Internet has traps abounding for unwary players in the form of all manner of email scams (phishing, Nigerian and Viagra are common examples), plus all manner of dangerous and fake websites. Plus of course untold traps for youngsters, for instance in the form of predators in chat rooms. In every case, the user has to know exactly what to do – and then do it!

Once again, the learning curve is steep, and the penalties for not learning, or not applying one's learning, huge.

[30] This theory derives in part from a reading of the psychological literature relevant to consumer behaviour, and partly on the author's experience as a marketing researcher and teacher of home users.

6.6 Lack of Learning Opportunity

To be able to access ICT technologies, one needs to know how, and learning to use it effectively and safely requires access to a teacher. For some people, finding an affordable convenient teacher is not easy.

Broadly speaking, ICT teachers fall into three groups:

- Teachers within teaching organizations such as schools, universities, colleges, and computer clubs. In addition, some public libraries employ ICT teachers, at least within the Northern Territory;
- Independent professional teachers – usually computer technicians who combine technical work with their teaching;
- Teachers who work through ICT technology itself – for instance, through Internet webpages or through interactive CDs. For beginners, these are never an ideal solution, but for more advanced students, they can be perfect.

In addition, there are, of course, friends or family members willing to devote the necessary time to help each other as teachers; these are, however, few and far between. In addition, there are countless others willing to flaunt their personal ICT prowess in the guise of teaching, although these can hardly be called teachers.

The next problem facing the person wishing to learn ICT skills is to find a suitable course (field of study). The field of ICT technology is far too large for any one course to cover everything; indeed, it is now far too large for any one person to know it all. So people have to, first, know what it is that they wish to learn, and then find somebody willing to teach it.

For home users, there are five groups of courses they will need to study[31]:

1. 'Beginners' – first, home users must learn the 'basics' of using a computer: how to switch it on and off, how to use the Desktop, and how to cut and paste. Until people learn the basics, they are at a severe disadvantage when it comes to learning more advanced skills;
2. System Administrator (Sysad) skills. In large organizations, the person who looks after the organizations computer is traditionally called a 'system administrator[32]', or 'sysad' for short. Without an active system administrator, computers sooner or later cease to work properly. Just as organizational computers need a system administrator, so too do home computers. And just as organizational sysads need to learn their craft, so too do home sysads. For home sysads, skills to be learned include basic troubleshooting, installing and uninstalling software, and installing and maintaining an adequate Internet security system. The skills needed to be an effective home sysad are quite extensive, and approach those needed to be a professional technician. To become an effective home sysad, therefore, represents quite an investment of time and effort on the part of a home user – one that not all home users are willing or able to make. Yet without somebody – home user or paid technician – acting as home sysad, the home computer

[31] An observant reader might notice that the following list does not include any mention of a course on hardware maintenance. The reason for this is that, while some people find such skills enjoyable to learn about or to practice, they are rarely if ever relevant in the context of bridging the Digital Divide.

[32] Windows operating systems are designed to be looked after by System Administrators. You can see this for yourself (if you are game enough) by deleting a few random files in your computer's Windows folder so that your computer no longer works properly. Thereafter, whenever the Windows system encounters a problem, a message will appear instructing you to 'contact your System Administrator'.

will soon cease to function properly, thus moving all of its users to the wrong side of the Digital Divide;

3. Basic Internet security. Anybody who uses the Internet needs to know about basic security. There are two aspects to this, which we can call 'SoftSmarts' and 'NetSmarts'. NetSmarts is a widely used term meaning 'knowing how to recognize dangers when on the 'Net (Internet), and being smart enough to know how to deal with them'. SoftSmarts is a neologism that means 'knowing how to recognize that your computer's security software is warning you of danger, and being smart enough to know what to do next'. All Internet users, young, old and in-between, need to become NetSmart and SoftSmart.
4. Routine maintenance: like motor cars, computers require suitable care to keep on working properly. Such care has to be provided very regularly – usually weekly – but it is not a particularly difficult task, and does not require the attention of a highly skilled home sysad. Nevertheless, the person who is to do it has to be shown how.
5. Courses dealing with particular applications. 'Applications' are the software programs that allow you to do interesting things with a computer, such as send emails, write letters, make movies, or download music. Application courses provide the skills needed to use specific types of software - email clients, word processors, movie makers, web browsers and so on.

To understand how all of this plays out in helping people stay on the right side of the Digital Divide, we might draw an analogy here with the issues of being able to use automobile technologies.

To use an automobile, one can choose to be either a passenger or a driver. Computer technologies are much the same. In this analogy, a 'computer passenger' is a person who gains benefit from the technology without any particular technical skill, without doing any particular hard work, but of necessity having to follow certain safety rules. For instance, in a motor car, a passenger just sits there, and is conveyed from place to place – but still has to observe safety rules, such as not opening the door or unbuckling seat belts while the car is moving. Much the same is true for computer passengers: they just sit there while the computer does its thing … but all the time they must avoid doing unsafe things like not giving their real name in chat rooms, and not clicking on links in spam emails[33].

Meanwhile, no matter how safety conscious the passengers may be, somebody has to drive the vehicle/computer, and to do maintenance on it, and generally do everything to make sure that it does its job. In automotive technology, this requires a driver and a mechanic; in ICT technology, it requires a sysad and a technician. The driver/sysad make sure the vehicle/computer goes where it is supposed to go; the mechanic/technician looks after the hardware.

To become either a driver or a sysad involves learning a huge array of skills. To become a driver, one must learn not only how to wiggle a steering wheel and dance on the pedals, but also learn the road rules and how to navigate around one's local neighbourhood and city, plus learn how to read street signs and street directories, plus how to anticipate the behaviour of other drivers. According to Northern Territory law, it takes at least a year (two years for

[33] At first glance, this analogy may seem to have a weakness: in a car, passengers really can just sit there and do nothing. Computer passengers, by contrast, have to know how to handle the particular application they are using. So it may seem that they are more active than car passengers. In the overall scheme of using a computer, however, a computer passenger hard at work using a spreadsheet is no more involved in the management of the computer than a car passenger who happened to be listening to an iPod is involved in the management of the car.

younger drivers) to become skilled enough not to need P Plates. Judging by their premiums, nsurance companies, by contrast, seem to think that it takes seven years to become a reasonably skilled driver. As we have seen, learning to become a skilled ICT user is an equally large task, and so it probably takes an equivalently long time.

(The major difference between motor car and computer technologies, in our current context, is that if somebody makes a mistake in a cars somebody is likely to die (worldwide, about two are killed on the road every second), while if somebody makes a mistake on a computer, the worst that can happen usually is that somebody will lose money.)

The point of this analogy is this: if people are to have access to ICT technology, they must not only have access to the means of learning how to use the technology, they must also have access to the means of learning how to keep it safe. For people on low incomes, and for people in remote locations, such access can be very hard to find.

Use of Internet and CD learning systems can be very useful for people on low incomes and in remote locations to revise basic skills, and to learn more advanced skills, but they are rarely if ever satisfactory for first-time beginners. For these people, 'live courses' either one-on-one or in a class, seem to be necessary. The criteria for a successful beginners course will be discussed later.

6.7 Lack of Update Information

One of the realities of life on the right side of the Digital Divide is the diminishing value of one's ICT knowledge and skills. As technology changes, everything one knows and can do becomes gradually useless. In the past year, we have seen five major PC operating systems become either obsolete or obsolescent (Windows 95, 98, Me, 2x and XP); floppy disks give way to USB flash drives, and Internet security threats have changed from a mild nuisance to major financial threats. To stay up-to-date with ICT technology requires constant effort.

People wishing to stay up-to-date in the ICT world face a major problem, which is that there is just so much new information to absorb. Every day brings news of new gadgets, new software, new methods; staying fully up-to-date becomes incompatible with 'having a life'. Some people react by simply giving up. They use the technology they are most familiar with (MSDOS or Windows 3.1, for instance), and refuse to advance any further. Slowly, they fall back to the wrong side of the Digital Divide.

6.8 Lack of Social Support

A final, but in many ways a most critical obstacle to being able to cross the Digital Divide can be lack of social support, that is, the lack of other people to help and guide one across the Divide.

There are two aspects to social support. These we may loosely term 'peer pressure', and 'peer support'. Peer pressure refers to the pressure that other people (technically, significant others' – friends, family, workplace colleagues, etc.) apply to each other to do whatever is considered 'the right thing'. For instance, peer pressure might be used to 'strongly encourage' a person to connect themselves to the Internet, or to undertake a particular study program, or to do the necessary practice to master a particular skill. Peer support is much the same, except that it is non-judgmental, and carries no sanctions. For example, suppose your good friend Fred is encouraging you to acquire a computer. If he does this indicating that he would be disappointed in you, or otherwise unhappy if you don't, it is 'peer pressure'; otherwise it is 'peer support'.

To see how this works in practice, consider a social group such as friends at school or work. Such friends can be expected, from time to time, to encourage each other to start using some preferred method of communication such as chat rooms, email, VOIP, messenger services or text messages. In addition, they encourage each other to use search engines to find information – to 'google it'. In all cases, there are 'social sanctions' (penalties) for not doing complying with

this pressure, namely, the threat of being excluded from the group by being unable to participate in its favourite activities.

Many people learn their ICT skills in kindergarten, or primary school, or in high school, university or college; in each of these places there are many people willing to provide peer pressure and support – and focused themselves very much on the issues relevant to the pressure and support. The same is true for people in the workplace. Home users, however, are often entirely on their own – or are surrounded by negative pressures and support. This is different from in other environments. In a school environment, for instance, all students face a common challenge of mastering a certain curriculum, so naturally their pressure and support to each other tends to be to rise to the challenge, not to avoid it. In home environments, however, this is not always the case. There, people can be too busy telling each other that they are too stupid/young/old (whatever) to learn a new technology to apply positive support, or can be too demanding of each other's time or attention to allow them to pay attention to their studies.

Just as learning to drive a motorcar requires that one sit at the driver's wheel and practice, so learning to drive a computer involves much the same. If other family members do not actively encourage – let alone actively discourage! - a person from doing the necessary practice, chances are that they will never learn the necessary skills.

If the skills to be learned are simple – for instance, the 'passenger' skills suggested above – strong motivation may easily overcome lack of peer pressure and peer support. If however, the skills to be learned are difficult – such as those of a home sysad – can easily prove the difference between success and failure. In such circumstances, a supportive home environment for those who live with other people, or a computer club for those who don't, may be an essential ingredient for success in crossing the Digital Divide.

6.9 In Summary

The Digital Divide, in the context of this paper, refers to the ability of individuals to learn how to access ICT technologies. There are strong pressures on them to do this, from family, friends, business and government. The obstacles facing many of them, especially those with low incomes, and those who live in remote locations, are formidable. Of particular importance for subsequent discussions are the needs for effective Internet security protection, and a suitably skilled sysad (system administrator) to help maintain equipment in working order.

7 The Community Challenge

As we saw in the preceding section, the obstacles to bridging the Digital Divide are many, and, for some people at least, the benefits few or unknown. As will by now be clear, relatively few people will be able to make *and sustain* the crossing without at least a little help from the rest of the community.

So who should provide this help?

It is easy in a paper such as this to say, "Oh, Government should do it!" When things go wrong, it is obviously the fault of the Government, so it follows that the Government should clear up its own mess. Strangely enough, however, Government does not always see it that way, especially when it sees people surfing the Net for pretty pictures or chatting online with their friends. At such moments, it starts thinking that maybe the people involved should set up their own self-help groups – for instance, organizations such as the many seniors computer clubs around Australia.

As this paper has attempted to demonstrate, however, the Digital Divide is a problem not only for the people involved, but also for everybody. When one person is on the wrong side of the Digital Divide, *everybody* is affected: the person's family and friends, the larger community, business and Government itself. Everybody. It is reasonable, therefore, for everybody to share the load of helping the whole community to access computer technology.

One way – perhaps the best way - of sharing the load is to use a mix of suitable leadership, suitable material resources, and lots of community volunteers. Between them, government and industry can best provide the necessary material and leadership resources, but where does one get the volunteers? The answer is computer clubs.

The computer club of which the author is currently president, Darwin Seniors Computer Club, is one of over a hundred such clubs in Australia, with many more similar organizations around the world. For well over a decade, these and similar organizations have been exploring ways of using volunteer labour to help home users bridge the Digital Divide. The use of volunteers turns what would otherwise be a financially Herculean task into one that can be considered as large but doable.

From a study of the activities of computer clubs, we may learn:

- Without help from Government or industry, and without proper leadership, computer clubs are generally unable to do anything useful;
- Properly lead and resourced, however, computer clubs are very good at marshalling lots of volunteers. These volunteers are suitable for teaching at the beginner level, for low-level technician's work, and for a variety of other socially useful but technically undemanding tasks;
- The nature of their activities means that the resources they need are similar in nature, if not necessarily in scale, to those needed by any other teaching facility, such as schools and colleges. For example, they need dedicated classrooms, with computers, projector, white boards, and so on; workshops for computer maintenance; storage facilities; and office space;
- The leadership they need includes the normal leadership of any organization (with characteristics such as drive, vision, etc), plus also technical leadership, in the sense of being able to encourage technical excellence (at an level appropriate to the organization's activities);

- Volunteers alone are not sufficient. To provide all the technical skills, at the time when they are needed, and in the places where they are needed, will of necessity require use of paid personnel.

8 Building Bridges

In this section, we consider how we can best help people cross the Digital Divide. In the process, we will need to ask ourselves how this can best be done; what resources will be needed; and who is to do the necessary work.

To help us consider such questions, let us follow the progress of a hypothetical family – we'll call them Bill and Sue Jones - as they progress from non-users to users of computer technology.

8.1 Information

Before the Joneses will even begin to think about crossing the Divide, they will need lots of information, such as:

- **Which** type of computer technologies should they acquire and learn to use?
- **How much** will cost them to acquire and learn about ICT technologies?
- **What** are their options for getting suitable ICT equipment, learning to use it, and then keeping it functioning and safe?
- **How long** will all of this take?
- **Why** should they bother? What advantages will they gain by being able to access and use ICT technologies?

There are many ways that this information could be provided, including:

Idea 8.1.1 – Information CD

Recommendation: A multi-media presentation (e.g. a video) to be prepared outlining the issues to be considered by a person thinking of crossing the Digital Divide – e.g. options for accessing a computer (buy one new or recycled, use public library facilities, etc); what you can do with a computer, and outlining the security risks. In other words, a 'perils and joys' look at using computers.

The Australian Government has a free video[34] for people who have decided to cross the Divide; this could be the 'prequel'. It could be distributed through websites such as Seniors.gov.au, and through public libraries and computer clubs.

(A booklet version of this video would also be useful for people lacking access to video players, and for the hearing impaired.)

Personnel: This would be a one-off event: the video would be written, produced and distributed. (The author has written a basic outline for this video.)

Volunteers: not needed.

Resources needed: storage and distribution facilities.

Idea 8.1.2 – Information Hotline

Recommendation: A telephone number, to be manned by volunteers, could be set up so the Jones's could call for information. Information should be:

- 'locally oriented', that is, it should focus on providing the Joneses with local sources of information, training and support as appropriate, for example, to their postcode;

[34] "Connecting with Computers", Department of Education, Science and Training.

- 'broad ranging', that is, it should cover all relevant services, whether offered by governments, industry, local schools, non-for profit organizations or individuals;

- 'multi-media', that is, information would be available through websites, email, posted pamphlets or on posted CD;

- 'broadranging', covering (at least in brief) all subjects such as buying a computer, Internet security, help in choosing the right training, and phone numbers for local computer clubs or other local facilities.

Presumably, one call centre could handle the whole of the Northern Territory, or even the whole of Australia.

Personnel: a management team and phone operators. The management team would gather and collate the necessary information; prepare handouts; recruit, train and supervise phone operators; and to promote the service.

Volunteers: could be used within management team, and as phone operators.

Resources needed: local-call telephone number; premises with telephones; space for storage and administration.

Without this information being made readily available, the Joneses may never make the move to computer technology.

Note: the information the Joneses want could simply be posted on the Internet, where no doubt it will be useful to somebody. The Joneses themselves, however, will not be able to access it until after they have learned to access the Internet – by which time, of course, they will no longer need it.

8.2 Computer Equipment

Having decided to gain access to computer technologies, the Jones's might decide to acquire a computer. So how might the Joneses be helped to do this?

As we have seen, there are four critical aspects to buying a computer:

- Buying the computer itself;
- Buying the Internet connection;
- Securing the computer against malware;
- Learning how to use the computer's security protection.

Without all four factors being satisfactorily covered, in very many cases the purchase of a computer will be at best a temporary fix to the problem. Thus these four issues need to be treated as a package.

Idea 8.2.1 – Refurbished computers

In section 6.3, it was mentioned that non-profit organizations such as GreenPC.com.au and WorkVentures.com.au (both based outside the Northern Territory) currently refurbish old computers, and sell them to low-income people.

Recommendation: Consideration could be given to creating a similar organization, or a encouragement of a branch of one of these organizations, within the Northern Territory. This would potentially have three benefits: it might marginally reduce the costs of computers to low income people; it would provide enjoyable work for some volunteers (those that enjoy playing with hardware); and it would help prolong the lives of computers that otherwise would be shipped out of the Territory for scrapping.

Personnel: To be eligible for industry support, computer refurbishment has to be handled by qualified technicians.

Volunteers: could be used to assist technicians, and in clerical and warehousing positions.

Resources needed: office, workshop, storage and distribution facilities. Industry support, including supply of computers for refurbishing.

Idea 8.2.2 – Internet Connection

In section 6.4, TADaustConnect.org.au was discussed as a non-profit organization involved in discounted ISP services. It was noted that, while TADAustConnect offered better than normal conditions of service, its prices are about normal.

Recommendation: The Government give consideration to arranging subsidies for Internet connection services to low income people.

Idea 8.2.3 – Malware Risk Assessment

In section 6.5, issues of Internet security were raised. It was noted that there appears to be little or no coherent information available to allow home users to calculate their risk (real-life probability) of loss through malware with different configurations of protection. It is not known whether this is because the information has never been collected or has been suppressed. Whatever the cause, the lack of this information means that home users are required to make important decisions without adequate information. This being the human thing to do, they assume that no visible smoke means that there is no fire, and they therefore assess their risk exposure as zero. Thereafter, they tend to treat all statements by government and industry on Internet security as either shrill hysteria or self-serving hype, to be ignored by all sensible people.

Recommendation: Government, universities, industry and non-profit organizations to work together determine and widely publish the risks of –

(a) Suffering malware infections with different protective configurations and regimes;

(b) Suffering different kinds of damage when/if infection occurs.

Idea 8.2.4 – Malware Protection Standards

Recommendation: Following identification and publication of infection and damage risk levels, Government to mandate, by legislation or otherwise –

(a) Terms which may be used by computer retailers to indicate that a computer is suitable for connecting to the Internet;

(b) Under what circumstances those terms may be used (in particular, what minimum software and other configurations are needed for each term);

(c) A prohibition on manufacturers and retailers using these terms when not supplying the minimum configurations.

The aim is to set evidence-based benchmarks, based not on the manufacturers' or retailers' commercial convenience but on real-life data and the consumer's interest, for what constitutes 'safe' configurations.

Note: the author is not suggesting that manufacturers or retailers be compelled to install a particular security system, or indeed any security system at all. The recommendation is that they be banned from doing as they do at present, namely, installing systems that the most independent experts regard as inadequate, and then claiming the computer to be safe.

Idea 8.2.5 – Malware Protection Standards to Endure

Recommendation: Government to mandate, by legislation or otherwise, that, if manufacturers or retailers claim that a computer is safe online, that its security be permanent (subject, of course, to users doing whatever is required of them) –

- Security software should give protection indefinitely, whether or not renewal fees are paid. For example, the present practice of some software manufacturers of having their products installed on new computers to give initial protection should be banned if the protection given is subject to expiry at a later date (or else claims that it protects the computer should be prohibited);

- Some software manufacturers provide both 'free' and 'paid' versions of their software, with the 'paid' versions almost invariably being very much easier and less time consuming to use. For instance, Lavasoft Ad-aware, a popular antispyware program, has two versions, one 'paid' and one 'free'. There are no major differences between the two versions, except regarding convenience of use: the 'paid' version can be set to do its weekly updating and scanning almost fully automatically, with little or no user intervention, while the 'free' version requires up to an hour of the users time each week. To this author, this seems a most socially responsible and enlightened approach to the issue of helping home users across the Digital Divide.

Idea 8.2.6 – Malware Protection Standard Training

Recommendation: Following the setting of a standard for secure configuration, the commissioning of research to determine the best way to enable home users to look after this configuration, and to use it to keep their computers safe. Of necessity, this will include development of new forms of software, re-design of some existing software, and development of suitable training programs. It is envisaged that the software will need to be developed either by industry or by programmers working within the Public License tradition, and that the training programs will be made available to industry and to the non-profit sector for implementation.

Idea 8.2.7 – Retailers to Provide Security Training

Recommendation: Government to mandate, by legislation or otherwise, that retailers to be required to provide training for all computers that they sell to home users as Internet-safe. This training could be by way of book, live classes (at the store, or, for example, at a nearby computer club) or a video presentation (on the computer or on DVD, but not online). Whichever way, it should provide step-by-step instructions for all the actions required of the user to keep the computer safe using the security configuration installed.

Idea 8.2.8 – Computer Installation Service

Recommendation: Once the Joneses have bought themselves a computer, they may need somebody to help them install it. For technicians and experienced users, this is a very simple task; for people with disabilities, however, it may be entirely impossible. People with arthritis or limited sight, for instance, may be unable to handle the plugs, while other people may have trouble lifting the heavier components.

This would be an ideal task for a local computer club to undertake.

Personnel: An administrative team to receive requests for installations, and to recruit, train and supervise volunteers.

Volunteers: to handle installations. Would need either to have their own vehicle, or access to a vehicle.

Resources: Office space and phone, volunteer and vehicle insurance, a vehicle or money for car allowance

8.3 Training

Having acquired their new computer, the Joneses now need to learn how to use it, and then, presumably, how to look after it. As we have seen (section 6.6), there are five groups of subjects for the Joneses to study, ranging from computer basics ('beginners'), through system administration (sysad) and Internet security, through, finally, to the use of specific applications such as web browsers, email clients, and word processors.

Amongst the best-served cities in Australia, so far as teaching for beginners is concerned, is Brisbane. In this city, beginners' training is provided by various colleges and public libraries, and also by the local computer club, Brisbane Seniors Online (BSOL). BSOL, which is supported by the Brisbane City Council, offers a wide variety of learning options, including group classes (of up to six students), one-on-one learning in the student's home or elsewhere, and self-paced learning on CDs. In short, there is something for everyone – for the people who like learning in classes, and for the people who don't; for the housebound people, and for those able to get out and about; and even for the people who wish to teach themselves. This seems an ideal model to copy.

The author's club, the Darwin Seniors Computer Club, has decided to adopt this model, and is currently preparing to establish it throughout the Northern Territory. To do this requires considerable restructuring of the Club to provide for a central organizing body to provide basic training resources, and local community-based bodies to provide the actual training. Once this restructuring is completed, Northern Territory communities should have access to a wide variety of quality beginners' training programs.

The situation is less rosy for sysad training, which it will be recalled deals with home computer maintenance. There are few if any training courses offered anywhere in Australia that deal with home computer maintenance or security. Some or all of the reason for this is that technical education is generally seen as 'vocational' and hence industry-oriented. This result of this training gap is that technicians receive little or no training in these subjects, and hence unable to offer their home user customers quality service. Likewise it means that home users cannot undertake training in these fields, and so are unable to act as volunteers helping, for instance, people with disabilities look after their computers.

Idea 8.3.1 – Sysad Training

The paucity of training in home computer care for IT professionals has been noted earlier. It may be that a similar paucity exists in high schools. This results in poor skill levels amongst IT professionals; difficulties for non-profit organizations in finding skilled volunteers; and ultimately unhappy home users.

Recommendation: Consideration to be given to creating courses in home computer care for high school students, volunteer teachers, the volunteers who look after computers in non-profit organizations, and for professional computer technicians. Such courses would focus on issues such as finding, evaluating, downloading and installing software; procedures for protecting home computers against malware; routine software maintenance; and data backup.

Idea 8.3.2 – Training Coordinating Organization

Recommendation: Consideration to be given to creation of a central coordinating body to undertake research into home computer training needs, and to help evaluate existing training activities. This body would work with Government, industry and consumer bodies to coordinate the activities of computer and software manufacturers, and training providers (including schools, colleges and computer clubs).

Idea 8.3.3 – Home Security Training

Recommendation: Government to work with industry and computer clubs to identify suitable training methods, and to set standards, for home users in home computer security.

8.4 Technical Support

Having acquired their new computer and learned how to use it, the Joneses may eventually need help, either in repairing or up-grading their computer equipment. The reasons for this may include: the equipment breaks down; the Joneses want it modified or customized to some new need; or they need it up-graded in some way short of buying an entirely new computer.

An option here is for an organization, perhaps analogous to the motoring organizations (e.g. AANT), to provide basic repair or maintenance services, and/or a referral service to suitably qualified technicians. (Given the total absence in the Northern Territory of training in home computer software maintenance, the need for a referral service is as desperately needed as the need for suitable training, and for suitably qualified software technicians.)

Idea 8.4.1 – Directory of Technicians

Recommendation: Consideration be given to creating a directory of technicians within each local area who are willing and able to assist home users. This information would presumably be used by the Telphone Hotline mentioned earlier.

Idea 8.4.2 – Home Technical Support Service

Recommendation: Consideration to be given to creating a home support service for people with disabilities or other special needs. This service would provide low-level technical support, including routine maintenance (e.g. security scanning and defragmenting).

(If there are enough suitably skilled volunteers, this program could be run using volunteers, in whole or in part. Otherwise, it would require funding for paid staff.)

8.5 Final Tasks

As the Jones's learn about their computer technology, they face four more tasks. These are:

- Keeping up their enthusiasm as they begin to realize the often-daunting complexity of computer technologies;
- Practicing new skills as they acquire them;
- Extending their repertoire of skills; and
- Staying abreast of new developments in computer technologies.

There, of course, very many ways for people to achieve these ends, but for many home users, computer clubs can provide the perfect all-in-one solution.

Before discussing computer clubs, however, let us look at other social environments with proven success in helping people to cross – and stay across - the Digital Divide: schools, universities and workplaces.

Each of these places provides a social environment in which it is possible to meet new people, make friends, and gain encouragement in the struggle to master computers; each provides opportunities to learn about new technologies, even if it is only through listening to one's friends bragging about the new gadgets they have recently bought. Very often, these places not only provide pressure to learn new computer skills, but also supply the training to make it happen.

To achieve similar success rates in keeping people maintain computer literacy, computer clubs have to provide an equivalent environment. That is, it needs to provide -

- Lessons in computer techniques (that is, how to use current technologies);
- News about new and emerging technologies (what to expect in the near future);
- Social opportunities (exposure to social peers who are knowledgeable about computers);
- Individual support (someone to help in an emergency).

There are, of course, many ways of providing these services, but there is no sure evidence as to which way is best. This is how Darwin Seniors Computer Club provides these services -

8.5.1 Club Room/Internet Café

From its inception, the Club has maintained a room in Nightcliff, which members can use as a social centre and Internet café. For several hours each day, members can surf the Internet, send emails, and work on their personal projects. They can also meet and mingle, entertain each other, swap files, and help each other.

Superficially, this room provides a service similar to an Internet café or the computer access service of many public libraries. There are differences, however, with the major difference being the interactions between members. At Internet cafes and public libraries, people usually work alone, quietly, and generally with time limits. At the club, however, there are few time limits, and the social interactions are a major part of the experience.

An important part of creating opportunities for social interactions is that people wish to mix with their social peers – others of similar age, social status and with similar interests and circumstances.

Idea 8.5.1.1 – Internet Cafés with Coffee

Recommendation: Public libraries and other community places with Internet facilities to give consideration to making these available, at least occasionally, as centres for social activities.

Traditionally, Internet cafés were intended to be used by students and tourists working by themselves, head-down, paying no attention to other people. Sometimes, computers were clustered in a circle (presumably for convenience of power and other cables), making social interactions between users even more difficult.

While the needs of solo users needs to be respected, this paper recommends that public Internet café facilities set aside at least some time for the computers to be used socially, with relaxed time and noise limits.

This paper also recommends that public libraries and other community services design future Internet café services with social uses in mind, such as by aligning computers in a straight line, so that users can easily see what others are doing; possibly having one or all computers linked to a projector, so that participants can display their screen for all to see; having computers linked to speakers, or having head sets available so that partipants can hear their computers, and share sounds; having seats for non-surfing participants close by (so they can join in the fun); and by having coffee/tea facilities available nearby.

(An important issue when creating opportunities for social interactions is that people like to mix with others that they consider their social peers – for example, people of similar age, background, social status or with similar interests or circumstances. It is envisaged that each social/surfing venue could serve a variety of different groups, each on different days, or at different times of the day. For instance, each could be used by youth groups and by seniors, by people with disabilities, and by people who share interests or hobbies.)

8.5.2 Volunteering

To keep the Clubroom open, and to keep its computers functioning, it is necessary for club members to contribute considerable amounts of time as volunteers. From the point of view of keeping people on the right side of the Digital Divide, this has two important benefits, one involving commitment, and the other performance.

The first benefit is that the *commitment* to volunteering encourages attendance at the club, in the same way that a commitment to be a school student, or an employee in a workplace, encourages attendance at the school or workplace. The fact of committing results in greater involvement in the club, which leads to greater access to the benefits of club membership, and hence (or so it seems) to improved computer skills[35].

The second benefit for volunteers is that the *performance* of volunteer duties also generally helps improve computer skills.

[35] The author has

8.5.3 Computer News Meetings

Once a month, the club holds a two-hour meeting. This meeting has a structured format, designed with the above objectives in mind. It has five sections, each of about 20-30 minutes duration:

1. Welcome, plus club news and notices;
2. Computer news: a run-through of news items of interest to home users, generally with beginner-level explanations.
3. Coffee break: a time for socializing;
4. Show & Tell: a time for members to talk about their pet projects, show off their latest purchase, or report on local computer technicians or retailers;
5. A lesson on some aspect of using a computer.

Overall, this meeting is intended to help with all club objectives: to encourage participation in the club's activities, especially as a volunteer; to learn about existing technologies; to learn about forthcoming technologies; and to help build social contacts.

(Computer news meetings could be beneficial for a wide variety of organizations and communities beyond the computer club environment. For example, the same or similar format might be used for youth groups, in homes for the aged, in Aboriginal communities, and in non-profit organizations with significant numbers of volunteers.)

Idea 8.5.3.1 – Rooms for Computer Update Meetings

Recommendation: Local government and other relevant bodies to give consideration to equipping community halls for computer news meetings. Requirements are a computer (ideally Internet-connected), a projector and a screen, plus refreshments facilities.

Idea 8.5.3.2 – Funding for a Journalist

Recommendation: Consideration to be given to funding a journalist to prepare monthly news bulletins in a manner suitable for delivery by club members and others. Conceivably, these bulletins could be used around Australia, and posted on the Internet for overseas users.

Consideration could also be given to recording these bulletins on video, in the manner, for example, of CNET bulletins. There are, however, arguments against doing this exclusively, as the only method of presenting the material. Presumably to keep file sizes small, the CNET presenters gabble their lines. This can make their presentations incomprehensible to the hearing impaired, non-English speakers, and many older people. Also, it makes the presentations very inflexible. So while a video presentation could suit many situations, it would not suit all.

8.5.4 Computer Training

The provision of computer training is a prime aim for most computer clubs[36]. As discussed earlier, there are many types of teaching programs, and many ways of learning

[36] Not all focus on teaching. There is another type of computer club, sometimes called a 'user group', whose primary focus is on the use of some particular aspect of computer technology, rather than the people who use it.

(section 6.6.). Not all of these options are within the capability of computer clubs, however, which tend to be best at providing volunteer teachers for beginners' training.

Training needs to be provided at a place and in a manner that is at least reasonably convenient to the student. For students who are intelligent, sociable, able-bodied and mobile, and who speak and read fluent English fluently, and live in towns, classes in a nearby community centre may be ideal. For other people, alternative arrangements may be needed, which may include on-on-one training (one teacher, one student) or solo training (students teach themselves using books, interactive video or similar methods). For some people, a mix of all three methods may give best results. The key here is flexibility: having 'training advisors' who can help select suitable training programs for each student, and having teachers and training aids to meet all circumstances.

8.5.5 Social Activities

As discussed earlier, social activities play an essential role in helping people stay on the right side of the Digital Divide. The provision of social activities, and making sure that these activities are enjoyable for the people concerned, is therefore an important part of a computer club's activities.

In the normal course of its activities, the Club provides a wide variety of opportunities for people to mix and mingle. For example, almost all volunteer activities, whether as teacher, administrator or committee member, involve dealing with other people. Likewise, almost all teaching activities involve social activities for students.

In addition to these kinds of activities, the Club also works to encourage or provide other kinds of social activities, such as trips to cultural events, movie nights and a Christmas luncheon. Providing such extracurricular activities is, strictly speaking, outside the Club's primary purpose, yet all opportunities for Club members to mix and to build relationships ultimately provide community benefits in reducing the impact of the Digital Divide. This matter is further complicated by the fact that, while all members join the Club to be involved with computers, not all want social activities – indeed, some positively do not want them! Accordingly, the Club has adopted a policy of encouraging or publicizing extracurricular social activities that are enjoyed by substantial numbers of members, but in ways that cost the Club little by way of time or money. For example, the Club happens to have, amongst its members, many who are involved with the local ballroom dancing scene. Accordingly, the Club encourages members concerned to use Club computers to, for instance, download dance music and prepare leaflets advertising dance events, and also allows some use of the Club notice board to publicize ballroom dancing activities.

So far as is known, there are two such groups within the Northern Territory. One is the Darwin Linux Users Group (known as Darlug for short), based at Charles Darwin University, which focuses on the Linux operating system; and the other is a group within Darwin that focuses on playing certain interactive computer games.

Appendix A: Darwin Seniors Computer Club

Darwin Seniors Computer Club Inc. was established in 2001 to provide computer-related services to seniors and people with disabilities. From the outset, it was recognized that these groups had special needs which 'regular' services did not meet. For instance, most computer-related services, both then and now, assume high levels of motivation and ability to learn and to use computer skills, plus high levels of income to pay for whatever services or equipment may be needed. In our target clientele groups, however, none of this is necessarily true. So the past years have been spent developing a range of alternative programs and services.

The Club has a relatively stable membership of around 60-100, of whom about 30 are occasional or regular volunteers. Its management committee is also very stable, with most members having served for two or more years.

Probably the Club's largest problem is the smallness of its clubroom. This tiny (about 4 x 5 metres) room within the Nightcliff Community Centre serves as: meeting room, club room, office, classroom, workshop, storage area and Internet café. Even though it is used almost every day, from morning to night, the lack of adequate working space severely limits the Club's ability to help the community.

Appendix B: Government Websites

The Australian Government has a number of websites that touch on Internet Security for home users. These include:

- www.Seniors.gov.au;
- www.StaySmartOnline.gov.au;
- www.NetAlert.gov.au;
- ScamWatch.gov.au/

Between them, these four websites appear to cover most if not all issues of relevance to home security. Two of them – NetAlert and ScamWatch – represent examples of good practice amongst advisory sites. The other two – Seniors and StaySmartOnline – represent the exact opposite[37].

First, the Bad News.

Seniors.gov.au is a portal site; that is, it aims to provide a 'first port of call' for seniors looking for information. For instance, a visitor to the site might click on a link entitled 'Need Some Help?' which takes him to a page offering three options, including one for new users ('New to the Internet?'), and one, presumably for more experienced users, entitled 'Internet tools and tips'.

The page for new users provides a whole host of links, not one of which deals with protecting one's computer. Apparently, the Government thinks that newcomers to the Internet don't need Internet security. This suspicion is reinforced if one watches the video 'Connecting with Computers' offered elsewhere on the website[38]. This otherwise excellent video tells viewers that they will "probably never need to know" how a computer is plugged together, and makes no mention at all that there are security issues involved in using the Internet. Considering the consequences involved, one might consider this as irresponsible as suggesting to somebody learning to drive a car that they will never need to learn how to put air in the car's tyres, and then failing to mention road rules or other traffic.

Meanwhile, the 'Internet tools and tips' offers some vague advice on Internet security (including an exhortation to 'install and maintain antivirus and firewall software on your computer'), but no mention as to how this might be done. It also encourages readers to "consider whether or not to purchase and install firewall software". These two pieces of advice are, however, seriously, even irresponsibly misleading. By failing to mention spyware, which is currently one of the worst kinds of malware, it implies that antispyware software is unnecessary. By suggesting that readers should 'consider' using a firewall, it implies that firewalls are 'optional extra', and hence largely unnecessary. By implication, the website is recommending that users consider putting themselves and their computers at risk.

In addition to its misleading advice, the 'Internet tools and tips' webpage provides a link to StaySmartOnline.gov.au, as having "has practical tips and advice on e-security". Clicking on this link, however, produces its own problem; one gets sent to a page that says:

[37] The material in this Appendix was prepared on 4 November 2007. It is possible that the websites discussed may have changed since.

[38] Produced by the Department of Education, Science and Training.

> *"Seniors.gov.au is not responsible for, and does not endorse, the site, its owner/maintainer or its content. For further detail please read our Disclaimer. If you have any questions please do not hesitate to Contact Us."*

This message is watched over by fierce-looking guardian, who seems to be saying, "You came to our Government website for reliable information, but we're not going to give you any. What's more, the only links we provide are to untrustworthy sites, so be afraid, be very afraid!" This is hardly a good way to reassure people nervously exploring new technology.

So sensible people stay in the safe but useless Seniors.gov.au website, and wait, unprotected, for the malware to get them.

But let us join the few hardy souls who brave official warnings and disapproval, and head off to StaySmartOnline.gov.au, where they find a page promising to show "home users and small businesses" to stay smart online. Here they click on a link "Securing your computer", which promises to show them how to "protect your computer and internet connection from hackers, viruses and theft". This takes them to a page with links to eleven steps to securing computers.

Only now, faced with eleven major steps, does grim reality begin to dawn for the poor Internet novice: securing their computer is going to be a very long and difficult project. But they are not going to find out here! Oh dear no! No matter what it promises, this site, it seems, does not give out practical advice. Ever.

To see what it does instead, let us follow one of these links: that of Number 4: installing and using a firewall.

Now, everybody agrees that a firewall is important. As the 'Number 4' page says, "A computer without a firewall is like a house without doors—there is nothing controlling who and what enters or leaves."

So our novice says, "Great, so tell me which firewall to use."

Not so fast, replies the webpage. If you want to know more, you have to go to the Internet Industry Association's firewalls section on their 'Managing Security portal[39]'.

Thus our novice is directed to an industry website with no less than ten different links, most of which are filled with information unsuitable for home users. Amongst these ten links, however, is just one for a specific home firewall – Norton Personal Firewall.

Meanwhile, our intrepid novice decides to click on a link called 'Free firewalls, gateways and routers'. This page contains a page packed with information, including the remarkable statement, "+++ Be aware Personal Firewalls DO NOT increase security. +++"[40].

So what is going on here? The Government is variously telling home users that firewalls are optional extra, necessary like the door of a house, and totally unnecessary. And all the while doing absolutely everything but give practical advice.

Presumably, the whole point of the exercise is to *avoid* giving users practical advice.

Then, the Good News.

The other two Government websites, NetAlert.gov.au and ScamWatch.gov.au, provide examples of how a good advisory site should be done -

---

[39] http://tinyurl.com/ynq5nr

[40] Some people might consider the information on this webpage to be totally irrelevant to a home user, which may indeed be correct. But that is itself irrelevant; the fact is that the Government website directs home users to that page as containing information important to them, and accordingly it must be considered that the Government endorses the opinions on that page. Even if it made disclaimers (which it doesn't), this would still be true.

- Both sites clearly state the issues to be addressed, and provide practical advice – that is, concrete, step-by-step instructions for dealing with the situation.
- Both sites clearly endevour to deal with all relevant issues, not just the ones that favour commercial interests;
- The NetAlert site demonstrates how security software should be dealt with: a short-list of software is offered, with each option being clearly explained, and a simple, easy-to-follow means of choosing between them is provided[41].

[41] It may be noted here that the software range exists not merely to 'give the user a choice', as if this were somehow automatically desirable, but as a response to allow for differences in the users' computer hardware, and in the users' need for different program functionality.

Appendix C: Computer Retailers

Many novices look to their local friendly computer retailer for advice and help. In part, this is because the retailers generally promote themselves as being helpful, and as having the consumers' interests at heart; and in part because the Trade Practices Act says they have to. Retailers, and the manufacturers who supply the goods they sell, do not always live up to the high standards that they claim, or that the public expects.

Forty years ago, Ralph Nader complained that automobile manufacturers made cars that "were unsafe at any speed"[42]. Today, much the same claim could be made about the computer that retailers sell. Most computers that are sold to home users have at best the most token of security systems, and so are accidents waiting to happen.

To substantiate this claim, we must consider two separate but interconnected questions: what does a state-of-the-art security system for a home computer look like; and who says so?

As discussed in the body of this report (section 6.5), the consensus opinion of respected websites such as Spywarewarrior.com is that an Internet-safe computer would have one firewall, one antivirus, and at least two different antispyware programs. It would also have its user accounts password protected and secured, and probably some method of backing up partitions and data, both to protect data and to allow for rapid and inexpensive recovery after a malware attack. By this standard, almost all home computers sold in Australia as 'Internet-ready' are sold under false pretences.

Are all of these steps necessary, however? Judging by their actions, neither manufacturers nor retailers think so. Quite reasonably, they might point to the relative lack of statistical support publicly available for these requirements, as mentioned above in Section 6.5. One cannot help but wonder, however, whether this is not the same kind of self-servicing ignorance that the tobacco and asbestos industries indulged in. In almost all cases, the missing statistics would be available to at least many of the companies concerned, so we may reasonably assume that the absence of these statistics is deliberate industry policy.

When Ralph Nader made car safety a public issue, Governments eventually moved to make such safety measures as seat belts and airbags compulsory. It seems apparent that the computer industry is in no hurry to deal with computer security. Will it take Government action to make them live up to their social responsibilities?

[42] http://en.wikipedia.org/wiki/Unsafe_at_Any_Speed

