# [1]Recommendations for Internet Safety at Home

Clark Thomborson
Computer Science Department
University of Auckland
http://www.cs.auckland.ac.nz/~cthombor

**Abstract.** We offer a brief, unscientific survey of the safety issues that are likely to arise in any home containing an Internet-enabled computer. For each issue, we recommend at least one way of minimising the risk, without losing sight of the benefits of wise Internet use.

Wise use of the Internet is possible, but only if each user has a rough idea of what the Internet can and cannot do:

- If you know nothing about the Internet, you cannot use it wisely.

Our first recommendation: everyone should learn at least a little about the capabilities of the Internet. Most folks need help in "learning how to learn" about an unfamiliar technology, such as the Internet, that is developed during their lifetime. By contrast, today's children have had the Internet all their lives. They find it as familiar as an automobile. Whether a powerful technology is familiar or unfamiliar, however, everyone should have some basic tuition on safety before a first unsupervised "surfing of the internet" or "driving of a car."

My favourite explanation of the Internet and its capabilities is based on a simple analogy. The Internet is somewhat like the public telephone network: both are popular ways of communicating over long distances.

Imagine, for a moment, how wonderful and frightening it must have been, when your grandparents or great-grandparents had their first conversation on a telephone. Now try to remember when you used the telephone for the first time. How did you learn that a telephone can transmit voices, and that it will transmit *only* voices or other sounds? How did you learn that the person on the other end of the telephone is not able to see your face, to see what you are seeing, touch you, or smell you? I think we learn such lessons best, by making mistakes. When using the telephone as a child, we may believe that the other person is in the same room with us, but is invisible for some reason. Eventually, through discovering errors in our communications, we gain a clear idea of the capabilities and limitations of a telephone.

A computer that is connected to the Internet is quite a bit more powerful than a telephone. Partly for this reason, the computer is much more difficult to use. Most people can quickly learn to use the Internet to *receive* pictures, written material, sounds such as human voices and music, and even motion pictures. It is somewhat more difficult to learn how to *send* textual messages, pictures or sounds over the Internet, but most people can accomplish this after a few hours of tuition. At this point, they have a functioning knowledge of the Internet as a communication medium, but they have not confronted a vitally important lesson in Internet safety.

A computer is quite different to a telephone, because of a computer's ability to send and receive *computer programmes* that will affect another computer's operation. This transfer of programmes is the mechanism by which computer viruses are spread. It is also the mechanism you should use, on regular occasions, to update your computer's protection from newly-created computer viruses. This is our second safety issue:

---

This article appears in *Proceedings of NetSafe: Society, Safety and the Internet, ed.* John Hosking, Technical Report 172, Department of Computer Science, University of Auckland, pp. 118-123, February 2002.

- ❖ Whenever your computer receives information from the Internet, it may be receiving a computer programme that will affect its future behaviour.

Suggestion: Your computer requires regular maintenance for safety. If the current situation in computer security continues to degrade, the government might institute annual Warrant of Fitness checks for all private computers, in addition to automobiles! At the risk of flogging the automotive analogy to death: we are still in the "model T" age of computing. Frequent maintenance is required. At least twice a year, you should install (or hire someone to install) all available "security patches". Learn how to load new "virus definitions" and to "scan for viruses". When your computer behaves strangely, find someone competent who will help you check it out.

- ❖ Your home computer's actions and inactions will surprise and frustrate you sometimes.

Our suggestion on this issue: consider what lesson you might learn, in each instance, about what a computer can and cannot do. As when you learned to use a telephone, through your miscommunications and frustrations on the Internet, you will eventually gain great insight into its capabilities and limitations, if you are perceptive and open to the lesson of the moment. Only with this insight will you be able to use the Internet wisely.

No matter what programme your computer may be running, it must employ an "input device" in order to sense any phenomenon in the real world. There are only a few types of input devices, and you should find a way to discover what devices are available to programmes running on your computer. As a trivial example: all personal computers have keyboards, and most computer programmes running on personal computers are sensitive to whether or not you are depressing keys on the computer keyboard. This observation on sensitivity may be understood as a limitation as well: touching any surface in your household, other than your keyboard or mouse-key, will not affect your computer's operation.

A computer is very analogous to a telephone in this respect. Almost all adults understand that a telephone has a microphone, and only a microphone, as an input device – this is why a telephone cannot transmit sights, smells or touches. No home computer, as yet, is sensitive to smells; however your home computer may be equipped with both a video camera and a microphone. This is our fourth safety issue:

- ❖ Anything you say within "hearing range" of your computer's microphone, and anything you do in front of your computer's camera, may be sensed by your computer. Anything that is sensed by your computer may be stored in its memory system. Anything that is stored in your computer's memory system may be retrieved at a later date, by anyone who has access to your computer.

Our recommendation: always behave as though the space near an Internet-connected computer is a "public place" and not a "private sanctuary". You can "lock the door" to this public place quite effectively and easily, by turning off your computer. Remember, however, that anyone who is able to turn on your computer, such as a family member, will have access to its memory and therefore (at least potentially) to any of your previous activities that your computer has recorded.

If it is inconvenient to turn off your computer, when you desire a high degree of privacy you should put a cover on the lens of its video camera, and disconnect or disable its microphone. The disk memory of a typical home computer can store several hours of high-quality video information, and several days of low-quality video information. I am not suggesting here that anyone should become paranoid about the possibility of computerised surveillance, by law-enforcement agencies, malicious intruders, or family members. If you have reason to be concerned about this possibility, rest assured that any knowledgeable person would be able to detect the disk activity and communications traffic that would be generated by any computer that is being used as a video-surveillance instrument. The absolute risk of video surveillance from a

contemporary computer is quite low. However, the risk will rise considerably, in the foreseeable future, when broadband "always-on" Internet connections and ultra high-capacity disk drives are commonplace in home computing.

A more likely risk than surveillance in contemporary home computing is that

- A few seconds of Internet transmission, conceivably initiated by a nasty computer virus, may reveal some very sensitive personal information that your computer has "sensed" through your previous use of its keyboard.

For example your name, credit card number and PIN code may be retained somewhere in the memory of your computer, if you have ever typed this information into your computer for an "e-commerce" purchase.

We therefore recommend you keep written records of all your e-commerce purchases, so that you are in a strong position to ask for restitution if you have sustained a loss from fraud. All reputable e-commerce websites and credit card companies will want to keep you as a "happy customer" if you are able to help them document a fraud, especially if your information helps them to track down a fraudster.

My intention here is not to foment fear and mistrust of our computers ability to record and transmit information. Instead, let us remember that our home computer's ability to record keystrokes, video and sound from our private lives at very low cost is a truly wonderful thing, if we are intending to communicate this information with our friends and loved ones!

Casting our first set of issues in risk/benefit terms, wise use of the Internet is possible when you are able to strike an appropriate balance between its risk to your privacy, and its benefit to you as a communications and financial mechanism.

We now develop a second set of issues and recommendations, from a brief overview of the history of the Internet.

The Internet did not spring into being, fully formed, from the efforts of a single research and development effort. It has been evolving for decades, and it continues to change rapidly. However some components of its trajectory of change are fairly predictable, to anyone who knows its earliest design goals.

The first precursor to the Internet is generally considered to be a research and development project called the Arpanet. The Arpanet was a network of computers, all of which were used for research and development that was funded by the US military or cooperating agencies. It operated from 1969 to 1990. The initial goal of the Arpanet was to develop convenient and reliable methods for exchanging information between geographically dispersed computer centres. Security against malicious acts was not a major goal in the development of the Arpanet, which may seem surprising in retrospect given its military sponsorship.

I will relate my personal experiences briefly. I started using the Arpanet in 1975. In 1978, I relied on it heavily for cross-continental communication of my research findings with my PhD supervisor, by email and exchange of manuscripts.

The thousands of people who used the Arpanet during the 1970s generally behaved as though only trustworthy people would have access to "our" network. Accordingly, we rarely bothered to hide or otherwise protect our files from each other. Instead we developed an ethos of sharing in a non-commercial environment: advertising was strictly forbidden on the Arpanet. We worried much more about software and hardware malfunctions, and careless operations, than about malicious intrusions. For example, I crashed the Arpanet by mistake, in 1979, when I set up an email-forwarding system incorrectly. No one accused me of malicious intent; instead the network

administrators calmly went about adjusting the computer programmes that controlled the Arpanet, so that similar mistakes in the future would not be catastrophic.

Fast-forward to today. There are now hundreds of millions of users on the Internet, and advertising is rampant. Despite these profound quantitative and qualitative changes, some aspects of the Internet only make sense if one believes (wrongly!) that this is still "our" network, and that all users can be trusted to "behave well":

- The Internet is a permissive communications medium. It was originally designed to allow any communication that was not specifically forbidden. Even today, *anyone* with sufficient skill, equipment and time is able to communicate with *any other computer* on the network. The minimum level of skill, equipment and time required to obtain access to specific computers can be raised, if special protective measures are taken, but ultimately every networked computer is accessible to a well-resourced hacker.

Our first suggestion in this regard is to be careful of what you information you store on an internet-enabled computer. It is not a "safe place" for your intimate secrets.

Also, we suggest you avoid giving out your own email address, or anyone else's email address, to untrustworthy or unknown individuals. Anyone who knows your email address is generally permitted, by the basic design of the Internet, to send you "spam" (unwanted commercial broadcasts) and other objectionable material. Messages with long lists of addresses in the "To:" list are security hazards, because every recipient can "harvest" all these addresses for future use.

Twenty years ago, there was essentially no spam on the Internet. Ten years ago, it was a rare occurrence. Currently, I must discard approximately five "spam" messages from my academic email inbox, for each legitimate communication that I read. Ten years from now… I'm not sure how we'll cope, although there are some partial solutions of which you should be aware.

Currently, almost all email systems permissively accept all incoming messages, except that which is explicitly rejected by what is known as a "spam filter." For example, a simple spam filter would scan all incoming messages, discarding any message that contains any word identified by the filter as pornographic or otherwise objectionable word. Such filters work quite well, except for people who would like to receive email messages from friends with a spicy vocabulary!

Ten years from now, most of us may adopt a second partial solution, of using "closed mailboxes" which accept email messages only from parties that we have placed on our acceptance list. Such mailboxes are much more difficult to maintain than our current "open mailboxes," because we'll have to keep our acceptance lists up-to-date. We may nonetheless choose closed mailboxes, thereby moving away from the original permissive model of the Arpanet, when this becomes a wise way to balance the risks of unwanted solicitations against the benefits of serendipitous communications from (say) long-lost friends who have recently discovered our email address.

- Cyberstalking, talking with strangers, and pornography.

If you have children who use email, we strongly suggest you talk to them regularly about the unwanted email they receive, and how they feel about it. Set some guidelines about "talking with strangers" on the Internet, and be aware that some people use the Internet as a gigantic "dating service" or worse. Talk with your children regularly, about "who they are meeting on the net". Supervise their Internet use: your child does *not* have an absolute right to privacy or freedom in their Internet use. (You would not permit them to drive recklessly in your automobile, would you?) Learn how to install and maintain a "spam filter," to limit the volume of pornographic and objectionable content that your children will receive in their email. Most email service providers offer assistance in this regard. You should also enable the "objectionable content" filter on your computer's Internet browser, to limit your child's exposure to pornography. No filter can be 100% effective, and all can be bypassed by a clever child, but even with these defects they will greatly

reduce the chance of your child (or you) inadvertently viewing a pornographic website. Such websites occasionally are found "cybersquatting" on a normally valid web address, or using a web address which is a commonly typed misspelling of a popular website.

Regarding cyberstalking, we strongly recommend that you explore http://www.netsafe.org.nz with your child, and discuss what you find.

Another outcome of the permissive Arpanet culture, still visible on today's Internet, is the ability of anyone to "write anything they want" on their website.

- Information on the Internet is not censored. There is no guarantee of authenticity or veracity, and it is impossible to be absolutely sure of the identity of its author.

Our recommendation is to be sceptical of everything you find on the Internet. If it contradicts something you have read elsewhere, don't believe it until (at minimum) you have found some corroborating evidence.

If you are a parent, you have probably already talked to your children about not believing everything they see on TV, or everything they read in the print media. Here we are recommending an even higher degree of scepticism. Publishing on the Internet is much different to publishing in traditional mass media such as television or the press. Traditional publishers have a financial stake in avoiding the lawsuits, public disapprobation, and criminal prosecutions that would result, in most societies, from egregious disregard for the truth (except in socially sanctioned contexts, such as fiction and political satire). By contrast, most Internet publishers have only a negligible financial stake in their website. Furthermore, they are difficult to reach with lawsuits and prosecutions, partly because it is difficult to establish their true identity and geographic location. They may enjoy the notoriety of public disapprobation.

On the positive side of this issue: the Internet is an incredibly broad and diverse source of information. An appropriately sceptical Internet surfer can conduct powerful research on just about any conceivable topic, at low cost, from their homes. Many institutions, such as libraries, and even more individuals maintain their websites with a careful regard for the truth. It is conceivable that a malicious hacker could falsify a small portion of a library's website, however any truly important information can be corroborated at multiple websites. It is almost inconceivable that a hacker could falsify all the websites that an appropriately sceptical user is likely to visit. So the actual risk of misinformation from your wise use of the Internet as an information resource is quite small. The potential benefit is huge.

Arguably the greatest glory of the Internet is that its permissiveness has encouraged a prolific flowering of a commons of knowledge, inexpensively accessible to almost anyone in the world. The presence of weeds in our shared garden is unremarkable, from this perspective, however we might all consider it our responsibility to do what we can to keep the weeds under control!

Up to this point, we have considered the risks and benefits of the Internet by considering it as a communications system, somewhat analogous to the telephone or mass media, that is permissive rather than restrictive. Our risks and benefits have involved the unfamiliarity of the technology, a series of tradeoffs between privacy and ease of communication, and tradeoffs between inadvertent financial loss and the convenience of e-commerce. We now close our paper with a very cursory survey of what we see as the educational, cultural and ethical risks of the Internet.

- Cut-and-paste mentality.

Students, even at the University level, are sorely tempted to construct reports by "cutting-and-pasting" paragraphs of information that they find on the web, sometimes without even reading it to determine whether or not it is truly relevant to the topic at hand. The cut-and-paste mentality is the opposite of the scepticism we advocate here, for the wise use of the Internet. Our recommendation

is that parents and teachers show interest in the content of reports written by their children and students. Discover the process by which the reports were written. Simple questions such as "where did you discover this information?" and "did you find any other authors who agree with this?" can go a long way toward encouraging a wiser use of the Internet as an information resource.

- Cyberaddiction – a lack of interest in non-computer activities.

In the early days of commercialised television, there was a vociferous debate about "what is it doing to our children?" Many parents, we believe rightly, responded to this question by limiting their children's access to television to an hour or two each day. We believe a similar response is appropriate to computer use. Interacting with a computer programme, even while communicating with another person, is limited to visual and audio stimuli with no smelling, tasting or touching. A healthy level of emotional connection and warmth rarely, if ever, will develop in such a narrow environment.

- Subliminal cultural influences.

The introduction of an Internet computer into the home opens a window onto the world, but advertisements often occlude the view. Most other contemporary mass media are financed in part or in whole by advertising revenues, so it should come as no surprise that the Internet is now a commercialised venue despite the original Arpanet restriction on advertising. Once the legal and social restriction on Arpanet commercialism was lifted, the permissive design of the Net immediately allowed commercial speech to spread without clear distinction from personal speech. The security issue we identify here is that the home computer, especially when it is connected to the Internet, will undermine the social and cultural influence of the parents. The subliminal (and sometimes overt) message of the advertisements is predominantly in favour of a worldview we would call American-style consumerism.

The Neopets.com website is particularly striking example of the cultural-export phenomenon we see on the Internet. NeoPets is hugely popular for kids "of all ages," but particularly for girls in English-speaking countries. Millions visit the NeoPets website each month. Here is how the website describes itself at www.neopets.com/consent.phtml: "NeoPets is a fun site that is completely free. You can adopt a pet, care for it, watch it grow, play games, chat to other people with similar interests, and much more." Our impression of the NeoPets website is that it is something like Disneyland: an enjoyable experience that subliminally promotes the virtues of the capitalist economy. NeoPets employees patrol the website unobtrusively, quietly expelling malefactors and other undesirable users.

According to www.101com.com/elx/article.asp?articleid=117, NeoPets "does not accept or allow banner advertising… Instead, it [employs] … immersive (or interactive) advertising. Somewhat akin to the popular motion picture industry practice of integrating product placements into movie screens (think of James Bond drinking a Starbucks' coffee while driving a BMW in pursuit of the bad guy)… NeoPets' Chairman [is] known for establishing the million-member research panel OpinionSurveys.com." The advertising on NeoPets is indeed subtle, and overall the NeoPets user experience is a capitalist fantasyland, whose economy is based on buying, trading and consuming make-believe items using a make-believe currency called NeoPoints. We believe NeoPets to be an excellent training ground for future capitalists and consumers.

Our final recommendation, regarding the possibly emergent global monoculture, is that parents stay in contact with their children as they explore the Internet. When your child is visiting interactive sites such as NeoPets.com, watch for "teachable moments", for cultural exports that you may or may not agree with, and for ethical decisions. If you have a teenage child, read and discuss the rules of "netiquette" as promulgated in http://www.albion.com/netiquette/book.