

The Information Society Library
GETTING THE BEST OUT OF CYBERSPACE

GOOD HYGIENE FOR DATA AND PERSONAL COMPUTERS

Stefano Baldi • Eduardo Gelbstein • Jovan Kurbalija



P R E F A C E

There is no shortage of books on all matters relating to information management and information technology. This booklet adds to this large collection and attempts to do a number of things:

- offer non-technical readers an insight into the few principles that are important and reasonably stable;
- present the material in a context relevant to the work of those involved in international relations;
- awaken the curiosity of readers enough that they will progress beyond this booklet and investigate and experiment and thus develop knowledge and take actions that will meet their particular needs.

The format of these booklets and their contents evolved from courses given by the authors over the last few years in various environments and the feedback of the attendees. Readers' feedback on these booklets would be greatly appreciated by the authors so that future editions can be improved. The coordinates of the authors are given at the end of this booklet.

ISBN 99932-53-01-4

Published by DiploFoundation

Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Switzerland: c/o Graduate Institute of International Studies
rue de Lausanne 132
CH-1211 Genève 21, Switzerland

E-mail: diplo@diplomacy.edu
Website: <http://www.diplomacy.edu>

Edited by Hannah Slavik and Dejan Konstantinović
Cover Design by Nenad Došen
Layout & prepress by Rudi Tušek

© Copyright 2003, Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

Any reference to a particular product in this booklet serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

C O N T E N T S

Setting the scene for information insecurity	5
Introduction	7
Computer crime and the world press	8
Personal risks in cyberspace	9
Vulnerabilities	16
Organisational risks in cyberspace	17
Building effective personal defences for navigating in cyberspace	21
Protective measures for individuals	23
Other good practices	31
Protective measures in a corporate environment	36
What to do if something bad happens	38
Conclusion	39
About the authors	41



SECTION



1

Setting the scene for information insecurity

*Let us not look back in anger or forward in fear,
but around in awareness.*

James Thurber

INTRODUCTION

The last ten years have seen an explosive growth in the use of electronic devices both at work and at home.

At the beginning of 2003, there were 600 million Internet accounts around the world. Cellular telephone sales are also counted in the hundreds of millions and Personal Digital Assistants (PDAs) are quickly becoming ubiquitous. Top-of-the-range PDAs include scaled down versions of the software found in personal computers as well as that needed for wireless communications.

The emergence of WiFi as a de-facto standard for mobile and wireless access to networks, including the Internet, has dramatically changed the landscape of information insecurity.

A substantial proportion of computer users who regularly connect to the Internet are well aware of the existence of malicious software in the form of viruses and worms as many have become their victims. What is perhaps less recognised is the fact that malicious software can also be spread to PDAs and, increasingly, even to cellular telephones.

This booklet is not a comprehensive guide to protecting every kind of device. It will merely present the problems that exist and the tools which are available to contain them. It will also present examples and guidelines of how such tools can be used to protect personal computers, particularly those owned by individuals, not organisations.

Any referrals to particular tools and products are simply examples and their presence in this booklet should not be construed as recommendation or endorsement of those products. Many other tools and products are available and each individual should select the ones that best suit his or her needs.

To limit the length of this booklet, no examples will be presented of the tools and products available for PDAs and cellular telephones. Interested readers should conduct their own research regarding the specific devices they wish to protect.

COMPUTER CRIME AND THE WORLD PRESS

Over the last few years the number of press reports relating to computer crimes affecting individuals has steadily increased. From these stories it is evident that computer crime is rampant and global, and that it is possible to become a victim without even owning a computer.

Many computer crimes are never reported. Sometimes the victim is unaware that a crime has been committed at all. In other cases, the embarrassment, or loss of image or credibility induces victims, be they individuals or organisations, to keep quiet.

Criminals keep quiet too, as they would prefer not to have to face the law (at least in cases where cybercrime legislation exists, which are minimal at the moment). Hackers, on the other hand, do not keep quiet, and in fact are very well organised and tend to share information about their successes and in this way enhance the whole hacking community's ability to conduct further and more technically challenging hacks.

This booklet examines the risks and threats that individuals face in cyberspace and the measures that they can take to reduce these risks to a manageable level.

The protection of the information assets of an organisation, on the other hand, is a considerably more complex subject and only the basic principles of what this involves will be discussed here.

In addition, a number of interesting news stories will be discussed in the following pages.

Story A CNN, 18th July 2001

The FBI found 184 stolen or missing laptops, including one containing classified information from two closed investigations. Officials refused to identify which investigations were involved, but said they were two or three years old. FBI officials insist there is no evidence any investigation was compromised.

Two FBI officials also said the preliminary findings indicate possibly three other laptops also contained classified information, but they are still checking on that. Of the 13,000 laptops used by the FBI, they said 171 were missing and 13 were stolen.

Story B Newsfactor Network, Cybercrime, 5th February 2001 (and many other newspapers)

The World Economic Forum (WEF) confirmed Sunday that hackers broke into its computer system and stole personal information from most of those who attended its annual meeting last week.

Among the notable victims whose personal information was pilfered were Microsoft chairman Bill Gates, Palestinian Authority chairman Yasser Arafat, U.N. Secretary-General Kofi Annan, former US Secretary of State Madeline Albright and former Israeli Prime Minister Shimon Peres.

The compromised data included credit card numbers, personal cell phone numbers and information concerning passports and travel arrangements for a number of government and business leaders who signed up for the group's annual meeting in the resort town of Davos, Switzerland.

PERSONAL RISKS IN CYBERSPACE

Surely, this business of personal peril in cyberspace is all hype. Why exaggerate when millions of people surf the Net quite happily and nothing ever happens to them?

Well, firstly, it is not hype. Computer crime and its consequences are real enough and one of the indicators of this fact is that a cybercrime simply is no longer newsworthy unless it affects a major corporation or a critical infrastructure. Secondly, concerning the millions of people happily surfing without any trouble, it is true that most of them will probably never be victims of a cybercrime, or if they are, it will be a nuisance rather than a serious problem. However, for people in positions of responsibility, such as those involved in international affairs, sometimes working from home and often working with equipment, software and data belonging to their employers, is it really worth taking an irresponsible risk when the actions necessary to mitigate this risk are not numerous and are relatively simple to undertake?

Here is a summary of the spectrum of personal risks:



Is your employer watching you?

Technical pests

- Malicious code
- Cookies
- Spyware
- Website logs
- Hackers

Bad ideas

- Unwise e-mail
- Bypassing firewalls
- Games over the Web
- Doubtful downloads
- Questionable websites

Time wasters

- Pop-up adverts
- Banner ads
- Spam and junk mail
- Scams

Organised crime

- Credit card theft
- Identity theft

Is your employer watching you?

Many managers and executives like to stroll around the office and may not be favourably impressed to find one of their employees playing a computer game. However, this is not the real issue.

The capability to monitor the online activities of employees connected through a network to the outside world, and in particular the Internet, has been available for many years.

Monitoring systems can track which computers on the network are connected to the Internet, which sites they are visiting and the duration of the visits. Reports can be produced identifying all those computer users who have exceeded certain thresholds or who have visited websites not on the “approved list”.

Similarly, it is possible to monitor an organisation’s electronic mail for volume, content and language (the use of proscribed words).

In all fairness, in practice the employer should make the rules of the game clear to all employees from the first day of the introduction of new systems or from the first day of employment by setting out formal policies of what is and is not permitted as well as explaining which actions may be taken if the policies are not complied with.

While every situation is different, it's better to be safe than sorry. Your employer may be watching you and is perfectly entitled to do so.

Bad ideas

Staying with the matters over which an individual has the most control, there are several actions that can be considered very bad ideas in the workplace and probably also at home (see Stories A and B above).

Bad idea no. 1: Losing a computer (or PDA or cell phone), particularly when it contains sensitive information.

However, there is no need to point out that equipment needs to be protected against damage and theft. Nobody is perfect and it is possible to forget to take the appropriate action at times. But measures are available to protect the information in a computer even if it is stolen and these will be discussed later in this booklet.

Story C The Risk Digest, Volume 10, Issue 78, 22nd January 1991

Just a quick word to advise RISKS readers that the MOD laptop computer stolen in the UK has been recovered by the MOD. The information was in the press last week. There was no mention of any arrest. Understandably, since the Gulf hostilities have just started, the MOD is keeping full secrecy about the outcome of the story.

The fact that classified military information was present on the hard disk of a laptop computer would certainly seem to be a risk in itself. It is even more unbelievable that the laptop was left unattended in a car in Acton (West London), which is not the safest of areas in London. I certainly would not leave a laptop (if I had one) in my car in that area!

Story D Several UK newspapers, 22nd August 2002

A third police officer in England and a policeman in Scotland have been arrested following an FBI inquiry into child pornography on the Internet.

Sussex Police says a second of its officers was arrested on August 9 on suspicion of possible Internet child pornography offences.

It follows the announcement on Wednesday that one officer from the Sussex force and one from the Metropolitan Police had been arrested in connection with the inquiry.

A police officer from Aberdeen has been suspended from duty as his colleagues seized computer equipment in a search of the 29-year-old man's home.

The arrests have come after FBI agents tapped into United States-based websites containing indecent images of children and collected the names of credit card subscribers.

The *really* bad ideas are all related to misusing an employer's equipment and facilities. For example:

Bad idea no. 2: Installing software that can bypass an employer's security perimeter (firewall).

Such software does exist, is relatively inexpensive and seriously undermines an organisation's ability to control how its information systems and facilities are used.

In fact, two problems may arise as a result of the action described above: the first one is that installing software on an employer's computer (either at the office or at home) may interfere with other software already there and, more significantly, may introduce changes to the computer's configuration, registry and other internal workings.

While these changes may not be immediately evident to the user, if a problem subsequently arises, the organisation's Help Desk may be at a loss to identify its actual cause.

The second problem is more serious: by bypassing the organisation's firewall security features, the employee is potentially in breach of the organisation's security policies and practices and if this is discovered it could lead to dramatic consequences for him.

Bad idea no. 3: Unwise downloading.

The World Wide Web is full of weird and wonderful things:

- Music files in mp3 format can be downloaded, even free of charge (sometimes infringing copyrights) through networks like KaZaA (a word of caution, you need to be careful with this software as it installs all sorts of extra files on your computer which may cause problems and which are very difficult to remove without having to reinstall everything!).
- There are many legitimate sources of free and paid-for music files in mp3 format too. The problem is that these files are fairly large (approximately 1 Mb for one minute of music, depending on the level of encoding) and put a considerable strain on networks, servers and storage space.

- Photographic files are not so big as to create a technical problem, but their content may be found objectionable by your employer if they are: a) unrelated to the work you are doing or; b) in “bad taste” – a very subjective and flexible definition. Video files are considerably larger and generally take a long time to download, which can also lead to a slow-down of the system.
- Software downloads and installations: see Bad idea no. 2 above.

Bad idea no. 4: Using e-mail inappropriately.

The appropriate use of e-mail will be discussed in a separate booklet, entitled *Appropriate Use*. For this discussion, it is important to remember that all e-mail created on a corporate system, using the employer’s domain name, remains at all times under the ownership of the employer.

Such e-mail can be used as evidence in a court of law, and it has been many times ranging from anti-trust cases to allegations of sexual harassment. You should never forget that e-mail programs do *not* have an “Undo” facility.

Outsiders intent on causing problems

These come in three distinct categories: organised crime, time wasters and technical pests.

Organised crime is a highly lucrative activity and organised criminals are very serious about what they do. As reported in Story E, the theft of personal identities and credit card information or private banking information has led to financial losses in the billions of dollars for a large number of individuals.

A major cause of these losses that individuals do not take adequate care of their personal information when storing it on their computers or submitting it during online transactions.

Time wasters are a growing nuisance on the Internet. They exist in many forms and no doubt they will be applying their creative energy to the invention of new schemes in the near future. The most common time wasters are:

Story E MSNBC News, 12th September 2002

For two years, a former employee at a small 65-person software company on Long Island allegedly managed to raid the nation's entire credit reporting system. And in the process, if the charges prove true, he could have sold virtually any American's digital identity.

P**** C***** spent three months as a help desk worker at tiny Teledata Communications Inc. three years ago. But that was all the time he needed to allegedly set up a simple crime ring that cost consumers at least \$2.7 million, and probably much more. Before he was finally arrested by authorities in November, authorities said he had sold the credit reports of 30,000 people. The digital dossiers C***** gave away included bank accounts, credit card numbers, even former and current addresses.

Advertisers: Advertisers make their presence felt either through banner advertisements on web pages or through pop-up windows. Web advertisers claim to be “good” for the Internet because they fund the existence of certain websites that can provide information to their visitors free of charge.

However, these advertisers often also install tracking software (called adware or spyware) on your computer. This software then “calls home”, whenever you're online to report the statistical data of your activities to the “mother ship”.

In theory, no personal data is collected from your computer. Even if this is true, you still have a mini-server installed on your PC that sends information about you and your surfing habits to a remote location without you knowing anything about it. The way to deal with this problem is discussed in section 2.5 on personal firewalls.

Spammers: Spammers send out substantial volumes of unsolicited electronic mail, which can rapidly become a nuisance. Most of these e-mail



Some spammers are more creative and use this mechanism to attract the unaware to participate in a scam financial scheme. These schemes have existed for many years and fax machines used to be their most popular means of dissemination. A typical example of such a scam involves a friendly message from a person claiming to be a well connected ministry official or the relative of such an official (in most cases from an African country) who is in urgent need of assistance to transfer a vast sum of money (or diamonds) illegally out of the country. For your help in allowing them to use your bank account, you are promised a substantial financial reward. Of course, first you have to provide an advance to them to get things moving. Do you believe in Father Christmas too?

messages are advertisements, ranging from magical medical treatments for non-existing illnesses to offers of university degrees from non-accredited universities. More bizarre offers also abound.

Sometimes spammers (the origin of this word has been traced to a sketch from *Monty Python's Flying Circus*, a cult British TV comedy series from the 1970s) act in concert to attack a corporate website with the intention of overloading the system and rendering it inoperable.

The term **computer virus** has entered our vocabulary and is used to describe several forms of malicious software, including worms and Trojan Horses.

A different and altogether more dangerous kind of spam mail is one that is sent out as a consequence of the action of a worm – a mechanism used to spread malicious code over the Internet. Many worms are programmed to read your e-mail address book and send copies of themselves to every address they find. Worm-infected e-mails usually contain a friendly subject line and message, with the malicious code included in an attachment.

The moment the recipient opens the attachment – as the e-mail will appear to come from someone he or she knows – the worm will infect his or her computer. It will again go through the address book it finds on the computer and send copies of itself to each address it finds there, and the cycle is repeated. In many cases, these e-mails will seem somewhat odd or not quite right – one example of this was the I LOVE YOU worm, so-called because it had the words “I Love You” in its subject line. Attachments with extensions such as “.exe”, “.vbs” and “.sr” should immediately be treated with suspicion, unless you specifically requested files of this kind.



In mid-July 2003 it was reported that unknown individuals presumed to belong to an organised crime group used the technique of hijacking personal computers connected to the Internet and using them as servers to disseminate offers of subscriptions to pornographic websites. The owners of the hijacked computers were unaware of this and had no means of tracing how and when this hijacking had taken place.

Technical pests comprise the final category of malevolent outsiders intent on causing problems. These individuals design malicious code with the intention of causing your computer to perform functions you would

not wish it to perform or to hijack its functions to conduct actions without your knowledge.

Spyware, already previously mentioned, is one example of a (normally) benevolent misuse of your computer that sends information to a third party without your knowledge or consent.

Software such as a Trojan Horse may also be installed on your computer by a hacker without your knowledge, taking advantage of vulnerabilities that are present in virtually all electronic devices. Such software can be activated by a third party while you are connected to the Internet and used, for example, to launch an orchestrated attack on a website by having thousands of such 'slave' computers (referred to as zombies in these circumstances) requesting the same web page from a server or to overload an organisation's e-mail system.

The tools needed to deal with this problem are discussed in section 2.5.

VULNERABILITIES

One of the open secrets of the information technology (IT) industry is that none of its products is perfect. Software, in particular, tends to have many vulnerabilities and most of these remain unknown. There are good reasons why vulnerabilities exist, and these include:

- Software development remains more of a craft than a true engineering discipline.
- Software is designed to perform clearly defined functions. It is rarely (if ever) designed to ensure that functions not part of the original definition cannot be performed.
- Software is hard to read, document and test. The effort put into testing is usually limited to meet deadlines and budgetary targets.

All commercially available software including operating systems (for example Windows) and applications (such as Excel, SAP, and Lotus Notes) contains programming errors and vulnerabilities. The terms and conditions of software licences absolve vendors from any liabilities for such errors and vulnerabilities.

Hackers systematically search for such vulnerabilities. Some of them, the ethical variety, communicate their findings to the vendors to allow them to create updates and fixes. The non-ethical variety exploit any vulnerabilities they find in order to cause disruption.

Even the best software will only be as secure as its installation and configuration. Installing a software firewall but leaving all of its security features “turned off” is not going to offer you much protection. Experience shows that most security failures occur due to simple omissions.

This subject is addressed further in section 2.

ORGANISATIONAL RISKS IN CYBERSPACE

Everything stated in the previous section also applies to an organisational environment, only more so. Organisations, regardless of their activities, can also become the targets of cyber-attacks for a variety of reasons.

INTERNAL ATTACKS

The term ‘internal’ is used to signify an attack by someone who has been given access to the computers and networks within the security perimeter of the organisation. There are two varieties of internal attacks:

- those carried out by an employee;
- those carried out by a non-employee.

Attacks carried out by an employee can be malicious – that is with the intent to defraud, extort, blackmail, harass, sabotage or carry out any other action designed to cause damage. Such actions may be motivated by financial gain, grudges (genuine or imagined) against the employer or by acute stress or psychological disorders.

The employer is protected from such actions through legislation. However, such legislation is very inconsistent around the world and the only example of international legislation covering this area is the Council of Europe Convention on Cybercrime.

Depending on the nature of both the organisation and the offence, penalties may include the immediate dismissal of the employee or transfer to some unattractive function and/or location.

Employees who are unaware of the nature of cyber-attacks can inadvertently be their instigators, for example, by opening an e-mail message containing malicious software and thus allowing it to infect the rest of the organisation's networked computers.

Non-employees with access to an organisation's computer systems and networks can take many forms: agency personnel filling-in for other individuals, who might be on holiday or sick, contractors working on a project in the building, consultants engaged by the organisation and given office space and facilities, maintenance engineers, in particular for the computer and telecommunications systems, building cleaners and visitors.

A non-employee's motivation will more or less match an employee's but the targets may surpass those of the employee, in particular in the case of theft of intellectual property, industrial (or other) espionage or ideologically-driven sabotage (cyber-terrorism).

Any one of these individuals could launch an attack from within the organisation's security perimeter if they possessed the combination of intent, motivation, knowledge and access. The last element has already been willingly granted by the organisation. The other three depend on the individual in question, and this is true for other forms of snooping and espionage too.



Many of these non-employees utilise the techniques of "social engineering" – tricking employees into revealing passwords or other information to gain access to the target organisation's facilities and systems:

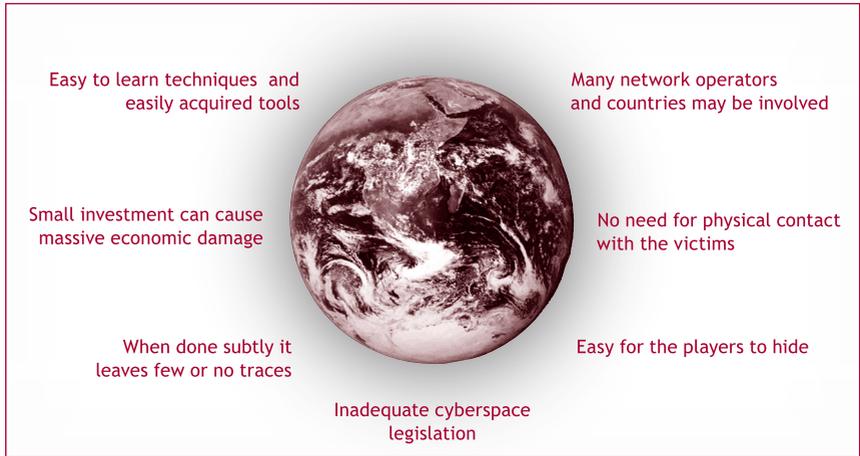
- A person may pretend to be a maintenance engineer to gain access to a computer room. An engineer's presence is rarely questioned.
- Another scam involves calling the help desk from an internal telephone extension and pretending that a password survey is being conducted. In this way a legitimate user ID and password can be obtained from the help desk.
- A visitor may pretend that he urgently needs to access his e-mail account and request the loan of a computer connected to the network "for a few minutes".

EXTERNAL ATTACKS

In order for external attacks to succeed, attackers first need to penetrate an organisation's security perimeter. In practice, this is not as difficult as it might seem because "hackers", the individuals who possess the knowledge and motivation to break into networks and systems, are very well organised and like to share their experiences and tools.

Many hacking tools are readily available from many sources on the World Wide Web. Some are free and others can be purchased for modest sums.

The features of cyberspace – the virtual world of data and software – that render it a suitable place for committing crime and, possibly one day, a theatre of war are summarised below:



If individuals and organisations that rely on information technologies do nothing in terms of building adequate protection measures, they are more likely to become the victims of an attack in one form or another.

Protective measures cannot guarantee 100 percent security, but this is also true of the locks and burglar alarms we fit in our homes and cars.

The way to deal with this problem is discussed in section 2.5 on personal firewalls.



SECTION



2

Building effective personal defences for navigating in cyberspace

*Fidarsi è bene. Non fidarsi è meglio.
(It is good to trust. It is better not to trust.)*

Italian proverb

PROTECTIVE MEASURES FOR INDIVIDUALS

You do not need to be a technical wizard to put a set of effective protective measures in place.

ESSENTIAL MEASURES

- 1. Ensure the physical security of your computer(s).**
- 2. Install trusted, licensed software from reputable vendors.**

Carefully store the original media (usually CD-ROMs) on which the software was obtained. Immediately make a backup CD-ROM of any software that you download. Always keep all the registration and activation codes that came with the software. Please note that some software, for example Microsoft Office XP, only allows one installation on a fixed computer or notebook, and that this is electronically controlled by the vendor to avoid software piracy.

If you plan to install “shareware”, software available at a very low cost, or “freeware”, software available free of charge, take the time and trouble to find out if it is any good. One reliable source of information on shareware and freeware can be found in the Downloads section of the ZDnet website: <http://www.zdnet.com>.

Regularly check for updates on the software you use at the vendors’ websites. Most of these updates – also known as patches – correct programming faults in older versions of the software, and sometimes introduce new errors that are then cured by a subsequent update. Updates are normally available free of charge.

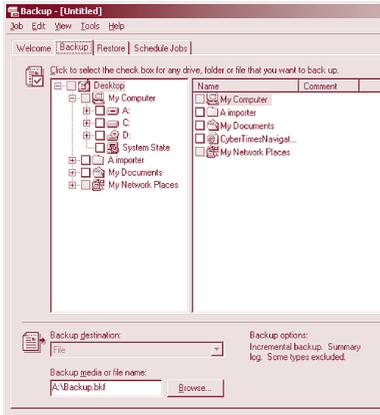
Do not configure any software other than anti-virus packages and personal firewalls (discussed below) to automatically download and install updates. If the computer is on loan from your employer, responsibility for loading updates and managing the computer’s configuration should ideally rest with the employer’s technical service.

If the computer is yours be aware that with some updates, particularly those for operating systems, there is a remote risk of creating

problems with your computer to the extent where only expert help can restore it.

3. Regularly back up all your data.

A backup is simply a copy of a computer file or files. Copies can be made on various media, such as a separate hard disk, a CD-ROM or a tape cartridge.



Backups come in several categories, including: 1) a complete backup (a copy of every file as it is at the moment of copying) and; 2) an incremental backup (a copy of only those files that have been changed after a certain date).

The incremental backup is much smaller and therefore faster to do, but a regular complete backup (once a week or twice a month) is easier to manage and use if the need ever arises to have access to the copies.

Because there are several versions of Windows in current use (Windows 95, 98, Millennium Edition (ME), 2000, XP, NT as well as other earlier ones), the way in which backups are carried out will differ for different environments.

In Windows 2000, the backup utility can be accessed through the following procedure:

Start Programs Accessories System Tools Backup

To select between a complete and an incremental backup, select from this panel: Tools Options... Backup Type (tab)

This utility is perfectly adequate, as is its help facility. However, some individuals do not find it particularly user-friendly. Older versions of Windows do not offer the same flexibility.

If you judge this utility, already installed on Windows computers, to be inadequate there are other relatively inexpensive (and some free) backup utilities. For a reliable source of possible alter-

natives, consult the Downloads section of the ZDnet website (<http://www.zdnet.com>).

Today, since the amount of data to backup has become large it has become necessary to use the CD-ROM as a storage medium. Consequently, the absence of a CD recorder in a personal computer becomes a serious limitation to the backup process.

Backup disks should be clearly labelled and kept in a suitable place. Ideally, they should be kept separate from the computer (otherwise, in case of a fire, for example, the backups would be lost together with the computer).

4. Install anti-virus software.

Anti-virus software is designed to identify malicious code through its unique signature (similar to the DNA of a micro-organism) and to remove it before it can infect the computer.

Good anti-virus software should be able to deal with viruses (which require an infected program to be run before they can replicate) and worms (which use self-replicating attacks and scripts (.vba files)) as well as with Trojan Horses and will also scan incoming and outgoing e-mail messages to prevent infection via this route.

The screenshot shows the Norton SystemWorks interface. The title bar reads "Norton SystemWorks". The main window has a navigation bar with "Home", "LiveUpdate", "Options", and "Help". On the left, there are several utility buttons: "Norton Utilities", "Norton AntiVirus", "Norton CleanSweep", "Web Tools", and "Extra Features". The "Norton AntiVirus" section is active, displaying "System Status: OK" with a checkmark. Below this, there are two main sections: "Security Scanning Features" and "Virus Definition Service".

Security Scanning Features	
<input checked="" type="checkbox"/> Auto-Protect	On
<input checked="" type="checkbox"/> Email Scanning	On
<input checked="" type="checkbox"/> Script Blocking	On
<input checked="" type="checkbox"/> Full System Scan	02-May-03

Virus Definition Service	
<input checked="" type="checkbox"/> Virus Definitions	08-May-03
<input checked="" type="checkbox"/> Subscription Service	29-Apr-04
<input checked="" type="checkbox"/> Automatic LiveUpdate	On

On the right side of the "Security Scanning Features" section, there is an "Item Details" box. It contains the text: "The items marked in red need your attention." and "Please select an item by clicking on the item at left in order to get more information and take the necessary action." The Norton logo and "symantec." are visible in the bottom left corner, and "Norton SystemWorks™ 2003" is in the bottom right corner.

A Trojan Horse is malicious code hidden within what appears to be a useful or harmless program or data. When activated, it can gain control of your computer and cause damage to the file allocation table on the hard disk, for example. A Trojan Horse may be spread as part of either a computer virus or worm.

Anti-virus software is rarely free – typically it costs in the range of US\$30-40. It usually comes with an updating service (called “Live Update” in the example shown in the picture above) that is free for the first few months of use. After this period, it is necessary to subscribe to the updating service for a modest sum of money – considerably less than buying a new copy of the software.

Updating malicious code definitions is absolutely vital as such software evolves very quickly and new designs emerge all the time. If not updated, your anti-virus software is as good as useless.

Most protection software will automatically search for updates every time your computer is connected to the Internet and it is recommended that you leave this option always “turned-on”. This is the simplest and most effective way of ensuring your protection is up to date.

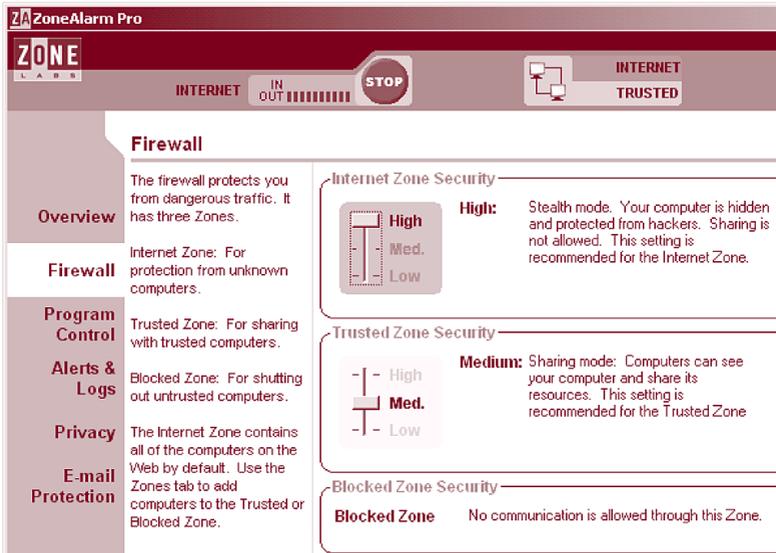
OPTIONAL MEASURES

5. Consider installing a personal firewall.

A personal firewall is software designed to protect a single Internet-connected computer from intruders. It is particularly useful for users with “always-on” connections such as DSL or cable modem. Such connections use a static IP address that makes them vulnerable to hackers.

Personal firewalls protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user’s computer, filtering inbound and outbound traffic and alerting the user to attempted intrusions.

Software firewalls can be obtained free of charge from various sources but have more limited functionality than commercial products, which cost in the US\$25-50 range.



The more elaborate firewalls provide added functions such as blocking banner advertisements and pop-up windows and allowing greater control of cookies than is available through a browser.

For a firewall to be effective, it must be properly configured and kept updated.

A selection of personal firewalls, as well as a discussion of their features and how they are regarded by their users can be found on the ZDnet website (<http://www.zdnet.com>) as well as others.

6. Carefully choose which e-mail package to use.

While Outlook Express (integrated with MS Internet Explorer) and Outlook (integrated with MS Office) are excellent products they have become the prime targets for virus writers because there are millions of copies of these programs in use around the world.

By targeting an e-mail system, the writers of malicious software use



The Best Email Software Just Got Better and - It's Free!

the addresses found there to select the targets to which the malicious code will be propagated. Many other e-mail packages are available, most of them free or very inexpensive.

Examples of such alternatives include Netscape (<http://www.netscape.com>), which combines an alternative browser to Microsoft's Internet Explorer with an e-mail package that – so far – has not been the subject of as much attention of malicious code writers as Outlook Express.

Other well established and popular free e-mail packages are Eudora and Pegasus Mail.

For more details consult <http://www.eudora.com> and <http://www.pmail.com>.

7. Consider a package to deal with spam, junk mail and spyware.

Many products can help you deal with spam, junk mail and spyware, by allowing you to define a list of “friends” whose e-mail will always be accepted and a list of “strangers” whose e-mail will be “blacklisted”.



It is possible to limit spam by using the filters available in an e-mail package. This is usually not as effective as using specialised anti-spam software, but it helps to contain the problem.



The package illustrated here as an example allows you to examine e-mail messages before they are downloaded from the server to your computer, and to delete, bounce or blacklist any undesired messages.

Some packages of this kind are available free of charge and commercially supported versions would normally cost between US\$15-25.

A decision whether or not to install such a program will depend on the amount of spam and junk mail you receive.

For those individuals who wish to maintain an even higher level of privacy other packages which can remove spyware are also available.

8. Consider a package and service allowing you to become anonymous on the Internet.

As the advertisement below states, “nearly every time you surf the Web, you’re getting tracked”. Your Internet Protocol (IP) address can be a source of information about your geographical location, your browser, and your computer configuration. In addition, potentially personal information can be read by the websites you visit.

FACT: Nearly every time you surf the web, you’re getting tracked.

The experts agree: "USE ANONYMIZER TO PROTECT YOURSELF!"



Anonymizer
Private Surfing 2.1

Eliminates online tracking and makes your surfing invisible.

Moreover, many websites create cookies. These are small text files stored on your computer and used by websites to keep track of you. For example, cookies may store your identity and password, as well as additional information, like the date and time of your last visit.

The above advertisement also states that you can use that product to:

- surf at work without being monitored by your boss;
- shop online with extra security;
- download pictures, movies and photographs in complete privacy;
- keep your personal information away from spammers;
- stay invisible to the websites you visit and online advertisers.

In this booklet we have already suggested that we consider the first and third of these possibilities to be Bad Ideas when they involve activities unrelated to your work.

9. Consider using encryption.

Encryption is a technique for converting data (normally text) into a form that is incomprehensible to anyone without a decryption key. The concept of encryption is nearly as old as that of writing itself and many books and articles are available on the topic.

Encryption of electronic data is widely used at various levels of sophistication. The more complex the encryption key, the harder it is to break. Ordinary encryption mechanisms are based on mathematical algorithms and can therefore always be broken given enough time and computing power.

On the other hand, the encryption mechanisms used by those who need the highest level of confidentiality (governments, financial institutions dealing with very large transfers of funds, the military) are of a much more complex nature and, in theory, unbreakable without inside knowledge.

For the purposes of this booklet, we will discuss just one e-mail encryption program - PGP ("Pretty Good Privacy") - as it is the de-facto standard for e-mail security.

Users outside the US can exchange PGP encrypted e-mail if they have the correct versions of PGP installed at both ends. Unlike most other encryption products, the international version is just as secure as the domestic one.

PGP can be obtained free of charge from this website <http://www.pgpi.org>. Once you install PGP you must register the public key that your PGP program gives you with a PGP public key server. This allows the individuals with whom you exchange messages to find your public key.

Network Associates maintains an LDAP/HTTP public key server that has 300,000 registered public keys. This server has mirror sites around the world.

PGP products

PGP is the name of a program originally written by Phil Zimmermann in 1991. Later versions have been developed and distributed by MIT, ViaCrypt, PGP Inc., and now Network Associates Inc. (NAI). But PGP is also a standard (RFC 2440: [Open PGP Message Format](#)). The following is a list of various PGP products that aim at supporting this standard.

- ▶ [PGP](#) : the *de-facto* standard for email encryption (173)
- ▶ [PGPdisk](#) : encrypt entire disk partitions (2)
- ▶ [PGPfone](#) : make secure telephone calls using a modem or over the Internet (6)
- ▶ [SDKs and programming libraries](#) (12)
- ▶ [The GNU Privacy Guard \(GnuPG\)](#) : free command line PGP replacement (2)
- ▶ [Tools, shells and plugins](#) (2)
- ▶ [Various PGP derivatives](#) (4)

As the screenshot on the left shows, PGP products can also be used to encrypt the files stored on your computer so that they are unreadable by other users or intruders. This will protect the information on your computer in the event that it is lost or stolen.

Another emerging service, somewhat related to encryption, is that of digital (or electronic) signatures. A digital or electronic signature is a device used to authenticate the identity of the sender of a message or the signer of a document, and can also ensure that the original content of the message or document has not been changed in the time between its transmission and reception.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate also contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is authentic.

Digital signatures can be obtained from a number of providers in the USA such as Yozons and Verizon. In Europe the situation continues to be under development.

OTHER GOOD PRACTICES

The days when personal computers were simple are long gone. Today's operating systems and applications are based on large complex software which usually has many vulnerabilities.

Moreover, the technical complexity of a current personal computer makes it necessary to keep good records of what has actually been installed and how the machine is configured.

Many external services also place demands on computer users to ensure that their privacy, identity and transactions are adequately protected. This section presents a few practices known to be effective in achieving this.

10. Install a PC auditor and consider having a clone of your hard disk.

Do you really know what you have inside your computer (in terms of both hardware and software)? Probably not. Should you know? Definitely!

The difficult way of doing this is to navigate through all the utilities that come with Windows and produce your own list. The easier way is to use software that performs this task for you automatically.

At least one such program is available free of charge and works well: the Belarc Advisor, downloadable from <http://www.belarc.com>.

BELARC Advisor

PC Audits in Your Web Browser!

The license associated with the Belarc Advisor product allows for **free personal use only**. Use on multiple PCs in a corporate, educational, military or government installation is prohibited. See the [license agreement](#) for details. The information on this page was created locally on your PC by the Belarc Advisor. Your computer profile was not sent to a web server. [Click here for more info.](#)

Computer Profile Summary

*Computer Name: Edward-8fgvmozr
Profile Date: Saturday, May 10, 2003 18:18:06
Advisor Version: 5.0m
Windows Logon: Edward Gelstein*

[Click here for Belarc's PC Management products, for large and small companies.](#)

Operating System	System Model
Windows 2000 Professional, Service Pack 1	Dell Computer Corporation OptiPlex GX150 System Service Tag: 2V0M60J Chassis Serial Number: 2V0M60J
Processor *	Main Circuit Board
1000 megahertz Intel Pentium III 32 kilobyte primary memory cache 256 kilobyte secondary memory cache	Board: Dell Computer Corporation OptiPlex GX150 Bus Clock: 133 megahertz BIOS: Dell Computer Corporation A10 07/29/2002
Drives	Memory Modules
19.96 Gigabytes Usable Hard Drive Capacity 14.04 Gigabytes Hard Drive Free Space	256 Megabytes Installed Memory 256 Megabyte Module Size - 1 Installed One Memory Socket is Empty

If your computer is critical to you, an option that requires an investment of some US\$200 is to buy a second hard disk and use a program such as Drive Image (from <http://www.powerquest.com>) or Norton Ghost (from <http://www.symantec.com>). These programs can access all the files on your computer to create a compact clone (“image file”) of the contents of the hard disk, including how the files are laid out. These products are smart enough not to copy the empty parts of your disk but the relatively high cost of such programs can only be justified if the computer is a critical article for you.

11. Consider having a file shredder.

One of the misleading terms related to the world of personal computers is “delete”. What actually happens when a file is “deleted”? It is only marked for deletion, i.e. the space it takes up is designated free and usable. This means that until that space is used up by a new file, the old “deleted” file can still be retrieved by using one of the many available “unerase” or “undelete” utilities.

The only way to ensure that a file cannot be recovered is to use a shredder utility that destroys files permanently by overwriting their contents. Many such utilities are available but because specific versions are needed for the different versions of the Windows operating system (95, 98, ME, 2000, XP), anyone interested in such utilities (many of the versions are free or cost under US\$20) should use a search engine to look for them, for example by using the following query string: +shred +PC.

For a selection of products performing this function visit the Downloads section of a reputable website such as <http://www.zdnet.com>.

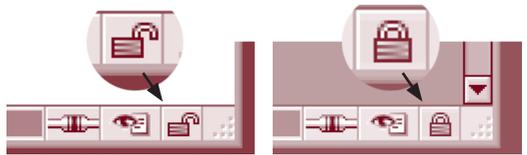
12. https and little padlocks.

The transmission of private information over the Internet is supported by SSL – the Secure Sockets Layer, a protocol developed by Netscape for this purpose. SSL is an encryption mechanism using a public key to encrypt data.

Both Netscape Navigator and Internet Explorer support SSL, and many websites use the same protocol to obtain confidential user information, such as credit card numbers. By convention, whenever an SSL connection is established, the web address of the site starts with https:// instead of http://.

In addition, when an SSL connection has been established, a closed padlock, like the one on the right, will be shown in the browser window

border. NEVER submit personal information to a website unless the URL begins with https:// AND the closed padlock is showing.



13. Smarter passwords.

Passwords are the simplest method of protecting information. They are also the easiest to circumvent because most users do not take much care about the passwords they use and select easy to remember combinations such as their first name, date of birth or dog's name.

However, choosing a more complex password, for example one that mixes upper and lower case characters as well as numbers leads to a different problem.

UM3qAz9T

The password above is a great password but not exactly easy to memorise. In such cases, users often write passwords down, which immediately devalues them as a security measure.



There are many ways to design better passwords, which are also easy to remember. Here are a couple examples of approaches that work well. Select an unusual word of four to six characters from a foreign language. Into this word insert two numbers (your lucky number perhaps?). Make the first letter after the first number upper-case.

Another approach is to use a personal code that converts numbers to letters and vice versa. Choose any words in any language that together have ten characters and that you can easily remember, for example:

Brown Quick

Assign the number 1 to any letter in the sequence, for example the 'Q' and go round until you reach the number 0 (the 'n'). Now convert the eight digits of your date of birth (in dd-mm-yyyy format) to the corresponding letters. A hard-to-break password will be the result.

If you happen to forget it, you can quickly work it out again and destroy the bit of paper afterwards. You can also use this technique to write the letters corresponding to the PIN numbers of any cards you may have on the cards themselves.

If the security policy in place at work requires you to change your password regularly, simply move the place where you place the number 1 to the right or to the left and you will generate a new password.

14. Virus scan all media (diskettes and CD-ROM) before opening any file.

This should become a routine action. Performed quickly, it can help you avoid serious problems. For a description of anti-virus software see section 2.4.

15. Manage the cookies planted on your computer.

Unless you regularly keep an eye on the cookies being placed on your computer, you will have many more of them than you realise as the majority of websites nowadays place or update cookies automatically, unless your firewall and browser configuration prevents this.

If you have too high a level of protection, though, it may prevent you from accessing many websites or doing anything useful on them.

The tools needed to manage cookies are included in your web browser and are simple enough to use. Regular cleanups of cookies, particularly those left by advertisers are a good idea. The same applies to spyware.

To manage cookies with Internet Explorer (version 5.5 or higher), select Tools  Internet Options from the menu bar.

In the middle block, “Temporary Internet files”, of the Internet Options panel click on “Settings”.

In the Settings panel click on the middle button “View Files”.

This will open another window showing all the cookies stored on your computer. Now you can decide which ones you wish to keep and which to delete.



The process of managing cookies with Netscape is essentially the same as for Internet Explorer. In the menu line select Tools and from the drop down menu, select Cookie Manager followed by Manage Stored Cookies.

This opens another panel which gives detailed information about each cookie and allows you to remove them one by one.

16. Electronic footprints.

Every time we use a personal computer, the operating system creates a number of records indicating what was done and when; similar to the footprints we leave behind when walking on wet sand.

The most important of these footprints are:

- the time and date files were last modified;
- the time and date files were deleted (deleted files can be recovered, as discussed in section 2.11);
- copies of all e-mail messages sent/received (until such time as you decide to remove them);
- history of all the URLs you visited (this will be kept for a set period of time that you specify);
- the cookies placed on your computer (see section 2.15).

PROTECTIVE MEASURES IN A CORPORATE ENVIRONMENT

Everything presented in this section is equally applicable to an office or large organisation.

However, several differences should be considered. Managing security in an organisation of any significant size is a fulltime job, and a difficult one at that as it includes more than technical responsibilities and usually becomes a way of life.

An individual or team of people charged with maintaining information security for an organisation need to deal with a much more complex environment than that facing an individual computer user.

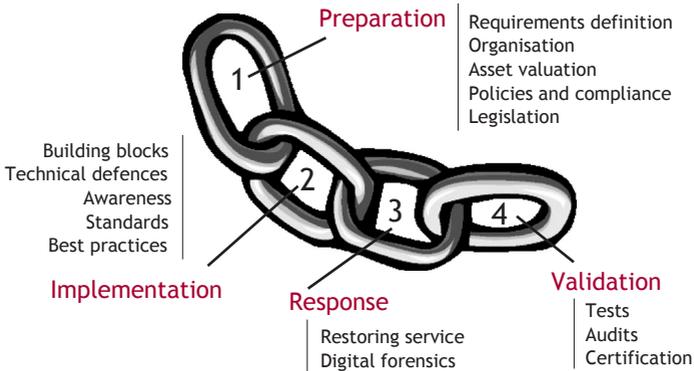
The first thing that makes this environment harder to manage is the problem of scale. The complexity of managing computers grows exponentially as the number of machines involved increases. By the time a network contains ten computers, it will have reached the level of a permanent headache. Anything more than 100 machines is a potential

nightmare unless they are managed in the style of a benevolent dictatorship.

Here’s a quick frightening thought as an aside; the US Department of Defence has well over one million networked computers to manage...

Gene Spafford, professor of computer science and philosophy at Purdue University (USA) said that “Securing an environment of Windows platforms from abuse - external or internal - is akin to trying to install sprinklers in a fireworks factory where smoking is permitted.”¹

A second complication arises due to the range of activities involved. This topic falls outside the scope of this booklet, but a summary can be found in the diagram below showing the four distinct groups of activities involved: development, management, maintenance and testing on a regular basis.



One of the most important factors in supporting information security is the level of awareness of all users of the issues and problems involved and their level of cooperation in supporting the efforts to maintain security.

An excellent description of a recommended approach for organisations can be found in the International Standard ISO 17799 document, “Code of Practice for Information Security”.

¹ URL <http://nativeintelligence.com/itsec-quips.asp>

WHAT TO DO IF SOMETHING BAD HAPPENS

The possibility that one day you'll have to deal with a security problem cannot be excluded. The two most important pieces of advice to remember are: 1) do not panic; and 2) try to prevent the problem from spreading from your computer to someone else's.

If the problem occurs at work, the first thing you should do is contact the Help Desk or Technical Support without attempting to fix the problem yourself.

If the problem arises from malicious software, and it occurs away from the office and you have to deal with it yourself, begin by disconnecting your machine from the Internet and any other network to which it may be connected. At this stage do not turn your machine off.

Your antivirus software should detect this malicious code and isolate it – put it in a quarantine area. Then you can take whatever action is appropriate. If it does not and you see no way of dealing with the problem you may wish to seek expert advice from a company providing a PC clinic service.

In the worst case, you may have to clean your computer by re-installing all of the software. Do not attempt to do this alone if in doubt. Consulting an expert is well worth the expense.

If the problem is one of fraud, for example, the theft of personal information such as a credit card number, immediately notify the card issuer and, if you believe it to be a criminal matter, notify the police too as quickly as possible.

In many countries, police forces are equipped to deal with cybercrime and possess the tools and techniques to recover data from your computer which can then be used as evidence in a court of law.

CONCLUSION

Never forget that when you link up to another computer, you are linking up to every other computer with which your computer has ever linked. There are many nasty things out there and many are contagious. Good computer hygiene is essential in minimising the risk of coming into contact with anything nasty.

ABOUT THE AUTHORS

Stefano Baldi

Stefano Baldi is a career diplomat in the Italian Ministry of Foreign Affairs, Counsellor at the Permanent Mission of Italy to the UN – New York. He has also served at the Permanent Mission of Italy to the International Organisations in Geneva, where he has developed several initiatives for the use of information technologies (IT) in the diplomatic community.

Baldi has an academic background in demography and international social issues. He also lectures on the use of internet for ministries of foreign affairs and missions at DiploFoundation's Postgraduate Diploma Course on Information Technology and Diplomacy. Baldi's most recent research focuses on the impact and future developments of information technology in international affairs.

<http://baldi.diplomacy.edu>

stefano.baldi@ties.itu.int

Ed Gelbstein

Eduardo Gelbstein is a Senior Special Fellow of the United Nations Institute for Training and Research (UNITAR) and a contributor to the United Nations Information and Telecommunications (ICT) Task Force and to the preparatory work for the World Summit on the Information Society. He is the former Director of the United Nations International Computing Centre.

In addition to his collaboration with the United Nations, he is a conference speaker and university lecturer reflecting his 40 years experience in the management of information technologies.

He has worked in Argentina, the Netherlands, the UK, Australia and after joining the United Nations in 1993, in Geneva (Switzerland) and New York (USA). He graduated as an electronics engineer from the University of Buenos Aires, Argentina in 1963 and holds a Master's degree from the Netherlands and a PhD from the UK.

gelbstein@diplomacy.edu

Jovan Kurbalija

Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with professional and academic background in international law, diplomacy and information technology. Since the late 1980s he has been involved in research on ICT and law. In 1992 he was in charge of establishing the first Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of successful work in the field of training, research and publishing the Unit evolved in 2003 into DiploFoundation.

Jovan Kurbalija directs online learning courses on ICT and diplomacy and lectures in academic and training institutions in Switzerland, United States, Austria, United Kingdom, the Netherlands, and Malta.

The main areas of his research are: diplomacy and development of the international regime on the Internet, use of hypertext in diplomacy, online negotiations, and diplomatic law.

jovank@diplomacy.edu

NOTES

NOTES