Good Digital Hygiene

A guide to staying secure in cyberspace

Dr Eduardo Gelbstein



bookboon
The eBook company

Ed Gelbstein

Good Digital Hygiene

A guide to staying secure in cyberspace

Download free eBooks at bookboon.com

Good Digital Hygiene: A guide to staying secure in cyberspace
1st edition
© 2015 Ed Gelbstein & bookboon.com
ISBN 978-87-403-0577-7

Download free eBooks at bookboon.com

Contents

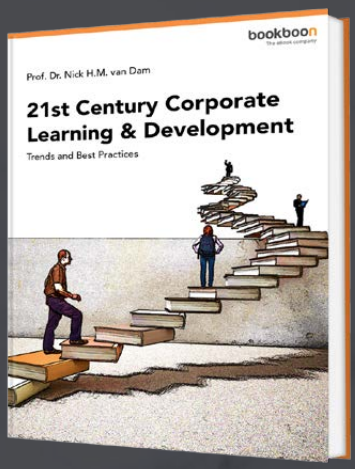
	About the author	**8**
	Introduction	**10**
	Purpose of this book and summary of key points	**12**
1	**A scary story for grown ups**	**18**
2	**The inhabitants of cyberspace's hostile side**	**20**
3	**Good digital hygiene: the essentials**	**23**
3.1	Malicious software	24
3.2	Anti-virus and Firewalls	25
3.3	Use a vault	26
3.4	Bad ideas	27
3.5	Disposing of your devices	28
3.6	Backups	29



Click on the ad to read more

Download free eBooks at bookboon.com

3.7	Passwords	30
3.8	Personal Identification Numbers (PIN)	32
3.9	Choosing software for your devices	33
3.10	Downloads	35
3.11	Sharing your devices	36
3.12	Locking your devices when not in use	38
3.13	Securing online transactions and “https”	38
4	**Your footprints in cyberspace**	**40**
4.1	Who is watching your online activities?	41
4.2	Your browser disclosures	43
4.3	Your cookies	44
4.4	Your disclosures	46
4.5	What others may be saying about you	49
4.6	Your IDs and privacy in cyberspace	50
4.7	Being selective about who is in your network	50
4.8	Social media and Internet Memory	51

Free eBook on
Learning & Development
By the Chief Learning Officer of McKinsey
Download Now


Click on the ad to read more

Download free eBooks at bookboon.com

5	**Hygiene and the cyber-minefield**	**52**
5.1	Spam and scams	52
5.2	Phishing and spear-phishing	54
5.3	Attachments	55
5.4	Click here to follow the link	57
5.5	Unencrypted “free” WiFi (or WLAN)	57
5.6	Encrypting your domestic WiFi	58
5.7	Bluetooth	59
5.8	Log out of everything you do online	60
6	**Beyond the essentials**	**62**
6.1	Inventory of your devices	63
6.2	Crapware, craplets and Scareware	64
6.3	Inventory of all your accounts	65
6.4	Lost your smartphone or your computer?	66
6.5	Tracking software for electronic devices	67
6.6	Remotely wipe the contents of your lost device	69
6.7	Encryption and digital signatures	69



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Click on the ad to read more

Download free eBooks at bookboon.com

6.8	Geo-tagging	70
6.9	Legislation you should know about	72
6.10	Jailbreaking or rooting your devices	72
7	**Good hygiene in the future**	**74**
7.1	Coming your way: the Internet Of Things	75
7.2	Digital hygiene in 2003	79
8	**In conclusion…**	**80**
9	**Other publications and websites**	**84**
10	**Acknowledgments**	**85**



Click on the ad to read more

Download free eBooks at bookboon.com

About the author



At home. © E. Gelbstein, All Rights Reserved

With nearly 50 years experience in the private and public sectors in several countries, Ed has been active in information security through publications, international conferences, workshops and also as an auditor.

After many years as a senior Information Technology manager in the pre-privatised British Rail, he joined the United Nations as Director of the International Computing Centre, a service organization providing services to many international organisations.

Following his retirement, he was invited to joint the audit teams of the United Nations Board of External Auditors and those of the French National Audit Office (*Cour des Comptes*), activities he continued for several years.

He is currently a Senior Fellow of the Diplo Foundation, an entity that provides online training to diplomats around the world. He is also a faculty member of Webster University, Geneva, Switzerland and a guest speaker at the Geneva Centre for Security Policy. He remains a contributor to security conferences in Europe, the Arabian Gulf and Africa.

His publications include several books and articles in peer-reviewed journals. Amongst them:
Information Security for Non-technical Managers", Bookboon, September 2013
"Quantifying Information Risk and Security", ISACA Journal, July 2013.
"Demonstrating Due Diligence in the Management of Information Security", ISACA Journal, January 2013.
"Strengthening Information Security Governance, ISACA Journal, November 2012
"Planning an I.T. Audit for a Critical Information Infrastructure", Chapter 11 of the book "Securing Critical Infrastructures and Critical Control Systems – approaches for Threat Protection" edited by Christopher Laing *et.al.* IGI Global, November 2012
"Law and Technology – Cyberwar, Cyberterrorism and Digital Immobilization", co-authored and co-edited with Professor Pauline Reich, IGI Global, November 2012

Download free eBooks at bookboon.com

"Data Integrity, the poor relation of Information Security", ISACA Journal, November 2011
"Crossing the Executive Digital Divide", Diplo Foundation, Geneva, 2006
"The Information Society Library", a collection of 9 booklets (3 of them on security), Diplo Foundation, Geneva, 2003 (in support of the first World Summit of the Information Society)
"Information Insecurity", United Nations Secretary General's Information and Communications Task Force, September 2002

Ed can be contacted at gelbstein@diplomacy.edu

Download free eBooks at bookboon.com

Introduction

> We learn from history that we don't learn from history
>
> Georg Hegel (1770–1831)

When Hagel wrote this well-known statement, poor hygiene was not recognised as a contributing factor of disease. Several plagues devastated populations over the centuries and the measures taken by the medics of the time did not focus on hygiene – a surgeon would typically wash his hands after performing surgery, not before (and of course no anaesthesia or antisepsis).

Worse still, those in the medical profession who advocated hygiene (like Dr. Ignaz Semmelweis, in Vienna, around 1840) lost their job by offending the medical establishment suggesting they should wash their hands. Then came Pasteur, Lister and many others and everything changed. Nevertheless, plagues continue to exist and hygiene remains an important factor. The problem however has not gone away: an article in Freakanomics published in 2012 entitled: "How to get doctors to wash their hands."



Click on the ad to read more

Download free eBooks at bookboon.com

We should also remember that bacteria and viruses have evolved in pace with new drugs to manage them and now we have resistant strains that don't respond to available drugs. Hospital infections are found around the world.



Figure 1: Memorial to the Great Plague of Vienna, 1679
CC BY bekassine SA

As far as the author is concerned, poor digital hygiene, as introduced here, is at the stage comparable to that existed in Vienna when the Great Plague hit: people are unaware of the need to protect themselves and are not particularly bothered with digital hygiene despite many guidelines and good advice being readily available. In addition, malicious software such as viruses, worms, Trojan horses, etc., continue to evolve faster than the capability of protective products to detect them and clean them.

Every person has a role to play to prevent and/or reduce the impact of a cyber-plague. It may not kill millions of people but could make life quite uncomfortable.

Download free eBooks at bookboon.com

Purpose of this book and summary of key points

> Prevention is better than cure
>
> Desiderius Erasmus (Dutch philosopher, 1466–1536)

Devices such as computers of various shapes and sizes, smartphones and tablets have become commonplace. Being "permanently connected" is a way of life for huge numbers of people and mobility is taken for granted. More devices are expected to join as the Internet Of Things initiatives and innovations advance.

By using such devices to connect to cyberspace – the intangible world of software and data that includes the Internet and its many services (the World Wide Web, the Cloud, Messaging, Sharing and much more) – people may not be conscious that they are visiting a foreign place in the same way as they do when they are physically in another country.

Travellers are advised to take appropriate measures to protect themselves against sickness, loss of belongings, accidents, sickness, etc. Focusing on sickness, sensible individuals take precautions as they known many are common enough, such as the "traveller's tummy" (Montezuma's Revenge, Delhi Belly, the Cairo two-step, and other such names). Some can be serious, such as Dengue Fever and even deadly. Many diseases can be prevented by vaccination (e.g. hepatitis A and B, yellow fever).

Losing one's belongings while travelling is another common event – from waiting at the airport carousel for the suitcase that does not arrive, forgetfulness, pickpockets, muggings, etc. Besides accidents happen… Cyberspace could be thought of a place that one visits because it has some many attractions. It is good to remember that, like physical locations, it has its own culture and language.

Download free eBooks at bookboon.com

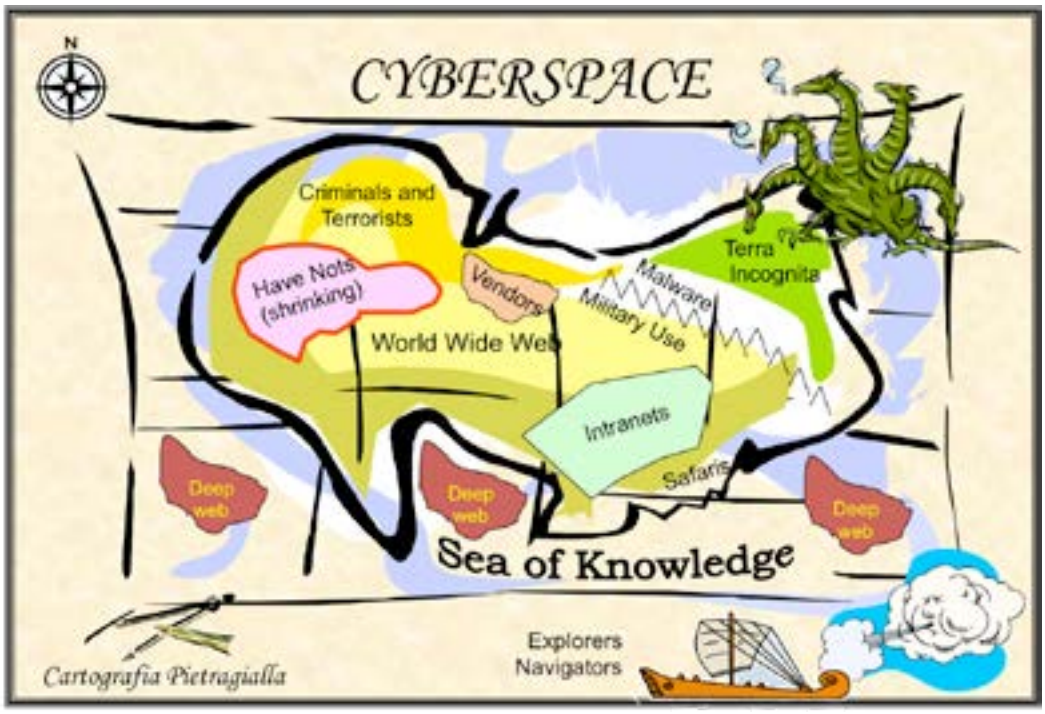


Figure 2: Symbolic map of Cyberspace
© Diplo Foundation 2003. Original design E. Gelbstein

Like all societies, cyberspace has thieves, fraudsters and other antisocial elements. Visitors should adopt sensible practices to protect their well-being. One big difference: you can buy travel insurance for most destinations. There is no such insurance for cyberspace.

This book describes in simple, non-technical language a collection of good practices that can be considered as sensible good hygiene. None of them is obligatory but there is a consensus that these things make sense. It may include terminology that may not be familiar but is nevertheless extensively used in the I.T. industry.

The book is divided in just a few fairly short chapters and includes selected sources for additional material:

Chapter 1: Your information security and the children's story of the Three Little Pigs
Chapter 2: A high level view of the many parties that may compromise your security
Chapter 3: The essentials of good digital hygiene
Chapter 4: Your footprints in cyberspace
Chapter 5: Landmines to avoid in cyberspace
Chapter 6: Beyond the essentials
Chapter 7: Cybersecurity in the future
Chapter 8: In conclusion…
And the usual Chapters on References (9) and Acknowledgments (10).

Download free eBooks at bookboon.com

Chapters 3 to 6 are written in a consistent format: **What** is the topic under discussion, **Why** it is an issue and **How** it can be addressed.

This book does not focus on any particular technology or vendor. It also does not recommend products but gives pointers on how to find them and independent reviews of their quality and performance. There are hundreds of products to choose from. None of them is perfect (but the vendor may tell you it is).

Innovation is fast and new products emerge all the time while others disappear. The reader should therefore search for details applicable to their choice of technology as well as product comparisons, easily found in the World Wide Web. This approach adopts Confucius's observation made over two and a half millennia ago:

> I hear and I forget. I see and I remember. I do and I understand.

This has, so far, never been disputed or proven wrong. This book lists some 40 simple actions you can take to protect your electronic devices (computers, laptops, tablets and smartphones) and the data they contain. All these actions these are optional. Some of them require a modest expenditure and a small amount of effort, mostly in learning.



Click on the ad to read more

Download free eBooks at bookboon.com

Any of the measures you choose to implement will give you two benefits: a reduced risk of a successful attack on your devices and data and increased knowledge on how to protect yourself and your family, particularly children, in cyberspace.

Anything in this book that may be unfamiliar or incomprehensible to the reader is there for a reason. Search engines and online encyclopaedias are there to help you and you are encouraged to consult them.

There are many publications, magazines and websites for enthusiasts that give step-by-step instructions on how to perform the tasks described in this book and review products that can assist in these tasks.

BEWARE! Some are excellent and well worth following. Others suggest actions that, carried out by someone with limited expertise, could prove to be troublesome and, in a corporate environment a potentially CLM (Career Limiting Move).

There are many reports from reputable sources that bad things happen in cyberspace to ordinary people, to businesses, to government departments, to the military and their suppliers. There are also many sources of guidance and advice (see the References section of this book for a sample) on what are considered to be sensible precautions to take. It would seem that many people either do not know about them or plan to take them "at some time in the future" – the *mañana* syndrome.

The references at the end of the book list a personal selection of reputable and trustworthy sources of information and detail.

One more observation

This experience-based book has been written with good intentions and the author is aware that there will be readers that will regard this material as unreasonably pessimistic, "can't be that bad" and too many things to do. It is therefore *your* choice to implement any measure that you are convinced is reasonable and will give you some value.

Proverbs have stood the test of time as representing an accepted truth and expressing it in a colourful way. In the context of the previous paragraph, one seems very appropriate: "you can take a horse to water but you cannot make it drink" (variants with cows and donkeys also exist).

There is a good case for giving the horse salty biscuits to make it thirsty… hopefully the sections in this book will be salty enough for the reader.

Download free eBooks at bookboon.com



Figure 3: You can take a horse to water…
© CC BY Dishychick, ND

Cyberspace and Yin Yang

In preparing this book, the author had to address several dilemmas:

What topics to leave out: This book is already optimistic by expecting potential readers to roll up their sleeves and implement 40 or so good practices about which they may not know much. Is there a minimum set? Perhaps the contents of Chapters 3 and 4, possibly 5, but don't expect everybody to agree. Of course, this depends on how many hygiene measures you have already adopted.

How much detail to provide on each topic: Would a 400-page manual really be that helpful? Besides, hardware and software change very quickly and newer models may need a different approach. In the end find out for yourself and the knowledge gained will be yours.

How to provide guidelines on what to expect in the near future: This assumes we can make a reasonable guess what this might be. Markets and Venture Capitalists get it right some times, but not always. An invention may be brilliant but it's timing may not be right.

Download free eBooks at bookboon.com

Looking back to 1992, imagine that nobody had, thought about or even wanted a digital music player (MP3) (analogue tape cassette and CD devices were popular), a hand held Global Positioning by Satellite (GPS) gadget, a cellular phone (these were around, about the size of a brick, expensive and a status symbol) or a Personal Digital Assistant (a pocket device that could be used as a diary planner, a note taker, even a communications device). At that time the Apple Newton allowed its users to design their own pizza and the order would be faxed (wirelessly) to be prepared. But the Apple Newton, a very smart design, flopped. Then, many years later of course, came the iPhone and the world changed.

This however, is the bright, warm side of the Eastern thought of Yin Yang – the two complementary forces that make up all aspects and phenomena of life. Both Yin and Yang are present at all times although the boundary between them is not fixed. Please look it up, it's fascinating stuff that helps to see things in a wider context.

This needs to be balanced by the dark side of cyberspace where we find bad things that people are prepared to do to people for whatever reason: persuade, influence, impersonate, bully, malign, harass, cheat, steal, interfere, blackmail, sabotage, fight a "war" and no doubt a longer list could be created. Can anyone wish to be a victim?



Click on the ad to read more

Download free eBooks at bookboon.com

1 A scary story for grown ups

There was a time when we were read stories before going to sleep…some of these stories involved beautiful princesses and knights in shining armour. Others were scary with Big Bad Wolves, Witches, curses, poisons and other nasty elements.

Yet, many of the stories had a purpose beyond getting a child to sleep, and one old favourite, the story of the Three Little Pigs and the Big Bad Wolf, is relevant to this book.



Figure 4: The Big Bad Wolf
© Steve Hathaway, All rights reserved

No doubt you recall that the Big Bad Wolf (BBW) wanted to eat the little pigs (LP). Two of them wanted to play and dance and built their houses quickly – one with straw and the other with branches. Of course the BBW blew them away with little effort.

It was only the third and most serious LP who decided to build a house carefully, using bricks and mortar so that it could not be easily blown away. And so, transferring this story to cyberspace, where there are no BBWs, there are many other characters with malicious intent (Chapter 2).

Download free eBooks at bookboon.com

What can (and does) happen to the unprepared in cyberspace? Here is a short list:

- Devices (computers, tablets, smartphones) stop working properly
- Infection of other devices (and other peoples') by contagion
- Loss of the devices through carelessness, forgetfulness or theft
- Irreversible loss of the data in the devices
- Exposure of personal and corporate sensitive data to various risks
- Exposure to unsolicited e-mail (spam), phishing, spear fishing and scams
- Exposure to unsuitable material (e.g. xenophobic, misogynist, political, pornographic, etc.)
- Risk of your children being exposed to unsuitable material
- Identity theft resulting in financial consequences
- Disclosures you may regret later
- And more.



Click on the ad to read more

Download free eBooks at bookboon.com

2 The inhabitants of cyberspace's hostile side

Most of us think of "hostile" parties as having strong bodies, being armed, faces hidden by masks or helmets and exhibiting menacing behaviour.



Figure 5; Find the hacker – they couldn't be, could they?
CC BY schwgir SA

The reality is that malicious actions in cyberspace involve well educated, smart, creative individuals with a good knowledge of information technology. Any of the above graduating youngsters could be one (or more) of the characters in the list below.

This list is not comprehensive and evolves through human creativity. Gaps in legislation, that develops at a slower rate than new forms of crime, allows hostile elements to act with impunity and immunity.

YOU, accidentally. The author assumes you would not act deliberately against someone else. In fact, you yourself could be the problem when your electronic devices have been compromised and are used to spread malware, spam or messages pretending to be from you but sent by a third party with malicious intent. USB flash memories (also called thumb drives) are notorious offenders.

Download free eBooks at bookboon.com

SOMEONE, deliberately. It does happen, in the form of fraud, sabotage, theft of intellectual property, planting compromising information on someone else's devices, etc. These are legally punishable offences but require the perpetrator to be caught and that the digital forensic evidence complies with legal requirements). It may also involve a non-criminal offence like giving you an infected USB memory as a gift that may not contain malware but has instead copies of copyrighted material.

Individual hackers. They could be anyone, anywhere, with good technical skills who choose to target a specific individual or organization. In 2002, a young Scotsman successfully committed what was described at the time as "the biggest military hack of all times" involving 97 US military and NASA computers. A request to extradite the individual to the USA, where the military hack took place, was denied by his country of origin on humanitarian grounds.

Malware suppliers. The design and distribution of malware has become a business (An article in The Economist referred to this as Crimeware As A Service or CaaS. Custom made malware designed to target a very specific target has been, designed, the best known being the Stuxnet malware used in 2010 to sabotage uranium enrichment facilities in Iran.

Professional hackers. The equivalent of a gun for hire, those who operate unethically specialize in the field of private detectives, industrial espionage and theft of intellectual property. Happily, many such professionals provide a service that tests the effectiveness of protective measures implemented by organizations. Called Ethical Hacking or Penetration Testing, it provides a "second opinion" (for a fee).

Hackers with a cause. Often referred to as "Hacktivists" work as loosely associated groups of individuals who have hacking skills and a particular target in mind (chosen by factors ranging from idealism to protest and revenge).

Cyber criminals. Working alone, in small groups or as part of Organised Crime, their motivation is primarily financial. They are behind the most successful scams that get individuals to give them money because they believe their stories.

Non-state actors. Usually referred to as "terrorists" or equivalent terms, their motivation is the disruption of civil society and governments.

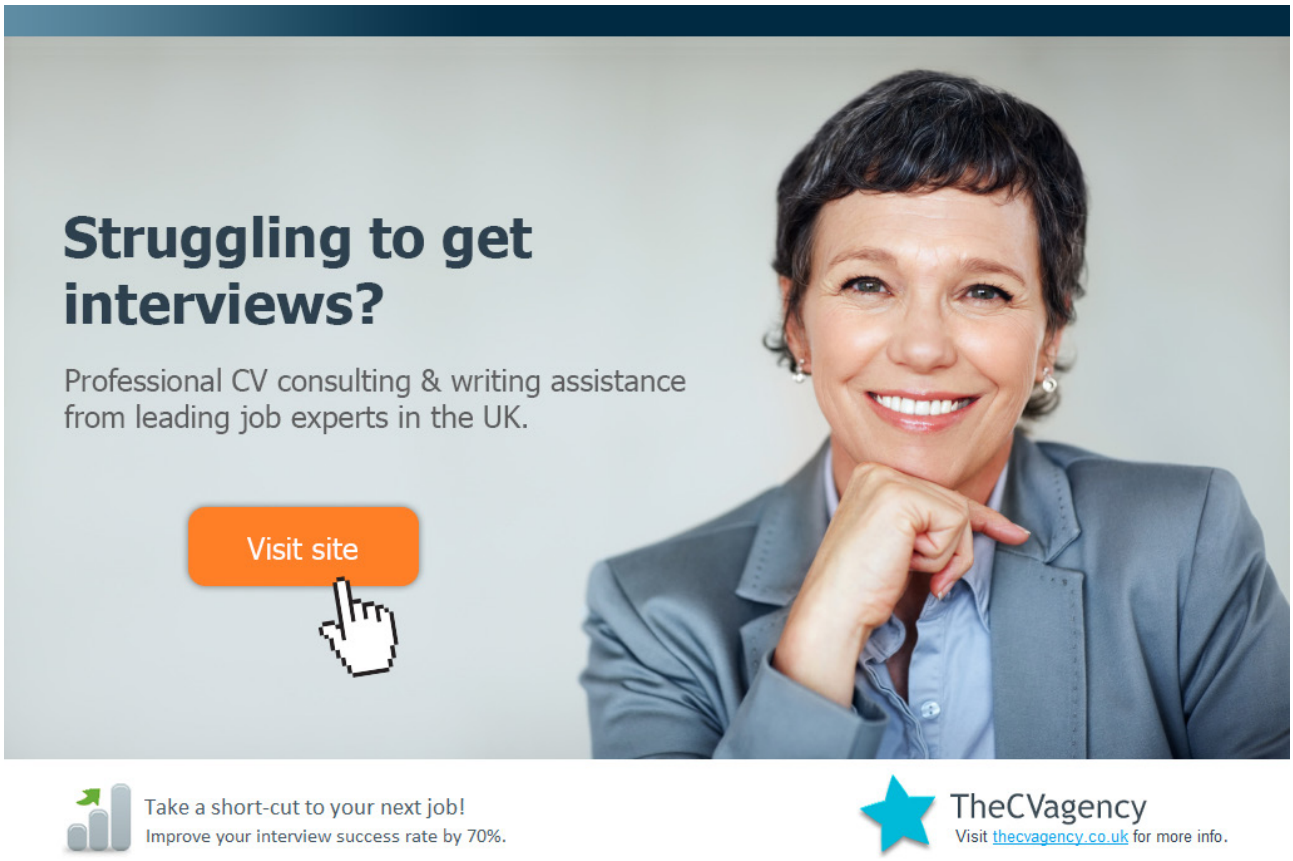
State sponsored. Referred to as "cyber-armies", these are increasingly being mentioned in the Media but rarely, if ever acknowledged by governments. Clearly, the gathering of Intelligence and Counter-intelligence the context of National Security is neither new nor unusual – the tools have changed. There is considerable debate about what might be the appropriate balance between defensive measures and offensive capabilities.

Download free eBooks at bookboon.com

Beyond the above list of players, there are others who provide questionable services such as downloads of music, video, electronic books, etc., that infringe the copyright of their legitimate creator, depictions of extreme violence, child pornography, hate sites and other. I you can think of it, you can find it. The same is true for software that if knowingly faulty or corrupted with malware. Best to be suspicious of "free" versions of software you normally have to pay for.

As there are no editorial controls or quality assurance on the World Wide Web, the contents of the 640 million websites (identified at the end of 2012), these range from trusted, high quality information to incorrect, biased, hateful content designed to mislead or influence.

To gain a quantified understanding of cyberspace, there are several sources of dependable information, such as http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/



Download free eBooks at bookboon.com

3 Good digital hygiene: the essentials



Figure 6: It could happen to you… are you prepared? (design based on many such signs everywhere)
© E. Gelbstein, All rights reserved

It's amazing to think that in 1977 the Chief Executive Officer of a major I.T. company (Ken Olsen, of Digital Equipment Corporation) said that: "There is no reason for any individual to have a computer in their home". While he subsequently clarified that he meant a computer that controlled many functions in the home (heating, lighting, etc.), it is a fact that, at that time, there were few home computers as we know them now and intended for enthusiasts and gamers.

Roughly at the same time, Bill Gates and Paul Allen (Microsoft's founders) talked about a computer on every desk and in every home. They were right but greatly underestimated how fast electronic technologies would be adopted around the world. We are now dealing with more than "a computer in every home" as the average person in the developed world owns several gadgets – desktop computers, laptops, tablets, smartphones (as well as cameras, GPS, game consoles, etc.).

This chapter covers things you should consider doing to fulfil basic requirements associated with their ownership and be reasonably secure in Cyberspace. But there is more to it than the things in this chapter and these are discussed in the chapters that follow. Please remember than 100% security is not achievable and you need to be prepared to respond when things go wrong.

Download free eBooks at bookboon.com

3.1 Malicious software

What is this?

Software designed specifically to make an electronic device perform things it has not been designed to do, almost always to cause damage, steal, corrupt or encrypt data, or otherwise allow a third party to control the device (e.g. to send spam) and cause other headaches.

Malicious software comes in many varieties with names such as "virus", "worm", "Trojan horse", "rootkit", "macro", "logic bomb", "backdoor" and several others. No computing device is immune to such malware: computers, tablets and smartphones are vulnerable and have all become targets.

Why is this an issue?

Malware designers have gone professional and are able to design, share and sell cyber-tools to attack primarily those who are unprepared. Indications to-date suggest that even those who are reasonably prepared can be successfully attacked.

What you should do about it

The actions listed below reflect lessons learned over the years and some of these topics appear several times in this book. The precautionary principle of Better Safe Than Sorry is worth following. The most important measures are:

- Make sure your devices software, including good quality security software is up to date
- Use a security-conscious Internet service provider (ISP) – "free" WiFi may not be secure
- Ensure that the websites you visit are legitimate and trustworthy before you go there – some sites are designed to infect your computer with malware
- Exercise caution when downloading files from the Internet
- Think carefully before installing any new software, particularly those that are "free". If you can, remove software pre-installed in your devices that you do not need or want (see 7.3 "crapware")
- Scan memory devices (such USB devices) that were given to you as a gift or were found
- Be suspicious of random pop-up windows and error messages
- Beware of attachments you don't expect
- Ignore any spam that may get through your filters
- Use security precautions software for your smartphone, tablet and other devices
- Systematically back up your files
- Ensure that your anti-virus software checks the files as they download and quarantines them if necessary
- Behave online as you would in real life: If in doubt, don't do it

Download free eBooks at bookboon.com

3.2 Anti-virus and Firewalls

What is this?

Section 3.1 touched on malicious software (malware) – designed by third parties to cause you inconvenience and/or damage. Your device, be it a computer, tablet or smart phone would normally not include anti-malware features and it is left up to you, the owner of the device, to decide whether you wish to install such protection. There are many products labelled "Anti-virus" or "Internet Security" that monitor data in the computer and peripheral devices (USB flash memories, CDs and DVDs for example) to check that they do not include any known malware.

Many, but not all, devices include in their basic software some form of a firewall – smartphones do not always include one at the time of purchase. A firewall uses a set of rules (defined by their designer) to decide whether incoming or outgoing data traffic should be allowed. It is specifically designed to detect if someone else is trying to access your device.

Why is this an issue?

A computer infected with malware can infect the computers of other people with whom you exchange data, for example an e-mail attachment, infect other devices such as USB flash memories, smartphones, record and send data that should remain confidential such as logins and passwords to allow others to impersonate you and other undesirable things.



Click on the ad to read more

Download free eBooks at bookboon.com

A device unprotected by some form of Anti-virus can be quickly compromised. The same is true without a firewall. Device owners should not underestimate the time and effort involved in cleaning an infected gadget and/or recovering any lost data.

What you should do about it

1. Select and install reputable anti-virus and firewall tools

There is a wide choice of products (some are pre-installed) for all kind of devices. Some are available free-of-charge. Others require an initial payment and subsequent renewal fees. The supplier issues regular, updates to reflect the rapid evolution of malware. Use a search engine for independent reviews of such products.

2. Ensure the selected tool is regularly, ideally automatically, updated

Each product has its specific process for being updated. This invariably requires a connection to the Internet. It is your responsibility to ensure that these updates take place.

3. Regularly scan your device for possible malware and deal with it

Most quality software will automatically quarantine and remove any malicious software encountered.

3.3 Use a vault

What is this?

In the same way as a bank vault can be used to reduce the risk of loss or damage to valuables and important documents, there are software products that perform the same function by creating an electronic vault in your computer or smartphone.

Why is this an issue?

It is prudent to control access to documents containing confidential or sensitive information (for example a list of document numbers, credit cards, memberships and the logins and passwords associated with them. The information stored in the vault is encrypted and access to the vault requires one (good) password. Without this password the data in the vault will not be accessible in a comprehensible format.

What you should do about it

A search engine will list many options for electronic vaults appropriate for the make and model of the devices you wish to use. Some vaults may be free while others require a (modest) fee. The example deliberately omits the name of the vault.

Download free eBooks at bookboon.com

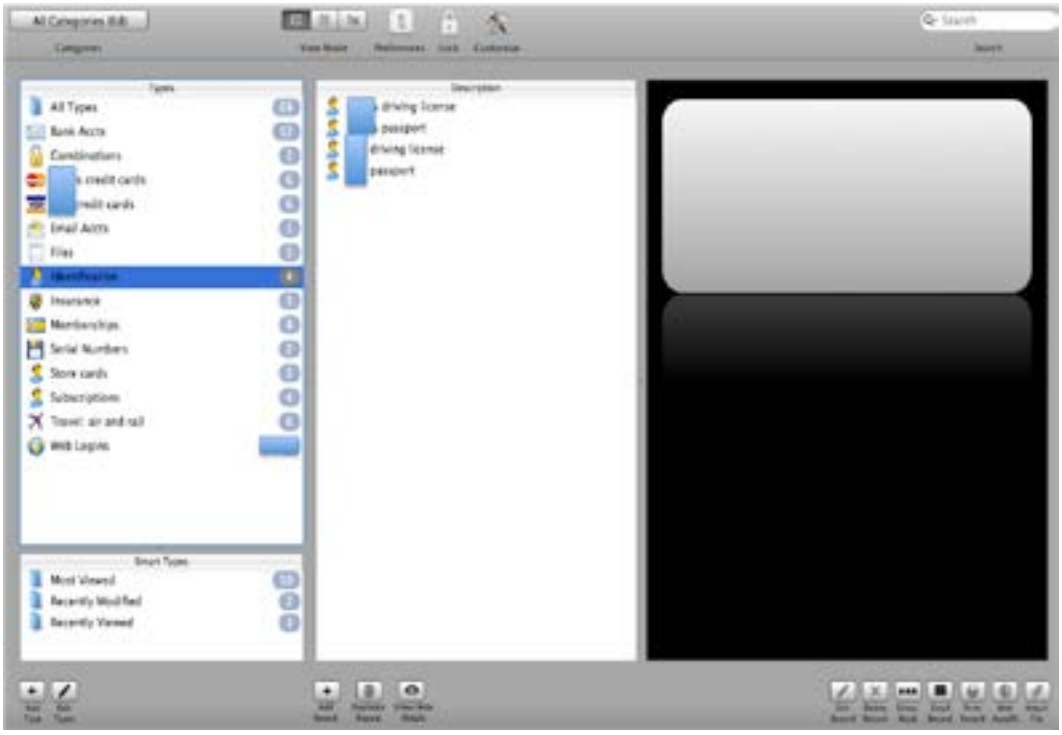


Figure 7: Example of an electronic vault

3.4 Bad ideas

What is this?

There are things you could do in cyberspace that you should always avoid. The list that follows is not exhaustive and is only intended to make you think about what "bad ideas" might look like.

- Having an unprotected interaction with cyberspace (no anti-malware and no firewall)
- Misusing your employer's systems and facilities (personal use of corporate e-mail)
- E-mailing your employer's sensitive material to your personal e-mail account
- Printing, taking screen shots or downloading your employer's confidential information and sharing with others
- Downloading and storing in your devices material best described as "inappropriate" – if deleted it could be easily recovered. If erased or shredded, a digital forensic expert will recover at least a part of it – should this happen you have not idea what trouble awaits you
- Making online comments that could be considered offensive, defamatory or libellous
- Planting malware or inappropriate material in someone else's devices
- You get the idea…

Download free eBooks at bookboon.com

Why is this an issue?

Because, to quote Albert Einstein: "The difference between genius and stupidity is that genius has limits". Therefore, you don't want to live to regret your actions, trivial as they may seem at the time or believing "I'll get away with this". Maybe, but you can never be sure.

What you should do about it

Say NO to temptation.

3.5 Disposing of your devices

What is this?

The day will come when your device has become old enough to be considered outdated, it no longer works properly or has failed and needs replacing. Before taking it to a recycling facility or giving it to someone else, it is prudent to remove all the data it contains – sensitive or not.

Why is this an issue?

Because failure to do so allows someone else to misuse your data, particularly if it is "interesting" as it may contain recorded passwords for your e-mail or other accounts, financial details and, most importantly corporate information about your place of employment.



Click on the ad to read more

Download free eBooks at bookboon.com

What you should do about it

If the device has failed beyond the point that it can be repaired, physical destruction is advisable. If it has a physical hard disk, remove it and take a large hammer to it or saw it in half. If it contains solid-state memory "chips", remove them and break them or burn them.

If the device is just "old" and still works, uninstall all licensed software and remove all the data. Recycle it if at all possible as it contains valuable materials in short supply.

BEWARE: using the "delete" key does not actually remove the data – it just makes available storage space for other data to overwrite it. This allows someone with a little knowledge and some tools to recover what you thought was "deleted".

A better way of removing the data is to use software designed for this purpose with names such as "Erase" or "Shred". Several anti-virus products include such a feature.

3.6 Backups

What is this?

In its simplest form, a backup is just a copy of data (text documents, music and video files, photographs, etc.) that is kept separately from the device in which it is stored. Ideally, the backup should be kept in a secure but accessible place. This applies to computers (and laptops), tablets and smartphones.

Why is this an issue?

Simply because there is merit in preserving and being able to recover data that has value to the person making the backup and may be hard or impossible to replace if lost – for example a video clip of a baby's first steps or words or software purchased online and downloaded, documents of personal value, like the various drafts of this book. After all an electronic device containing such data could fail catastrophically, be lost or stolen.

What you should do about it

There are several choices to backup data. None is particularly complex or expensive.

Offline options: Recent operating systems (Windows and Apple) include facilities to backup your data automatically. Older operating systems that do not, can be complemented with commercially available backup software. The most effective solution is one that performs the backups automatically without a need for manual intervention.

Download free eBooks at bookboon.com

Such backups can be stored in a separate hard disc, ideally physically separate from the computer, a storage device connected to a home network, to a USB memory, a DVD (re-writable or not) or CDROMs. USB memories, while convenient, are easy to misplace, mislabel or lose.

Backups, regardless of what is being backed up take two forms: full backup and incremental backup. In the latter case, only those files that have changed since the previous backup are stored.

Online options: Many Internet service providers and other companies offer backup services "in the cloud", usually for a modest charge. This implies that to access your backed up data you must connect to the Internet.

Use a search engine to find details of products and services for the specific devices you wish to protect.

3.7 Passwords

What is this?

Passwords – something you know – have been used for a long time to authenticate a person's identity. There are other ways of doing this, such as "something you have" such as a device, a card or a SMS enabled cellphone and "something you are", say a fingerprint scanner. All of them are in common use.

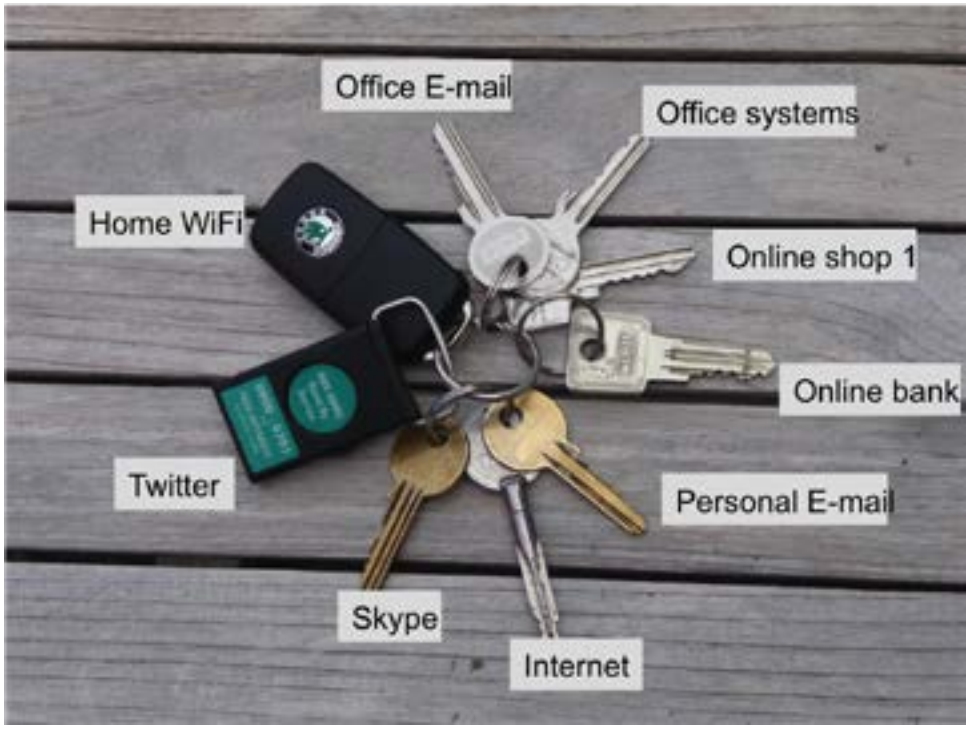


Figure 8: You have many keys – you should have many passwords for the same reason
© E Gelbstein, All Rights Reserved

Download free eBooks at bookboon.com

Why is this an issue?

Because passwords are so widely used, one that is too simple and therefore easy to guess may allow others to impersonate a person and misuse or abuse their privileges. They could do so by making inappropriate postings in a social network, unauthorized online purchases and clean up your bank accounts.

In the same way as we all carry bunches of different keys: front door, garage door, car, desk drawer, etc. good practice requires that the passwords to our computer, vault and all online accounts should be different and hard to guess.

Not surprisingly, people often use the same password for all their devices and accounts. Worse, these passwords tend to be easy to guess. Studies have revealed that one of the most common passwords in use are "password", "123456" or a date of birth.

What you should do about it

The real problem with having many different passwords is that they are hard to remember and therefore, have to be written down. This greatly weakens their usefulness is someone else can get a copy of the written record. One way to reduce this risk is to store the passwords in a vault, as described in a previous section.



Click on the ad to read more

Download free eBooks at bookboon.com

Stronger passwords can be generated in several different ways. One is to mix lower and upper case letters and then replace some letters by numbers. Then add somewhere a non-alphanumeric character, for example 3dW@rd. (strangely enough, some websites only allow alphanumeric characters)

Another way is to do as above by using the first (or second or any other) letter of an easy to remember phrase. For example the password TwBatST@72 uses the first letter of the starting words of Lewis Carroll's poem "Jabberwocky": "Twas brillig and the slithy toves" followed by the @ sign and the last two digits of the year of its publication (1872).

Alternately, there are several websites that generate non-guessable passwords – for example a pronounceable kuxoro22 or an unpronounceable 5+@7kgsq. Some vault products also include password generators.

WARNING: an inability to keep good records of such passwords could cause you considerable trouble should you lose them. A vault and good backup practices are good things to consider.

Unfortunately, there is no such thing as an unbreakable password given enough time and computing power. This is why the use of two-factor identification is growing, particularly by financial institutions and credit card companies.

In two-factor authentication the end user (you) is given a device (looks like a calculator that can read a smart card). This device has its own password (often six digits – see the next section on PINs) and generates a one-time passcode. Other arrangements involve sending a validation code to your mobile telephone. WARNING – by adopting this you may need to carry with you yet another device.

3.8 Personal Identification Numbers (PIN)

What is this?

In the same way as passwords, a short sequence of numbers, usually four to six, are associated with payment cards and smartphones. When an individual has acquired enough of them the challenge of remembering them grows. Not remembering them at the right time can prove inconvenient, as many operators will block the card after three unsuccessful attempts to enter a PIN.

Why is this an issue?

As with passwords, having to write them down is inconvenient and risky as payment cards and smartphones are used in public places and the risk of losing the list of such numbers by accident or theft is real.

What you should do about it

There is an easy answer – write the PIN with indelible ink on the card itself, but NOT as numbers.

Download free eBooks at bookboon.com

To do this find one or more easy to remember words (in any language) that add up to ten characters and in which no letter is repeated. For example: BROWN FLUID or GOD MAKES IT (there are thousands of such combinations).

Select any letter (for example the F in fluid) and make it correspond to the number 1. Thus

B	R	O	W	N	F	L	U	I	D
6	7	8	9	0	1	2	3	4	5

Now, you can convert any sequence of numbers to letters you can write on your card (just don't tell anyone what the words are! A PIN number of 2498 thus becomes LIWO.

3.9 Choosing software for your devices

What is this?

Software makes your devices perform something that you, the owner, considers "useful" and everyone has a different perception of what useful means. There are many ways to categorise software and, this section considers the following categories:

- Operating systems – the basic software that makes the device work – the most popular systems at the time of writing include Windows and OSx (Apple) as well as Android and iOS for tablets and smartphones. There are others (Linux and Blackberry OS amongst them).
- Browsers – used to access the World Wide Web/ Internet. Some are pre-installed and linked to the operating system (Internet Explorer and Safari) and others are available as options (e.g. Firefox, Chrome, Opera, etc.)
- Drivers and other software needed to support peripherals such as printers, scanners, routers, etc.
- Assorted utilities and tools pre-installed by the device vendor or a network provider, including crapware (software you don't need, don't want and would not install yourself)
- Anti-virus and security software – used to protect the device from malicious software.
- Applications software (including Apps) that perform specific functions (ranging from office tools to photo and music editing, etc.) as well as entertainment (games, social media, etc.).

All of the above are available as licensed (and paid for) software, as shareware (the designer and distributor would like a non-obligatory financial contribution) and freeware (no charge to download and use). Some freeware is funded by advertisements that appear every time you use it and other freeware may be questionable in terms of its legality and security features.

Download free eBooks at bookboon.com

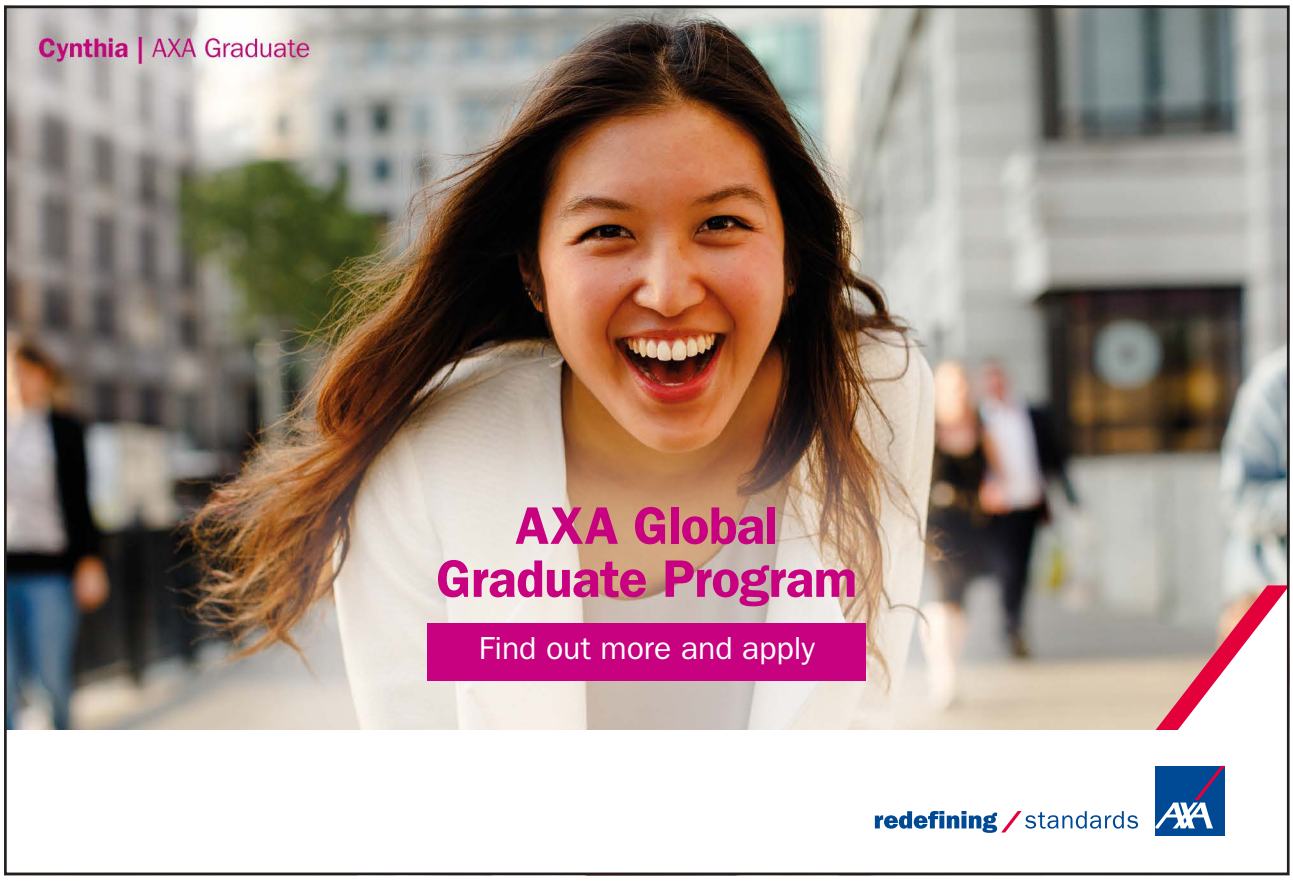
Why is this an issue?

All software should be assumed to contain errors, many of which are not known to the designers or vendors. Some software may also contain malware by design and the designers have no liability (End User License Agreements make this clear). Such malware may allow others to steal data from your computer or use it as a Zombie in a botnet used to disseminate spam or launch coordinated cyber-attacks without your knowledge, let alone consent.

When it comes to apps for smartphones and tablets, it may be worth noting that starting in 2014, the Dutch government is planning to monitor apps that allow individuals to self-diagnose medical conditions. It appears that there are hundreds such applications of unknown origin and quality.

What you should do about it

The prudent choice is to only install software that has some form of Quality Assurance and this implies a reputable vendor. The Quality Assurance process is reflected in the price of the software. Reputable vendors also provide support for their products in the form of updates and support (online, by e-mail or phone).



Click on the ad to read more

Download free eBooks at bookboon.com

Software downloads have become very popular as illustrated by the number of Apps available for smartphones and tablets – in January 2013 there were a reported 780,000 for iOS and 800,000 for Android and the numbers are growing. When it comes to free or really cheap or free software, remember the old adage that "There Is No Such Thing As A Free Lunch". Quality Assurance and support may not be available. None of them has a real warranty. Caveat Emptor.

3.10 Downloads

What is this?

The previous section focused on software. However the World Wide Web (or the "Internet" as many people consider both to be the same) contains many other things that people may want to have copies of such as:

- Material produced by governments, businesses and others posted online with the intention that it be shared and used – usually free of charge but may require some form of registration
- Legally licensed music, books, photographs, magazines, newspapers, etc. These usually require a payment or subscription
- Material that people are willing to share without restrictions e.g. blogs, cookery recipes, photographs and and all kind of other things
- Material that can be downloaded but doing so may infringe its copyright
- Material that can be downloaded at your own risk (inappropriate, illegal, malware, etc.)

The first two categories can be assumed to have the lowest risk of malicious software. Some, particularly commercial websites may insert spyware and adware into your device. The remaining categories may provide items of questionable quality, as there are no editorial or quality controls in the Wide World Web where anyone can be a publisher.

Uploading, downloading and sharing copyrighted material (video, audio, electronic books, etc.) are widely practiced as well as illegal. Many governments are keen to put a stop to such practices through legislation, reporting by Internet Service Providers and law enforcement. Ask yourself if the savings achieved by not paying for a license are really worth the potential complications if caught.

The final category includes truly inappropriate material which, if found on one of your devices could ruin your life.

Why is this an issue?

First and foremost, every download introduces into your devices unknown elements, some of which may not be detectable and, if found, hard to remove. Good digital forensics can recover stuff that you may believe had been thoroughly removed from your devices. The consequences of finding them in your device are unknown until they hurt you.

Download free eBooks at bookboon.com

Many download providers require you to provide personal details, usually an e-mail address and sometimes more to be registered.

What you should do about it

Downloads are an essential tool in cyberspace and, in principle, a useful one as they allow many good things to be shared. Good hygiene requires that:

The source of the download is known and trustworthy – such as a form from your tax authority or a document from a reputable vendor, a book in electronic form for an electronic book reader, etc. should all be considered to be OK.

You should ask yourself the question WHY is the item offered as a download – as a gift, as a well intentioned offer to share, as a means to gain revenue, as a means to collect your personal information, etc. If you don't know much about the source, look them up using your search engine. After all, you tell your children not to accept sweets or car rides from strangers.

3.11 Sharing your devices

What is this?

Some things are intended to be shared with family and friends. Others are designed to be shared with co-workers. However there are many situations where sharing should be limited to exceptional circumstances, i.e. when there is no alternative. A toothbrush is a good example of an item that is not normally shared.

To what extent should you share your computer, tablet or smartphone, your passwords and PIN numbers, etc. and under what conditions?

Why is this an issue?

Imagine that one day you switch on your device and discover that, for example:

- You turn your computer on and the usual screen does not display what you are used to. Worst case it does not display anything, or your password no longer gives you access to your device
- Your mouse cursor has been changed
- You discover that someone else has been reading your e-mails
- You find that new software has been installed without your knowledge or permission

Whoever did this may not know how to put things back as they were and, let's face it, maybe you would not know how to either. Could you really?

Download free eBooks at bookboon.com

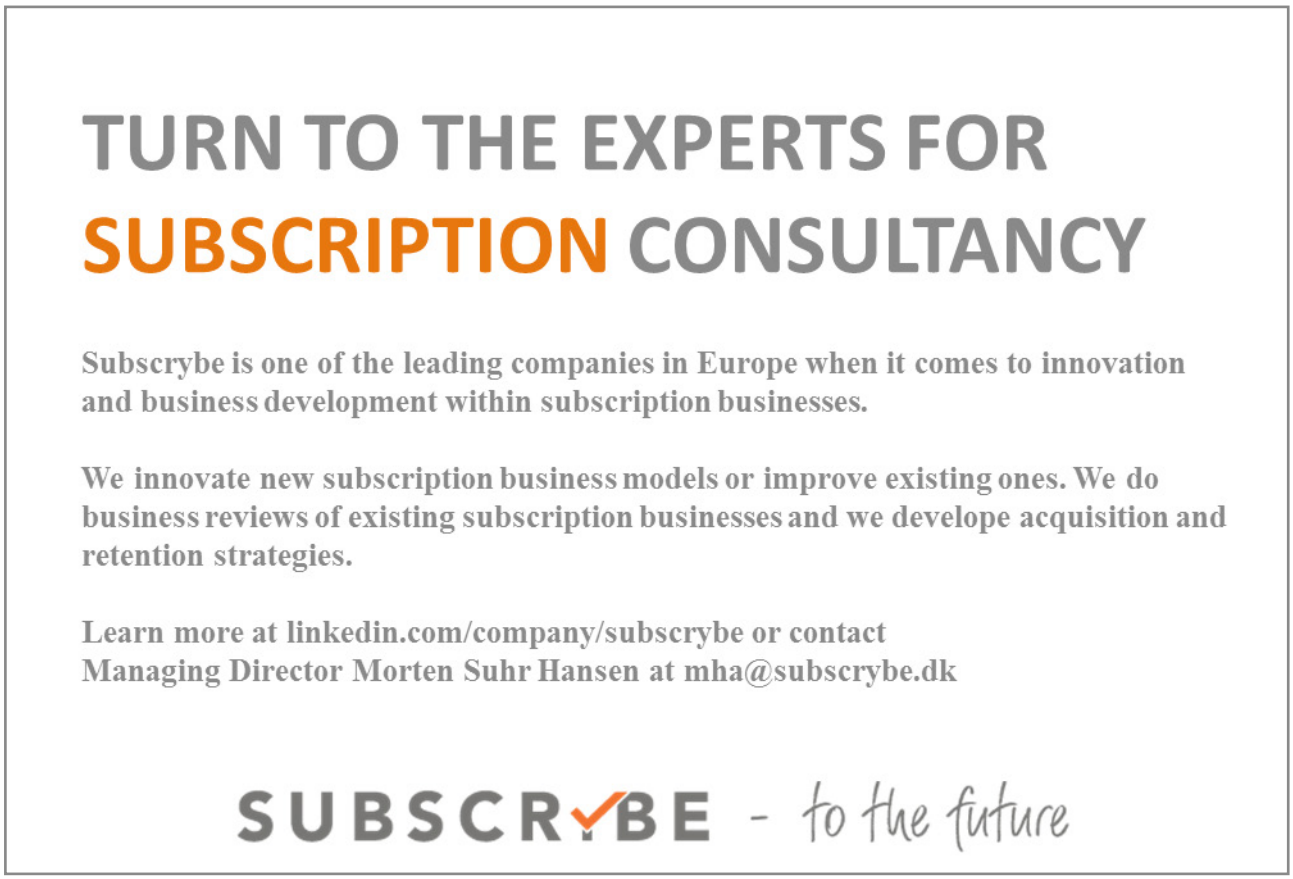
In the workplace, sharing your device with an unknown person is asking for trouble unless this is permitted by design and individuals have individual accounts. When conducting audits the author often asked a person being audited if he could use their computer for a few minutes, to which almost everybody agreed. All it takes is to insert a USB with malicious software to their computer to take control of the network. Such action may not be detected for a considerable time. Best to say: "NO, sorry, it's company policy not to allow third parties to access the network".

What you should do about it

The simplest way to share your devices more securely is to create multiple user accounts. This feature is available for most devices, each of which has somewhat different procedures for doing so. A search engine will give you the details for those you own.

Each account ("Guest", "Child #1, etc.) should define what the individual is allowed to do. You should for example prevent others from installing software or making purchases on your behalf. A search engine looking for "how to set up separate accounts on a (your device name and type)" will lead you to step-by-step instructions.

Many devices also include a Parental Controls feature. How they work and how to set them up can be found using a search engine. While the protection of children going online will not be discussed further in this book there are many websites providing good guidelines, such as
http://www.getsafeonline.org/safeguarding-children/safeguarding-children/



Click on the ad to read more

Download free eBooks at bookboon.com

3.12 Locking your devices when not in use

What is this?

It is good practice to lock your doors and windows when you leave a place unattended to prevent intruders who could steal and/or damage your property. Your electronic devices are no different except that your "property" consists of an intangible asset: your personal data and access to online services, including banking and shopping.

Why is this an issue?

An unlocked electronic device (computer, tablet, smartphone) gives someone who has access to it, with or without your permission, an opportunity to become "you" and do things you would not wish to happen such as for example: install software on your device (perhaps a game?), download inappropriate material, change the configuration of your device (as a "joke") or purchase items on your behalf at your expense.

An additional domestic risk is that of children using the device in the absence of parental controls to purchase games or, worse, come across an inappropriate website, of which there are many. Would you really want to explain to a four year old what those people without clothes are doing on the screen?

What you should do about it

Locking your devices has several dimensions from the simple use of a password-protected screen saver that is activated when the device has not been in use for a given time (that you specify). If the device will not be used for some time it may be best to use features such as "Lock Workstation" (Windows) or Log Out (Apple) and their equivalents for other operating systems.

When using your devices in a public place you should turn off features such as WiFi, Bluethooth, GPS and other such features as these allow others to capture information from your device.

A search engine can provide details of how to use the various locking options and parental controls of your specific devices.

3.13 Securing online transactions and "https"

What is this?

Electronic commerce, online banking and many other activities involve giving a third party confidential information, such as the details of a credit card. It is important that you, the owner of this information should be able to trust the party to which the information is given as well as the process for doing so.

Download free eBooks at bookboon.com

Why is this an issue?

Sensitive information can be misused and abused by people who intercept or acquire it. Credit card information may be used to defraud you, other personal details (name, address, bank account number, social security or tax identifiers, etc.) can be used to steal your identity and allow someone else to be "you" in the online world. It does happen.

What you should do about it

Like discussed in Downloads, trust between the parties is essential but not enough. Exchanges of sensitive and confidential information should only take place if you are satisfied that they use the https (Hypertext Transfer Protocol Secure). You can look this up in an online encyclopaedia or with a search engine – the technical details are irrelevant for this discussion.

The use of https in a website requires that an independent trusted party (a Certificate Authority) vouches for a legitimate website and that the website provides a valid certificate. The use of https also requires that your browser implements it correctly – this is why it is essential that your browser software should always be up to date.

The use of https is essential over unencrypted networks such as WiFi to prevent others sharing this network to be able to discover your confidential information or inject malware into your device.



Click on the ad to read more

Download free eBooks at bookboon.com

4 Your footprints in cyberspace

Happily feeling secure and private behind our screens – regardless of the device used, it is easy to forget that every action in cyberspace is recorded somewhere by someone for various reasons, all of which imply knowing more about you and what you do in cyberspace. Recent media reports have confirmed what information professionals have known for years: monitoring it is possible and we have the technology to do it. Every technology has the potential to be misused and abused.

The sections that follow present the "what" and the "how" of the potential watchers with a few hints of "why".



Figure 9: Footprints – have you looked for yours?
CC BY Andy_3255, SA (flickr)

For the sake of an example, on August 4, 2013, there were media reports about a family from New York State, USA, who were detained and interrogated under suspicion of terrorist activity. The story revolves around "Mother" searching for pressure cookers, "Father" searching for backpacks and "Junior" wanting more information on the Boston Marathon bombings of 2013. The monitoring computers correlated these searches and reported a potential terrorist threat.

Download free eBooks at bookboon.com

4.1 Who is watching your online activities?

What is this?

Given the massive flows of data across the Internet and the global telephone networks it would be impossible for "people" to watch all of it. But what is too much for humans is digestible for computers which can therefore monitor all or parts of all this traffic and be programmed to produce appropriate reports.

Some of the parties that know what you are up to with your devices are the obvious ones like your Internet Service Provider and your mobile communications provider. But there are many others. If you are using your employer's networks and/or devices your activities may be tracked by your employer. Legislation about this varies from country to country.



Figure 10: Big Brother (and his family) are watching you
© E. Gelbstein, All rights reserved

Why is this an issue?

It really depends on how each individual feels about "privacy" and the extent to which each society applies the concept of "freedom of speech". While the latter is the subject of Article 19 of the United Nations Declaration of Human Rights of 1948, the Article recognizes that such freedom has limitations.

The most common limitations include items such as: slander, libel and defamation, the disclosure of confidential information, obscenity, etc. The World Summit on the Information Society of 2003 made a statement on the importance of the freedom of expression for the Information Society. Details can be found with a search engine.

Download free eBooks at bookboon.com

Governments around the world are dealing with the challenge of maintaining a suitable balance between privacy, freedom of speech and national security. What elements of these strategies are communicated to the general public and the legal provisions around them vary from country to country and may change in a relatively short time.

What you can do about it

Recognise that it is hard to be totally anonymous in cyberspace. It is prudent to be aware of the extent to which you (and your devices) collect and disseminate information about yourself and your activities in cyberspace.

On this basis, individuals should take steps to maintain the level of privacy they consider appropriate and use their right to express themselves within the bounds of what is sensible and legal. Failure to do so may lead to unpleasant experiences.

The pages that follow explore how your devices commit indiscretions, how you are making disclosures to others – not all of whom may be known to you – and being aware of what others may be saying about you in cyberspace.



Click on the ad to read more

Download free eBooks at bookboon.com

4.2 Your browser disclosures

What is this?

Every time you connect to the Internet, the browser (part of your device's software) is designed to provide information to whatever you are connecting to.



Figure11: Beginning of the list of your browser's indiscretions (screen capture)
© Eduardo Gelbstein, All Rights Reserved

Many website owners collect this information as it tells them many items of interest: what software you are using, where you are connecting from (your home, a hotel, an airplane, etc.), the language you use, the speed of your connection, and a lot more. Browsers also indicate to each web page the link used to reach it (the referral link). To find out what your browser has to say about your arrangements, visit www.mybrowserinfo.com

Why is this an issue?

Your browser's information is essentially geographic. This means that a multinational company will direct you to their national website – in e-commerce this may result in substantially different prices. Other entities may use this information to block access to copyrighted material (try accessing the BBC iPlayer from outside the UK). When tied together with cookies, privacy becomes an issue to consider.

Download free eBooks at bookboon.com

What you should do about it

Subscribe to an anonymiser service (there are several commercial providers). This implies connecting to the anonymiser's website which acts as a switch, removing your IP address. While not particularly expensive anonymous browsing may raise concerns to observers (everything is recorded these days) along the lines of "does this person have something to hide?"

4.3 Your cookies

What is this?

Cookies came about with the World Wide Web and graphical user interface browsers. Essentially a small amount of data placed in your device by a web server whenever you visit a web page. The purpose of cookies is to personalise the web pages you visit (advertisements, automatically log you in "welcome back Eduardo" or prefilling a data field with your data. They do so by collecting data of what you do on the particularly website and other information stored for your convenience such as login and passwords, account numbers by clicking on a box "Remember me". So far, so good, because websites can only read the cookies they plant.

There are several kinds of "foreign" cookies placed by other parties – advertisers, collectors of statistical data. Tracking cookies are placed by a third-party website, often advertising. These cookies may contain information fed to it from the webpage visited such as the name of the site, particular items viewed, pages visited, etc.

When you later visit another site containing an embedded advert from the same third-party site, the advertiser will be able to read the cookie and use it to know more about your browsing history. This allows them to place adverts specific to you.

Why is this an issue?

Many people see tracking cookies as an invasion of privacy since they allow an advertiser to build up profiles without the consent or knowledge of the individual concerned. This highlights the differences in legal systems concerning the protection of personally identifiable information. In Europe there is a European Directive that has been adopted into national law.

In Europe, each website must state that it will be using cookies and that by agreeing you have given the site implied consent. If such consent is not given some of the website functionality will not work.

Elsewhere there is widespread use of privacy policies often written by lawyers. These are complex and detailed statements of how an entity collects, uses, discloses and manages personally identifiable information. Many, but not all websites have a privacy policy. Most people cannot be bothered to look at them in the belief that they have nothing to hide.

Download free eBooks at bookboon.com

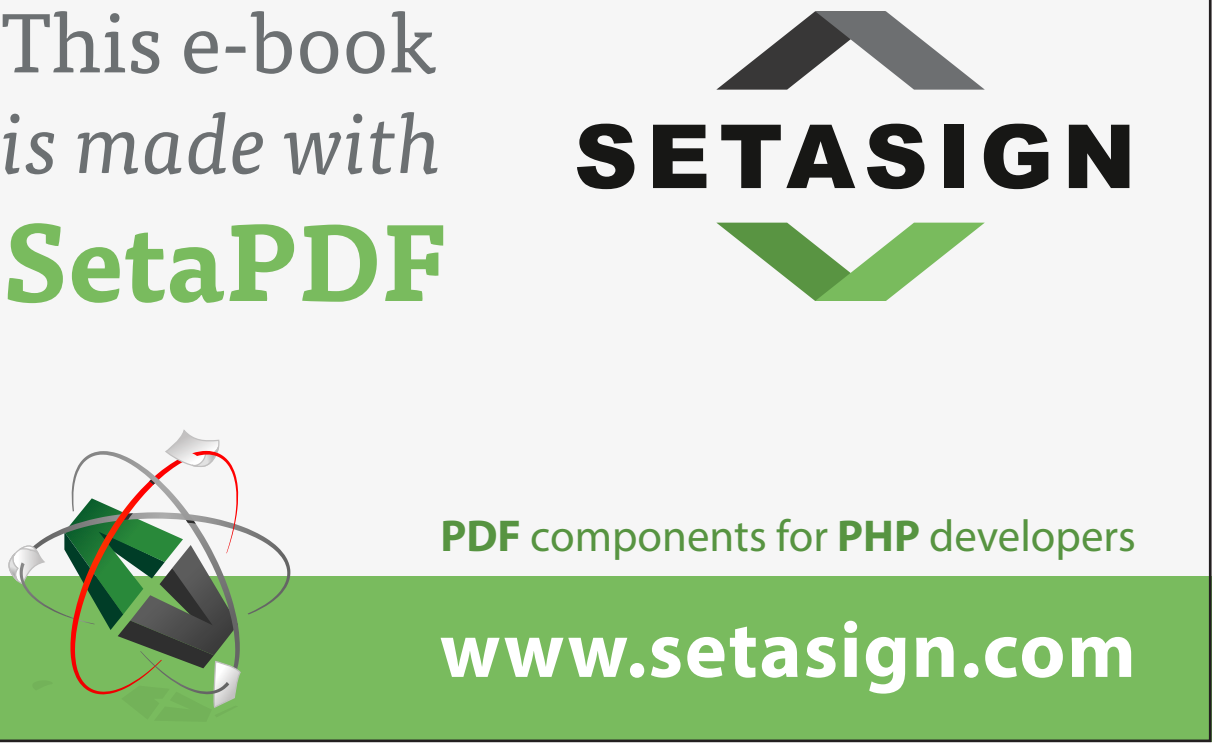
While smartphones do not use cookies, there are products for mobile marketers to track users across devices whenever you synchronise your mobile device and your computer's cookies.

What you should do about it

Verify that the website you visit has an explicit Privacy Policy and read it (or at least try to), then find answers to the following questions:

- Does the website have privacy settings? If so use them and be ungenerous – some websites frequently change their privacy practices.
- Do you know who has planted cookies in your machine and how many there are?
- Would you be surprised if the majority are from places you never heard of?
- Do you know how to delete the cookies in your devices?
- Do you know that you can block and delete cookies in your browser – but it is prudent to find out what the consequences might be before doing so. The author does both regularly without adverse effects – useful cookies are retained.

This e-book
is made with
SetaPDF



Click on the ad to read more

Download free eBooks at bookboon.com

4.4 Your disclosures

What is this?

The Internet and other innovations in Information Technology have fundamentally changed the way in which we interact with organisations, with each other and, in turn, these changes have had a major impact on how we understand "privacy".

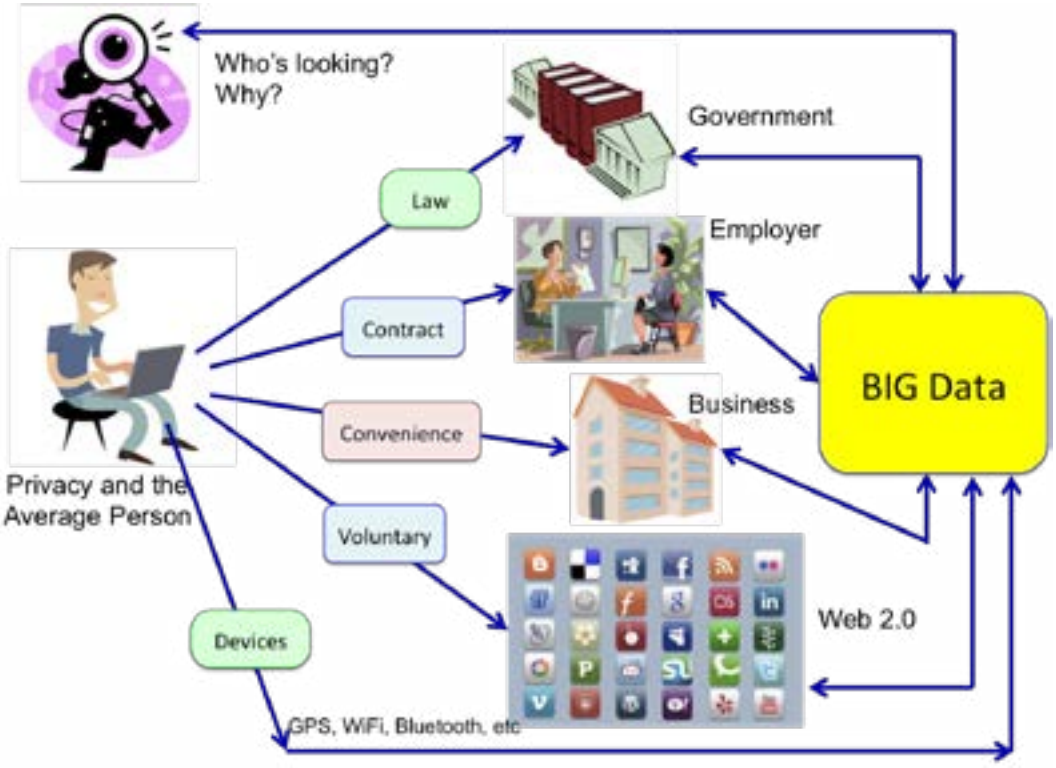


Figure 12: Scope of individual disclosures
© E. Gelbstein, 2013, All rights reserved

The figure illustrates the many information exchanges that begin with us as individuals. This first section on disclosures examines those we do because we are required by law and/or contract.

Disclosures required by law tend to be government requirements. These include civil status (births, marriages, divorces, deaths), property records, taxes, social security, driving licenses, etc. Historically done on paper, the adoption of e-government around the world is moving us into an environment where information about individuals is in electronic form and therefore easier to search (no need to dig into a dusty archive in a dark basement).

Disclosures required by contract include those related to employment, where an individual needs to provide details such as address and contact numbers, dependents, bank accounts, diplomas and certificates, etc. They are also required by banks, insurance companies, airlines and other businesses.

Download free eBooks at bookboon.com

Disclosures for convenience are commonplace as well as optional. In exchange for a Frequent Flyer card and the opportunity to earn miles or points, or a supermarket Loyalty Card that may give you discounts and special offers, people willingly agree to provide a considerable amount of personal information, including a personal profile, address, income and more. Each time any such service is used, the party managing the scheme acquires information about the individual and how it uses the scheme.

Voluntary contributions cover all those things we do because we want to. These may include hotel and restaurant reviews, online comments on news items, blogs and other Freedom Of Speech actions as well as more intimate disclosures on social media – feelings, opinions, photographs and more.

Finally, there are the disclosures made by your mobile devices, particularly those that have networking capabilities (Bluetooth, WiFi, contactless protocols, etc.) and also GPS.

Why is this an issue?

Perhaps it is less of an issue for the two first mandated activities, except that as individuals, we may want some assurances that the information will be used appropriately, be adequately protected and that these processes comply with any relevant legislation. The European Union for example has issued (and is currently updating) a Data Protection Directive that has been implemented by the member countries in ways that reflect their national culture and other related legislation.

Whenever you choose to make disclosures "for convenience", you can expect the party to whom this information has been provided to use it for their benefit, not just yours, and with your explicit consent (sometimes without it) share this information for marketing purposes with what they call "partner organizations". In the worst case you will receive more junk mail in your letterbox or you e-mail in-tray as well as unsolicited phone calls.

Voluntary disclosures require careful thinking because they are irreversible and forever. Various attempts by groups have been made, mostly in Europe, to have "the right to be forgotten" in social media. They remain unresolved and will no doubt be the subject of debate and ethical questioning for years.

The reader may consider (re)-reading George Orwell's book Nineteen Eighty Four (published in 1949) as the book anticipated social developments in society that have become reality. The GPS capability of mobile devices and the ubiquity of video cameras have more than a passing resemblance to "Big Brother is watching you".

Download free eBooks at bookboon.com

What you should do about it

For the first two sets of disclosures: not much. It is prudent to ascertain that the information held about you is correct, accurate and up to date. It is good to remember than financial institutions rely on such information to assess your credit worthiness before granting a loan.

The convenience category is a matter of personal choice. There are people who, in order to maximize their privacy do not even use credit cards and do not join any loyalty schemes. At the other extreme there are the "junkies" who joined dozens of such schemes.

You can say online almost anything you wish, as most societies guarantee you extensive freedom of speech rights. Many countries have introduced legal restrictions on what they consider appropriate use of freedom of speech. Such restrictions include topics such as incitation to harm, offence and hate. An employer would not take kindly to their employees using social media to disclose sensitive information or even criticism. In September 2013 a low cost airline denied boarding to a passenger who used a social media tool to make adverse comments about the boarding procedure.

Items posted on social media must be assumed to be kept forever and require forethought. The "funny" photograph of 2005 could become a major embarrassment in 2015 and the candid comment made about someone else may result in litigation. The challenge here is that social media features encourage spontaneity, the opposite of careful consideration. In cyberspace there is no UNDO function.



Click on the ad to read more

Download free eBooks at bookboon.com

4.5 What others may be saying about you

What is this?

People who know you (and some who don't) may be "talking" about you in Cyberspace and this may range from the positive and helpful to malicious gossip, posting embarrassing photographs and worse. Social media and blogs are the most common channels for doing this. Unfortunately, some items of information about you may go viral and end up being published in the media.



Information security for non-technical managers

By David Lacey on July 18, 2013 10:33 AM | No Comments | No TrackBacks

Tweet 7 | More

It's surprisingly hard to find good quality guidance for business managers on information security, and even harder to find material that is free. Far too much essential reference material is priced beyond the budgets of small enterprises or individuals.

I was delighted therefore to hear that Eduardo Gelbstein has published a free book "Information security for non-technical managers".

For those of you that don't know Ed, he's a highly experienced CIO, former Director of the United Nations International Computing Centre and a fountain of streetwise knowledge on IT Governance. Ed as a good grasp of how to bridge the gap between management theory and business reality.

The book is a good overview of the subject for business managers, IT staff or auditors. It also very kindly references my Wiley book "Managing the Human Factor in Information Security".

Figure 13: Blog posting about the author's other Bookboon book (screen capture)
© Eduardo Gelbstein, All Rights Reserved

What is this an issue?

While you may have little control over what others say about you, it's better to know than to remain ignorant. There have been so many misuses and abuses of social media – where spontaneity displaces thoughtfulness – that have resulted in people losing their jobs for having created embarrassing situations for their employers.

Knowing your public profile on the World Wide Web allows individuals to explore what actions they may wish to take to protect their reputation and privacy, ranging from gaining a better understanding of legal options to consulting a lawyer with specific knowledge and experience of cyberspace legislation.

What you should do about it

Use a search engine and be surprised… this also gives you the option of setting up an alert whenever you (or someone with the same name) is mentioned in a website that allows search engines to access its content.

Download free eBooks at bookboon.com

4.6 Your IDs and privacy in cyberspace

What is this?

Identity Theft if a common crime in cyberspace. Using information collected from multiple sources – and much of this information is readily available to the patient searcher, it is possible to become a "copy" of you that is good enough to allow others to pretend they are you.

This may have only minor impact – the Secretary General of Interpol, Roland Noble, was the victim of this when someone pretended to be him in Facebook, created a page and used it to make "friends" with other senior police officers around the world. This happened again in 2012 and the victim was a senior NATO military official.

Identity Theft becomes a serious matter when financial matters are involved and you – the genuine person – starts getting demands for payment for major expenditures.

Why is this is an issue?

Mainly because of disclosures made in goodwill without thinking of the possible consequences: credit card numbers and other important information sent in an e-mail, personal details revealed in blogs, chats, text messages, web pages and social media can all be used against you and cause you considerable trouble to unravel.

What you should do about it

Remember the words of the North African proverb: "a closed mouth catches no flies" (original: Dans une bouche fermée, les mouches n'entrent pas). Discretion works well and, to quote Benjamin Franklin, Three can keep a secret if two of them are dead.

4.7 Being selective about who is in your network

What is this?

A young man is proud of having over 500 Facebook friends. Several professionals have over 500 connections in Linkedin, while others have thousands of followers in Twitter. None of them can confirm that they actually know these people, write down a credible list of their names or even remember how and where they had something in common to justify such associations.

Why is this an issue?

Amazingly, it is possible to buy "Friends" and "Followers" to apparently enhance one's image (any search engine will lead you to places that will sell you such services).

Unknown people wishing to link up with you may therefore not even be real but, by linking, they will have access to all the information you choose to provide and may subsequently use it against you.

Download free eBooks at bookboon.com

What you should do about it

The answer is simple and difficult to apply, particularly those who like social media and spend considerable time immersed in it. Don't link to anyone you do not know, however good the reasons others may advance for accepting them.

Review your links regularly – you can in fact remove people from your network (a search engine will give you step by step instructions). Some social media sites make it more complicated that it should be.

4.8 Social media and Internet Memory

What is this?

Social networks (and/or social media) are popular and have large numbers of subscribers. Their main purposes include linking up people with shared interests, those who lost contact with old friends, etc., and allow them to express and discuss views, opinions, reviews and feelings.

Why is this an issue?

From and information security perspective, the main issues are:

- Social networks operate on the assumption that everyone can be trusted.
- There are no guarantees that any Third Party Applications or links posted in these networks are free of malware or are genuine websites
- A hacker could take control of your account and use it to spread disinformation, malware and scams – and you will be blamed
- As stated before, everything posted becomes the property of the Operator and it is hard or impossible to remove such postings – The Internet Memory seems to last forever.

What you should do about it

Virtually all of the things discussed in this book should be considered and, ideally, applied. In particular:

- Ensure you have the latest updates for your security software, web browser, and operating system
- If there are any privacy and security settings on your social network websites use them to define your comfort level for sharing information. Less is always better than more
- Use strong passwords and have a different one for each social network you use
- Don't hesitate to delete, un-friend or whatever action is required to keep your network free of people you don't actually know or wish to network with
- Don't follow links in email, tweets, posts, and online advertising

Download free eBooks at bookboon.com

5 Hygiene and the cyber-minefield

The symbolic map of cyberspace in Figure 1 shows areas inhabited by criminals and terrorists as well as a military area and unexplored areas (*Terra Incognita*). Many parts of cyberspace also contain the electronic equivalent of landmines, intended to cause you emotional, rather than physical, injuries and, at the very least, considerable inconvenience.

It is regrettable that, so far, the little legislation there is for cyberspace does not properly address the issues listed in this part of the book and therefore you are largely on your own when visiting the many cyber-minefields which, unlike the one photographed here, are not marked.



Figure 14: Demining operations
CC BY ANZ Cluster Munition Coalition, ND

5.1 Spam and scams

What is this?

"Spam": the name given to unsolicited bulk electronic mail sent indiscriminately to millions of people, mostly for advertising purposes but many are also "scams", confidence tricks that aim to abuse weaknesses in human nature.

Download free eBooks at bookboon.com

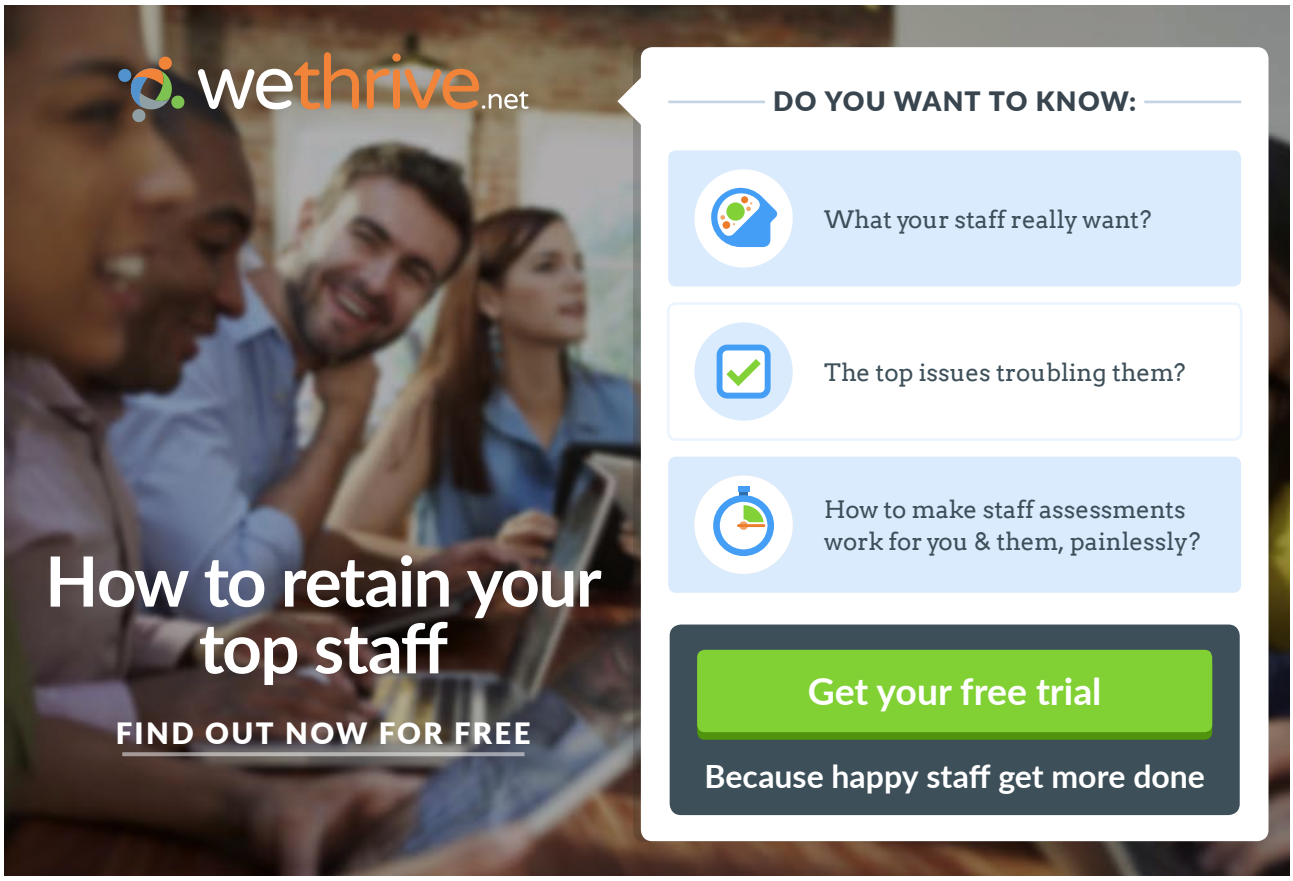
Typical **spam** messages are easily recognized – do you really want to buy medication without a prescription from an unknown supplier who may be located somewhere far away and certainly in a remote jurisdiction who, having taken your money will send you nothing or a fake product. Of course there also many who are legitimate and will fulfil your order but how do you know in advance?

Scams are numerous and some are well thought out – they may tell you that the nephew of a minister in a distant country needs to transfer millions of dollars to another country and that if you help them there will be a large fee… except that they need you to give them some money in advance to facilitate the process. Incredible as this may sound, hundreds of people continue to fall for such scams.

A more sophisticated one uses the compromised e-mail address (and contacts list) of someone you know to send you a message that they were mugged during their travels, lost their passports, money and telephones. Therefore they urgently need you to send them money to help them return home.

Why is this an issue?

Two reasons – spam fills your electronic mail inbox with trivia or worse. Scams can cost you financially and, if have fallen victim to one, make you feel truly stupid.



Click on the ad to read more

Download free eBooks at bookboon.com

What you should do about it

Get a spam filter. Many e-mail service providers include one in their offering but some spam will get through.

If it sound too good to be true, it almost certainly isn't. Never reply to spam, not even to take up their offer to "remove yourself from the mailing list". Doing this confirms that your e-mail address is active and that you have read the message. This is an invitation to receive much more of it.

Don't give money to anyone before you have confirmed his or her situation. The person supposed to be travelling may well be at home, and if not, should be in a position to give you a way to reach them.

Many e-mail service providers offer an anti-spam service that lets you verify what they detected as spam in case there are false-positives, i.e. messages you wish to see.

5.2 Phishing and spear-phishing

What is this?

The generally accepted definition is "an attempt to obtain confidential information by pretending to be a trusted entity in cyberspace". Well designed phishing attacks may use electronic mail details that appear genuine (the address of the sender looks like a genuine organization, for example a bank, and may include a link to a fake website designed to look like the real thing, where the victim is asked to enter confidential information (login, password, credit card details, etc.) and/or infect the victim's computer with malware planted on the fake web page.

Spear Phishing is a more sophisticated form of this attack that targets specific individuals (often corporate managers) using messages that indicate knowledge of the person (title, nickname, other) with the same intent. The plausibility of the message makes it easier for the message to be accepted as genuine.

Why it this an issue?

Because this has become a widespread practice done well enough to take advantage of the unaware. The most likely targets are those who have visibility due to their professional roles.

What you should do about it

First and foremost, remember that a government department, business or any other entity, will often accept and even encourage you to transact online – at **your** initiative and will have taken adequate precautions to protect your data. This applies to doing your tax returns online, electronic commerce, online learning and much more.

Download free eBooks at bookboon.com

On the other hand, these entities would NEVER send you a request asking you to provide sensitive or confidential information by e-mail, particularly one including a link to follow.

If in doubt, question the entity that sent you the (potentially phishing) message as to its authenticity by phone, not by e-mail as the e-mail address may be a fake.

Spear phishing practices include faking the e-mail address of somebody you may know to send you an attachment with a plausible name that contains a purpose-designed item of malware. You should not download or open such an unexpected attachment as it may include software that can run infect your machine and those of others in the same network.

Deleting such e-mails may be an unexciting chore that adds to the pressure of your daily activities. It's good to remember the title of a book by Andy Grove (Intel's CEO in its early days). It was "Only the paranoid survive".

5.3 Attachments

What is this?

One of the useful features of electronic mail is that of being able to add files to a document. Such files can be documents, photographs, video clips, music, etc.

Unfortunately, it is also possible to add files that can run a program, usually referred to as "executable" and these can infect your computer with malicious software or perform functions that prejudice your security – by, for example, capturing your logins and passwords.

Every file (a single document in digital form) has an extension that describes what it is. Extensions are of the format "dot followed by three or more letters", for example **.mp3** describes an audio or music file, **.pdf** describes an item as being in Portable Document Format**, .jpeg** sometimes .jpg describes a graphical item in Joint Photographic Experts Group format, etc.

Why is this an issue?

Opening an attachment that is a form of executable file (software that can run on your device) can infect your computer. Once infected, your device could infect other devices, those of people you share data with. Hackers wanting to penetrate a corporate network often use the faked e-mail identities of someone you know to send attachments including professional quality malicious software that collects logins and passwords and gradually allows them to acquire confidential information and penetrate networks.

Download free eBooks at bookboon.com

What to do about it

Gain an understanding of what the many types of file do and learn to distinguish "safe to open" files from executable files.

A search engine query for "dangerous file extensions" or "malicious file extensions" will return a long list of file extensions including: **.exe, .com, .bat, .cmd, .lnk, .vbe, .vbs, .jar** and dozens of others. Beware of files that have been compressed to the **.zip** format as you cannot tell what they contain until they have been decompressed (unzipped). If in doubt about it's origin check with the sender. If unexpected, delete without opening.

It is good practice to download only files that have a safe-to-open extension and this requires you to ensure the file extension is visible – some operating systems hide file extensions by default and it is up to you, the user, to modify the settings so that they are visible (search engine to the rescue!).

Hackers can change file extension so that they appear to be a safe-to-open one. Ensuring that the true and complete file extension is seen will show files that should NOT be opened. Your antivirus software should be set to scan files as they are downloaded and, in any case, before they are opened.

Attachments to e-mail from people you do not know (and unexpected attachments from people you know) should be treated with care – better safe than sorry… In any case, if you did not expect it, you will not miss it.



Click on the ad to read more

Download free eBooks at bookboon.com

5.4 Click here to follow the link

What is this?

The World Wide Web functions through links. By clicking on a link (usually in blue and underlined) your browser will open a new page from the website to which the link took you. This is great stuff and one of the many factors that has made the Web so popular as this is easy to use.

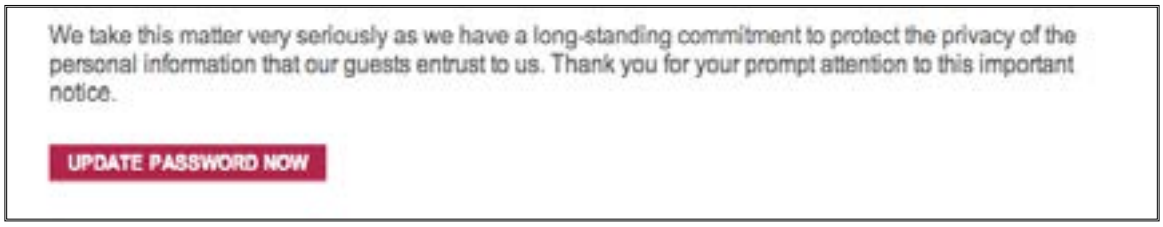


Figure 15: Screen capture of a phishing email sent to the author. He reported this to the company from which this was supposed to originate.
© Eduardo Gelbstein, All Rights Reserved

Why is this an issue?

Because some links are not there to help you but to take advantage of you in many different ways, ranging from taking you to fake web pages that resemble the real thing, to take you to genuine web pages where the content may be doubtful (quality, intent, potential infection).

What you should do about it

When you are dealing with a legitimate and reputable organization (a government department, electronic commerce, academia, etc.), there should be reasonable confidence that there is little risk and using the links in their pages should be safe enough.

When the link has been sent to you in an e-mail, the decision whether or not to follow it by clicking on it, should reflect your knowledge of the sender and the confidence you place on their communications. For example, several electronic commerce sites regularly send the author mails with links announcing new releases or new products. These links can be assumed to be right and proper.

Check and think before clicking and rely on your intuition, experience and antivirus software to confirm you are doing the right thing.

5.5 Unencrypted "free" WiFi (or WLAN)

What is this?

A widely practiced commercial incentive to attract customers that exploits the perceived need of many people who feel the need to be permanently connected. The Internet has also created an illusion that information and access to it should be "free" – why pay if you don't have to, right?

Download free eBooks at bookboon.com

Why is this an issue?

WiFi (also known as a Wireless Local Area Network or WLAN) is great and convenient. When it is free, it is also unencrypted which means that others connected to the same network could (with a little bit of skill and the right tools) capture all your data traffic, including your e-mail address, login and password and whatever else you may be doing online. The same is true for having Bluetooth enabled in your devices.

What to do about it

If you are simply surfing the World Wide Web for non-sensitive and non-critical tasks, for example reading newspapers online, looking at the weather forecast, etc., it's basically OK.

For anything more sensitive – checking your bank balance, your credit card activity, buying something online or even using your e-mail, think twice before using an unencrypted network. The charges for using a secured network are mostly reasonable. From the several encryption protocols available for such wireless networks, WPA2 is regarded as the strongest The basic WEP encryption can be broken in minutes.

5.6 Encrypting your domestic WiFi

What is this?

Many of us have at least one home network and this network is, increasingly, wireless. These networks connect multiple devices, including other computers, tablets, smartphones, external storage, printers, etc. Such wireless networks have a fair range – in the order of 20 meters inside a building, more outside. The range of Bluetooth networks is smaller and these support wireless devices (keyboards and mouse) as well as smartphones.

Why is this an issue?

A third party could make parasitic use of an unencrypted network if it can find such a hotspot. These hotspots are easily found. If no password is required your data can become theirs

What you should do about it

- When installing a wireless network at home using a router, the supplier provides installation and configuration instructions which include an encryption algorithm such as WPA2 (Wi-Fi Protected Access also called RSN Robust Secure Network) and a long and impossible to memorise a long password that can be between 24 and 63 characters long. Keep a copy of this password in a secure place so that it can be re-keyed if necessary, although this is unlikely to be a frequent need
- Activate the Media Access Control (MAC) to ensure only your devices are paired with the WiFi router (detailed instructions can be found in the documentation and/or online).

Download free eBooks at bookboon.com

- Change the default Service Set Identifier (SSID) so that a scanner looking for WiFi hotspots cannot know to whom the router belongs.
- Ensure the router software, firmware and related device drivers are up to date.
- Use your firewall to prevent incoming data traffic through the router.

5.7 Bluetooth

What is this?

Bluetooth has become a de-facto standard for low power, short-range wireless communications and it is extensively found in electronic devices. Early applications of Bluetooth were found in wireless keyboards and pointing devices such as a mouse. This has expanded to include other devices (such as printers and scanners – many of which also support WiFi such as headphones, loudspeakers, etc.

The most frequent use of Bluetooth is in mobile devices such as smartphones and tablets and the environments where these are used – for example enabling hand free phone calls while driving a car.

Why is this an issue?

While considerable attention has been given to security features in Bluetooth, the emergence of Internet enabled appliances and the Internet Of Things make Bluetooth an essential protocol over which you – as an individual – may wish to exercise control.



Click on the ad to read more

Download free eBooks at bookboon.com

A key feature of Bluetooth is that while appliances may exchange data and recognize each other, in theory at least, they require an individual user to intervene to pair the appliances. However like with most security vulnerabilities it is also important that the end users be aware of what they are allowing to run in their devices. Hackers create tools to compromise vulnerable devices. Bluetooth has been hacked and known attacks included processes called bluejacking, bluesnarfing, bluebagging and bluetoothing. Several hacking tools are readily available if you know where to look.

The potential for interfering with appliances – cars that drive themselves, heart pacemakers, insulin pumps and other medical implantable devices, surgery robots, electronic locks for home use and so-called "smart" appliances are all potential targets.

What you should do about it

Use a search engine to learn more about the various ways in which Bluetooth can be compromised.

- Keep Bluetooth **off** when you are not using it and make sure you are pairing with known devices whenever you need too.
- Monitor devices and links for unauthorized Bluetooth activity.
- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- Use device firewalls, regularly patch Bluetooth devices, and keep device anti-virus software up to date.
- Comply with all applicable corporate directives, policies, regulations, and guidance.

5.8 Log out of everything you do online

What is this?

Many websites, particularly social media ones would like you to be permanently connected to make it easy to interact with your friends/followers/contacts, etc. all the time. Many of them do not make it entirely obvious that you remain connected and that logging out requires finding how to do it and then remembering to do it.

Download free eBooks at bookboon.com

Why is this an issue?

Using small files (cookies) that get installed in your device by most webpages allows them to collect data about you, even after you have logged out, allegedly for "security purposes and aggregate statistics". In fact this may allow a website or social network to track and map you usage of the World Wide Web. They can also track your physical location and keep records of it.

What you should do about it

In the first place ensure that you actually log out from all websites that require a login. This may not be enough if the website has installed tracking cookies in your device, therefore:

- Find out how to delete individual cookies from your computer. The way to do this varies from one browser to another, and essentially the process requires you to identify which cookies have been planted and delete them – every time you visit the relevant sites.
- Alternatively, you may install a separate browser (there are many to choose from – Firefox, Chrome, Opera, etc.) and use it exclusively for your social media activities. Some of them accept third party software plug-ins that are designed to block cookies and tracking cookies.



Deloitte.
Discover the truth at www.deloitte.ca/careers
© Deloitte & Touche LLP and affiliated entities.

Click on the ad to read more
Download free eBooks at bookboon.com

6 Beyond the essentials

How far are you prepared to go to protect your devices, your family and yourself in cyberspace? The list of good practices can get very long and it forces all of us to make choices. Every one of the measures in this section will require you to consider its pros and cons, the amount of time effort that they'll require and the value they will return to you.



Figure 16: The proverbial tip of the iceberg
© E. Gelbstein, All Rights Reserved

Download free eBooks at bookboon.com

6.1 Inventory of your devices

What is this?

A typical inventory in 2013 would include one or more of the following (and a few more items)

- Home computer (desktop or laptop), including operating system and pre-installed software
- Other home computers, laptops or notebooks, including operating system and pre-installed software
- Tablet computers, including operating system and pre-installed software
- Smartphones (corporate and personal), including operating system and pre-installed software
- Other software, licensed as well as shareware and freeware
- Backup and other storage devices (disks, USB memory, DVD and data CDs, other)
- Connection and account(s) with an Internet Service Provider
- Wireless and other connectivity devices (home network, routers or switches, etc.)
- Warranties, maintenance contracts, support telephone numbers, etc
- Passwords and password-related devices (e.g. tokens, cards or password generators)

Why is this an issue?

Simply because it is the only way to have records to report details such as serial numbers, date of purchase, software license numbers and other information you may need to report loss or damage to the police, insurance company, internet service providers and other parties with which you may need to communicate.

What you should do about it

Many items of the equipment and software you own have basic information about them in electronic form, such as serial numbers, product ID and software version. The software packaging or the order confirmation if bought online often includes a Product Key necessary to activate it. You may have many items that do not have such data, for example USB memory devices – it would be however prudent to keep track of them to, at least, be conscious if one or more is lost.

While it may laborious, either a word processing, spreadsheet or database package can be used to build a comprehensive list that is easy to keep updated. The following parameters should be recorded:

- Hardware: Make, model, serial number, date of purchase, length of warranty
- Software: Name and purpose, version, product ID or serial number, date of purchase
- Services: Name and purpose, access codes and passwords (these should not be in clear text!)
- Networking: Provider, terms of contract, access codes and passwords (these should also not be in clear text!)

Download free eBooks at bookboon.com

There are several programs, many included with your devices software or available as downloads that simplify this task. Given the wider range of devices, operating systems and utilities each owner has to look for the most appropriate tools for each environment. A search engine can help…

6.2 Crapware, craplets and Scareware

What is this?

Pre-installed software (in a computer, tablet or smartphone) is referred to by the device vendors as "bundled". Buyers tend to think of such software as "crapware" because some of it reduces customer choice – for example pre-installed anti-virus software which may be difficult and time-consuming to remove, or "craplets," software that the device manufacturer was paid by a software company to include. Craplets are of dubious value to the buyer, such as evaluation copies of products or outdated games.

Scareware is the name given by security writers to software sold on questionable ethics by causing anxiety or fear to insufficiently informed owners of devices. They do so by displaying warnings of malicious software infections that must be immediately removed by downloading (and paying for) their software. Alternatively, the message suggests that a particular product could greatly enhance performance – such as registry optimisers or cleaners.

Why is this an issue?

- It may be bad for you
- It limits the buyer's choice
- It makes it difficult to install an alternative product (e.g. anti-virus products)
- It consumes computing resources
- It may contain malicious software to capture and report sensitive data
- It is limited to the computer on which is was installed
- It has a limited period of validity, after which it must be purchased
- It does not come with the media necessary to re-install it should this become necessary
- It is difficult (sometimes impossible) to remove

What you should do about it

Crapware and Craplets:

- Identify the inventory of software pre-installed in the device
- Look for any Uninstall options that any software you don't wish to keep may have
- If not found, use a search engine for guidelines on "how to uninstall XXXX" from a "CCC", where XXXX is the software in question and CCC is the make and model of your device
- Remove anything that you don't wish to keep.

Download free eBooks at bookboon.com

Scareware:

Advertisements for scareware will appear on your screen when you are online. Some will tell you that you have a major and urgent problem sometimes giving you a "free" diagnostic. Buying their product is always the answer. Many of these products will do nothing and may introduce malicious software to your device. Others, such as Registry management software may cause your computer to malfunction. Should you feel that your computer needs attention and you have no access to expert advice, start by using your search engine to look for product reviews (see also the section on "downloads").

6.3 Inventory of all your accounts

What is this?

If your device(s) may be shared at some time or another, you should take steps to control what others can access and do with them. Creating individual accounts does this. These specify what others may do without compromising your personal data.

Even if you do not share your devices it is good practice to keep your login identities and passwords to online services secret to avoid others – unknown and unknowable – from impersonating you and conducting financial transactions, abusing your social networks, writing blogs, etc.



Click on the ad to read more

Download free eBooks at bookboon.com

Why is this an issue?

It is likely that, like the majority of people these days, your devices are used for accessing subscription material, bank accounts, assorted bookings and reservations, electronic mail, blogs, social networks and more.

If you are a regular use of Web-based services it is likely that you will be required to have a login identity and, typically, a password. As these may be numerous, it creates a dilemma: make it easy for yourself by using the same login identity and password for all of these accounts or, like physical keys to open locks, have a different one for every account.

The latter is a more secure option but it requires you to have an excellent memory or write them down. If you write them down, this inventory must be kept away from anyone who may misuse it or abuse it.

What you should do about it

The first step consists of identifying and listing all the login identities and passwords you have and what they are used for. While the number of login identities need not be large – many online services use your electronic mail address as your login identity. Your choice is whether to use your "real" name or a made-up identity (e.g. Retired.Auditor@….). However, passwords should be different for each service.

Having established the list, it should be protected by, for example, storing it in encrypted form, password protected and/or in a data vault.

Ensure you have also left your log-on credentials with a trusted/loved person. You never know what uncertainties life will confront you with and they may need to access your system in the event of an emergency.

6.4 Lost your smartphone or your computer?

What is this?

The popularity, affordability and usefulness of electronic devices in the hands of a large population implies that either due to oversight, distraction or any other human weakness, devices get lost, misplaced or forgotten. Many of these devices, particularly the very recent and/or fashionable become objects of desire and therefore, get stolen. They also get left behind in airport security checkpoints, restaurant tables and almost any other place. You may be lucky. More often than not, this is not the case.

Why is this an issue?

If the device cannot be recovered, obviously there is the cost of replacing the device. However, and more importantly, the device may contain personal and/or corporate information, including stored passwords to network connections, electronic mail, bank accounts, etc. that could be abused or misused by a third party.

Download free eBooks at bookboon.com

What you should do about it

There is no shortage of options for each type of device (i.e. computer, tablet, smartphone). If the lost device has been provided by the business in which you work, they should be the first to be informed.

If you have lost a computer or tablet, the second step below may help you. If it doesn't, don't hope for much. If the device is your telephone or smartphone you should try the following steps first:

- Call your phone and listen for it to ring or vibrate. If someone else has it, they may answer it
- Do a thorough visual search (if you did not hear it maybe because the battery is flat) and retrace your steps
- Send a test message offering a reward for its return
- Contact your service provider and report the loss
- Report it to your insurance company (if you have such insurance)

You can help yourself by installing software that helps you trace the location of your lost device and, just as importantly, protect the data in your device. Other sections in this book give some more details.

> Expect the worst and you will never be disappointed.

6.5 Tracking software for electronic devices

What is this?

Given that electronic devices, particularly new models, are small and lightweight, they are easy to misplace and steal. Trustworthy sources report that in the U.S. alone, there are up to 2 million laptops stolen every year and as many as 600,000 are left behind at airport security points and lounges. Similar numbers are reported for stolen and lost mobile phones.

Why is this an issue?

Numerous studies conducted by serious researchers indicate that at least half of the lost or stolen devices contain confidential company information and the majority of the devices do not have measures to protect such information.

Besides, if the devices are yours, it does not feel good to misplace them, have them stolen and not being able to do much about it.

Download free eBooks at bookboon.com

What you should do about it

Mobile phones and tablets

First thing to do is to note your phone's IMEI, MEID or ESN number (it's on a sticker under the battery), Which one of these numbers applies to your device depends on its manufacturer and model. The police and your network provider will ask for it when the phone is lost.

The mobile phone GPS tracking facility can be used to locate it and most network providers offer a tracking service (for a fee). There are several tracking applications (Apps) to choose from. You may consider using them if you have given cellphones to your children.

A search engine query on "cellphone tracking software" or "cellphone tracking services" will give you several options to explore.

Laptops

There is an adequate selection of laptop tracking software (fee-based) that you need to install and subsequently activate when the device goes missing. If and when the laptop is turned on and connected to the Internet, it can be located and you can provide this information to a law enforcement agency.

A search engine query on "laptop tracking software" will give you several options to explore.



Click on the ad to read more

Download free eBooks at bookboon.com

6.6 Remotely wipe the contents of your lost device

What is this?

If someone else has you device and it is not protected by a good password or PIN, whoever now has it will have access your contacts, text messages, stored documents and everything else that you may have in it. If password protected, this may not be too difficult to break.

The best way to ensure the confidentiality of all the data in a mobile device is to remotely wipe it.

Why is this an issue?

Simply because your data is yours and nobody else's business – the belief that "I have nothing to hide" is no excuse to allow others access to your data, particularly if it includes details of your bank accounts, friends' telephone numbers and personal messages, as you lose control of how they may be misused or abused.

What you should do about it

Many devices, particularly smartphones may include the facility for remote wiping and there are many software products and Apps that perform this function. Several of them are included in the software that allows a missing device to be tracked.

A word of caution: if the data in the missing device has not been backed up, remote wiping will leave you without any trace of this data – would you like to lose the only copy of your baby's first words or steps?

Search engine query "remote wiping of (product name and model)".

6.7 Encryption and digital signatures

What is this?

Encryption and digital signatures use mathematical processes for somewhat different purposes. Both have been in use for many years.

Encryption (also called cryptography) is intended to transform a document (usually text) into a format that cannot be read without having the right tool (a "key").

Digital signatures use similar tools to ensure either (or both) that the originator of the document is the person who "signed" it and that the document has not been modified after it has been signed.

Download free eBooks at bookboon.com

Why is this an issue?

As activities migrate to cyberspace, it has become essential to protect the confidentiality of valuable and sensitive data, i.e. the ability to read such data is restricted to a limited number of authorized individuals.

Similarly, it has become important to be able to demonstrate that the data's integrity, i.e. that the data has not been modified by an unauthorized third party.

What you should do about it

A private individual (as against a corporate entity) should consider several different situations:

a) The encryption of some or all the documents in a computer or smartphone so that, should the device be stolen or lost, the personal information in the device is not readable by the new "owner". While an expert having the knowledge, tools and time can break such encryption a casual thief or finder will most likely give up
b) The use of encryption in everyday activities, such as electronic mail is good to ensure the privacy of such communications. However, given that it has been reported that there are surveillance mechanisms that track electronic communications, the use of encryption – totally legal – draws attention to the parties to such exchanges. As a result, it is prudent to remember that electronic mail is essentially the same as sending a machine-readable postcard and you would not put the details of your credit card on a postcard, would you?
c) The use of digital signatures is advisable when there is a risk of dispute about the authenticity and/or accuracy of a document or transaction

If you need to provide sensitive information such as a credit card number to someone you really trust, instead of encryption you could apply the technique described in 4.8 on condition you use words other than the ones you use to encode your PINs.

Finding encryption and digital signature tools is relatively easy. Your favourite search engine should be your best friend

6.8 Geo-tagging

What is this?

Geolocation is the ability to identify the position in the world of a specific item or device using a variety of techniques including Global Positioning by Satellite (GPS) and Internet Protocol (IP) address location.

Geotagging is a feature increasingly available in electronic devices such as photographic cameras, notably those in a smart phone that records the location where the photograph was taken.

Download free eBooks at bookboon.com

Why is this an issue?

It may or may not be an issues, depending on your cultural attitude about being tracked.

On the positive side, being able to track a person by locating a geolocation-enabled device is a valuable feature in situations such as finding a misplaced or stolen device, or in a Search and Rescue operation. If you are a parent and you give such a device to your children, you'll have the ability to find out where they are should they not answer their phone. Geolocation and geotagging can also be valuable in forensic investigations.

On the negative side, to what extent do you want your physical location to be known by others – not just friends but also potential stalkers and others with malicious intent?

What you should do about it

Make a choice that is appropriate to your circumstances, recognizing that being "invisible" and "anonymous" is gradually becoming harder.



Click on the ad to read more

Download free eBooks at bookboon.com

6.9 Legislation you should know about

What is this?

A big enough topic to justify a fat book. This is not the intention of this Section, which is to make you aware that there are many areas of activity that are covered by legislation and it is sensible to avoid breaking the law.

Among the many areas covered (in different ways in different jurisdictions) are:

- Intellectual property – copyright and copy protection for digital media
- Software licenses (did you read your End User License Agreements (EULA) and understand it?)
- Unauthorised access, data privacy, dissemination of spam and other "computer misuse"
- Data retention
- Use (and particularly export) of encryption
- Computer evidence and digital forensics
- National security (e.g. the USA Patriot Act of 2001)

Why is this an issue?

Because "ignorance of the law is no excuse".

What you should do about it

Be curious about this and using a search engine or online encyclopaedia to find out more about those areas of the law that are relevant to you.

6.10 Jailbreaking or rooting your devices

What is this?

Jailbreaking is a term associated with a specific series of products manufactured by Apple using the iOS operating system (iPhone and iPad amongst them). These devices come with several restrictions imposed by their design, notably that applications (apps) need to be downloaded (some are free) from Apple's App Store. The security design of these devices ensures such apps run in a confined and controlled environment (a sandbox). Other restrictions apply to the use of the device only with a contract carrier that the end user cannot change as well as the customisation of the device beyond the parameters set by the vendor.

Rooting applies to devices using the Android operating system and is about allowing the user of the device to have access to privileged functions such as modifying or deleting system files as well as removing apps pre-installed by the vendor or carrier.

Download free eBooks at bookboon.com

Why is this an issue?

Apart from invalidating the device's warranty both jailbreaking and rooting introduce new security vulnerabilities – by jailbreaking the device, you allow apps from sources other than Apple and that may not quality assurance and/or contain malware to run. As such applications would not run in the sandbox provided by iOS, they can corrupt the device and allow the malware to access personally identifiable information.

Jailbreaking is not supported by Apple and there are many articles about its risks and disadvantages.

Rooting, however, is permitted and reflects the open source software history of this software. The real issue is one of knowledge and responsibility. The statement that Genius has limits but Stupidity does not applies.

What you should about it

If you are a good hacker, you may have many reasons for exploring and exploiting both.

If you are a knowledgeable and experienced person with expertise in information technologies, you should already know that some things are best left alone and that any actions you take should have a genuine valid reason.

If you are not, and just read an article in an enthusiasts magazine – good luck to you because that's what you are going to need.

Download free eBooks at bookboon.com

7 Good hygiene in the future

This book started looking into the history of disease and the role hygiene had in driving progress.

IF the assumption "the digital hygiene as practiced today is poor" is valid

THEN the opportunities for reducing the impact of some of the undesirable, antisocial and/or criminal activities are many.

Several things had to happen in the past before diseases and plagues could be managed:

- People had to discard the idea that personal hygiene was not an issue ("a millimetre of dirt is warmer than a centimetre of wood")
- Health practitioners had to learn more about how diseases propagate and identify environments propitious to bacteria, viruses and their carriers
- The owners of those environments had to take measures to make them safer for human use (e.g. water supplies)
- Researchers and manufacturers had to find substances that could target specific diseases, manufacture them and make them available to the public



Click on the ad to read more

Download free eBooks at bookboon.com

All the above steps continue to be required. If you want to keep your teeth, you better brush them regularly and properly and see your dentist frequently enough.

In terms of cybersecurity, these steps can be reworded as follows:

- People have to accept that digital hygiene is important and, really, not an option.
- Academia and practitioners will continue to learn about developments in malware and transmission vectors
- Product designers will focus on Security By Design
- Researchers and vendors will develop and provide features (hardware and software) that improve security

If you want to keep control of your data, your privacy – I hope this book will point you in the right direction as everything continues to evolve.

Today there is a big difference between the medical environment and that of cyberspace:

Medication is tested extensively before being used and every package includes a leaflet describing contra-indications and side effects. The profession is regulated and drugs must get formal approval.

In Cyberspace it is more like the Wild West of the 1800s – largely unregulated, anybody can design and sell a product (or give it away free) and a typical End User License Agreement (almost certainly written by lawyers that you must accept to install and use the product usually states that the vendor/designer has no liability for anything that may happen to your device and/or your data.

7.1 Coming your way: the Internet Of Things

What is this?

Essentially, an environment in which:

- Physical objects are integrated into an information network
- Objects have an Active Digital Identity and can exchange data
- They can be controlled by accessing them through Apps
- Objects can connect to Social Networks and vice versa

Download free eBooks at bookboon.com

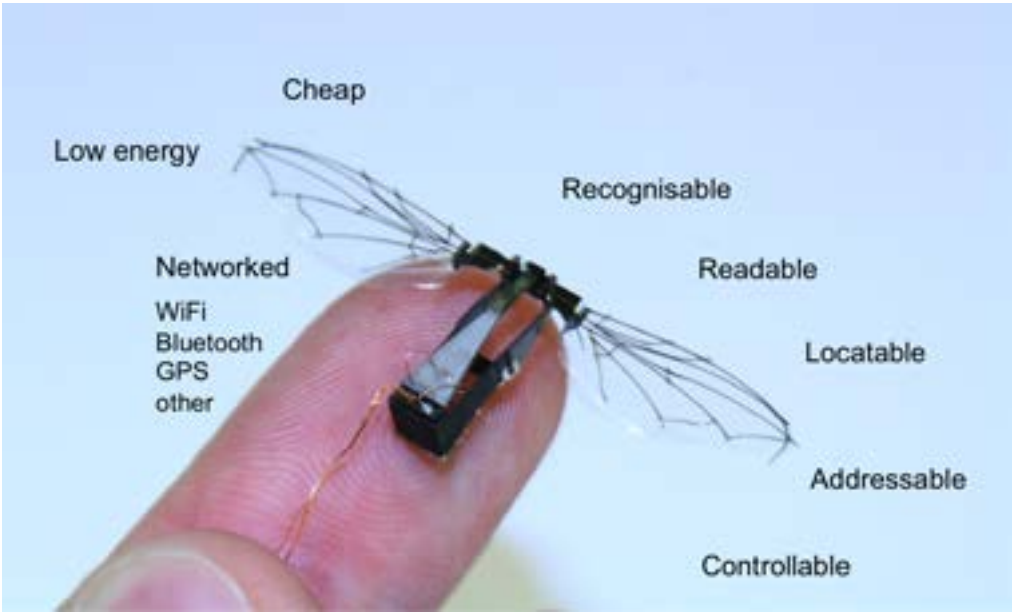


Figure 17: Robotic bee, Harvard University, 2011
© Ben Finio, Allr Rights Reserved

Most of the elements required to meet these two conditions are already available and in use. Many have proven popular, have been the subject of articles in magazines and newspapers and seem to appeal to the owners of smartphones and tablets.

bookboon.com
Corporate eLibrary
See our Business Solutions for employee learning
Click here
Management
Time Management
Problem solving
Self-Confidence
Effectiveness
Project Management
Goal setting
Motivation
Coaching
Click on the ad to read more

Download free eBooks at bookboon.com

Some of their uses are "fun" and expressions of human creativity and show how the boundaries of the possible get expanded – for example, a pair of shoes that contain an accelerometer, a gyroscope and a pressure sensor. These link with Bluetooth to a smartphone app. The latter processes the data collected and translates it into motivating comments to the wearer.

The serious includes implantable medical devices such as insulin pumps and heart pacemakers, robots that perform surgery. Medical electronics is seen as an area of great potential. The serious is likely to change the way we live and coexist with technology, being permanently connected gradually building a symbiotic relationship.

The Internet Of Things (IOT) will take this much further by giving objects an identity that can be accessed and verified electronically. The figure below gives a summary of the current status of the IOT and how it may develop.

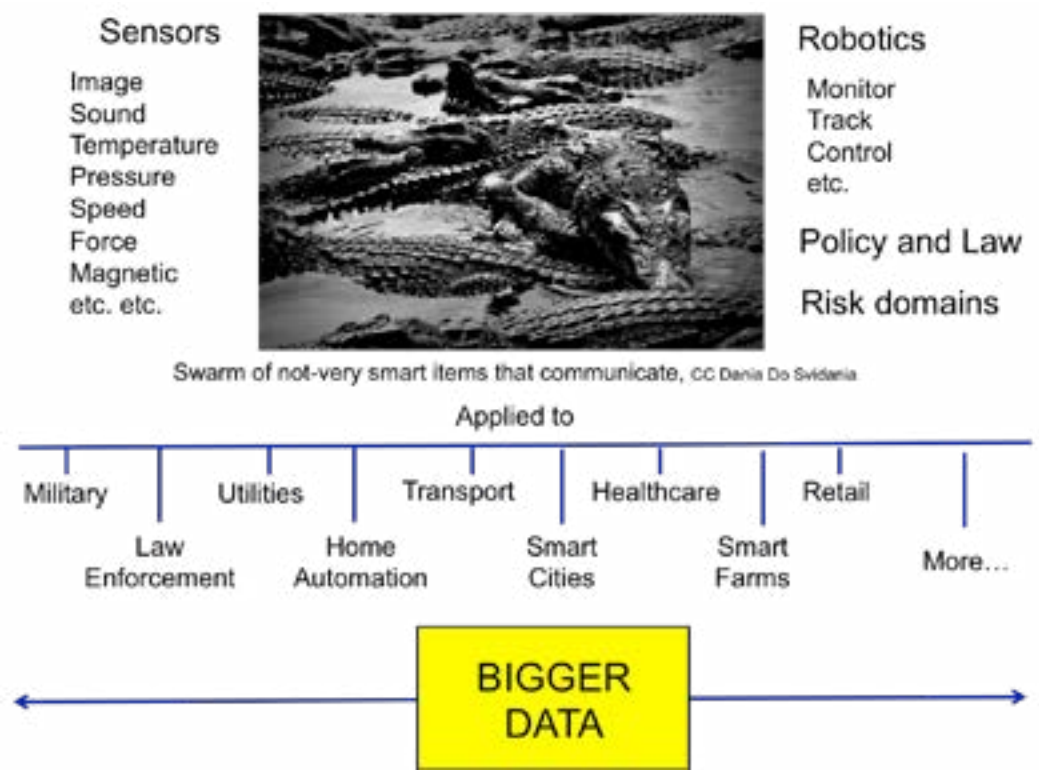


Figure 18: Summary of how an Internet Of Things might develop.
© E. Gelbstein, All Rights Reserved

There is much optimism about the many benefits that an IOT will bring and enthusiasts talk of up to 50 billion devices being connected to it. Driven by Venture capital, commercially motivated vendors, designed by geeks and rushed to the market, we can expect many unintended consequences.

Download free eBooks at bookboon.com

One of them is a change in behaviour – a single device as the robotic bee above is reasonable predictable and controllable. This is not the case when such devices use their connectivity to become a swarm (wasps, locusts, blackbirds, crocodiles, schools of fish and others exhibit such behaviour), something scientists admit they don't fully understand.

We should also know from history that such innovations can be used for good as well as for evil and that for as long as legislation is well behind technology as is always the case, the evil applications will be creative, smart and successful.

Why is this an issue?

Devices exchanging data with each other are definitely progress and should be welcomed. We know that the mobile devices with which they will interact are not necessarily secure – someone else may be able to access, remove or modify the data either on the device or hijack it and use it to control another device such as heart pacemaker: in such a situation a smartphone becomes a deadly weapon that does not need licensing or regulation.

Privacy, Security, Transparency, Cross-border data flows, liabilities and, finally Standards will have to be good enough for the IOT to fulfil its promise.

The risk domains of unintended consequences and malicious use, autonomous swarm behaviour, irreversible dependency and how these will impact the future of work and our relationship with technology are all fascinating topics for research. As it happens, Alvin Toffler defined "Future Shock" as the situation when the future arrives before you are ready for it.

What you should do about it

Becoming an informed observer may be a good idea. Follow the media and discover for yourself whether your character makes you:

- An Early Adopter: those who must have the new "item" as soon as possible. There are many pictures of hundreds of people queuing overnight outside a major brand shop to achieve this.
- A Watcher: those who wait until the "item" has been used for a while, how successfully or otherwise, what issues emerged, what alternatives may be available, etc., before deciding.
- A Laggard: those who are not inclined to adopt new things. They can however become addicts if they receive such an item as a birthday gift but have no concept of cyberspace and are therefore at risk.

Whatever you decide is right for you, please remember you are doing it at your own risk.

Download free eBooks at bookboon.com

7.2 Digital hygiene in 2003

What is this?

The 2003 World Summit on the Information Society took place in 2003. The Diplo Foundation (www.diplomacy.edu) produced and published a series of booklets under the umbrella title of "Information Society Library" – several of these booklets focused on information security and one of them addressed Good Hygiene. The mindmap below summarises the topics covered.

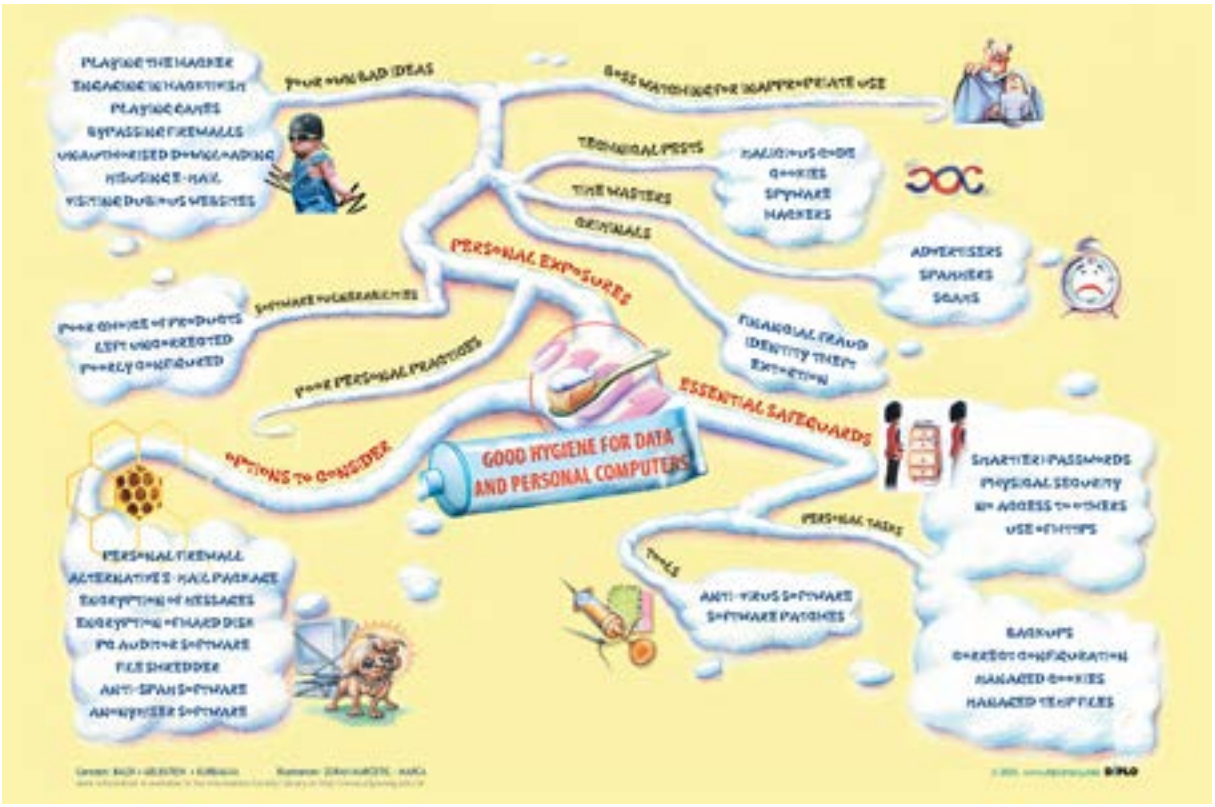


Figure 19: Mindmap from the 2003 Good Hygiene booklet,
© Diplo Foundation, All Rights Reserved

Looking back ten years is instructive as it highlights the explosive rate of growth of the interactive electronic world and how much the need for good hygiene has changed.

The term "Web 2.0" was first used in 1999 and marked a departure from the static catalog style of web pages and the emergence of "anyone can be a content creator" that characterizes the web in 2013.

The "smartphone" – a device that combines telephony with computing capabilities was first commercialised in the mid 1990s and these found a measure of adoption in the corporate world. The introduction of the iPhone in 2007 created a popular market for these devices and its thousands of applications (apps). The emergence of tablets and other models of smartphones just increased the need for end users to protect themselves from the dark forces that inhabit cyberspace and the need to practice good hygiene will grow and continue to evolve.

Download free eBooks at bookboon.com

8 In conclusion…

The wave of rapid innovation of the last 10 years shows no signs of slowing down and attempting to predict which developments will be successful is a matter for gamblers willing to invest in promising consumer oriented initiatives and see what happens.

Where such innovations will take society is another unpredictable topic. What we should have learned by now is that the ease of use of such products hides a great deal of complexity, and this, in turn, the reality that all such products contain imperfections – the author refers to them as "bugs" while some of the designers call them "features".

This is understandable when we consider the many parties involved in delivering innovative technologies. Looking at smartphones for example, they require the fusion of the work of:

- Hardware designers and manufacturers – processors, storage, screens and so on
- Operating system designers – the essential software that makes the device work
- Application designers – ranging from large software houses to single individuals
- Service providers – offering voice and data service contracts, sometimes adding apps to the devices they retail
- WiFi Hotspot providers – including shops, hotels and restaurants offering WiFi services, sometimes free of charge
- Device assemblers usually in low wage economies

All of the above work independently of each other and deal with devices of such complexity that no amount of testing prior to production can identify 100% of the possible vulnerabilities and bugs. This complexity is hidden from the end user. When this person is unaware of how to protect the device and the data it contains, disappointment, frustration and headaches are likely outcomes.

To this, we need to add the context in which some of the above activities are carried out:

- The role of venture capital and expectations of a rapid return on investment, which drives time to market
- The entrepreneurial ambition of becoming a millionaire by age 25 and a billionaire by age 40, often involving an Initial Public Offering (IPO)
- The technically highly skilled developers that sometimes lack empathy or concern for the end user
- The pressure to reduce costs

Download free eBooks at bookboon.com

And finally those for whom this book is intended: The individuals that have not thought about the many vulnerabilities associated with new devices and therefore are unaware of:

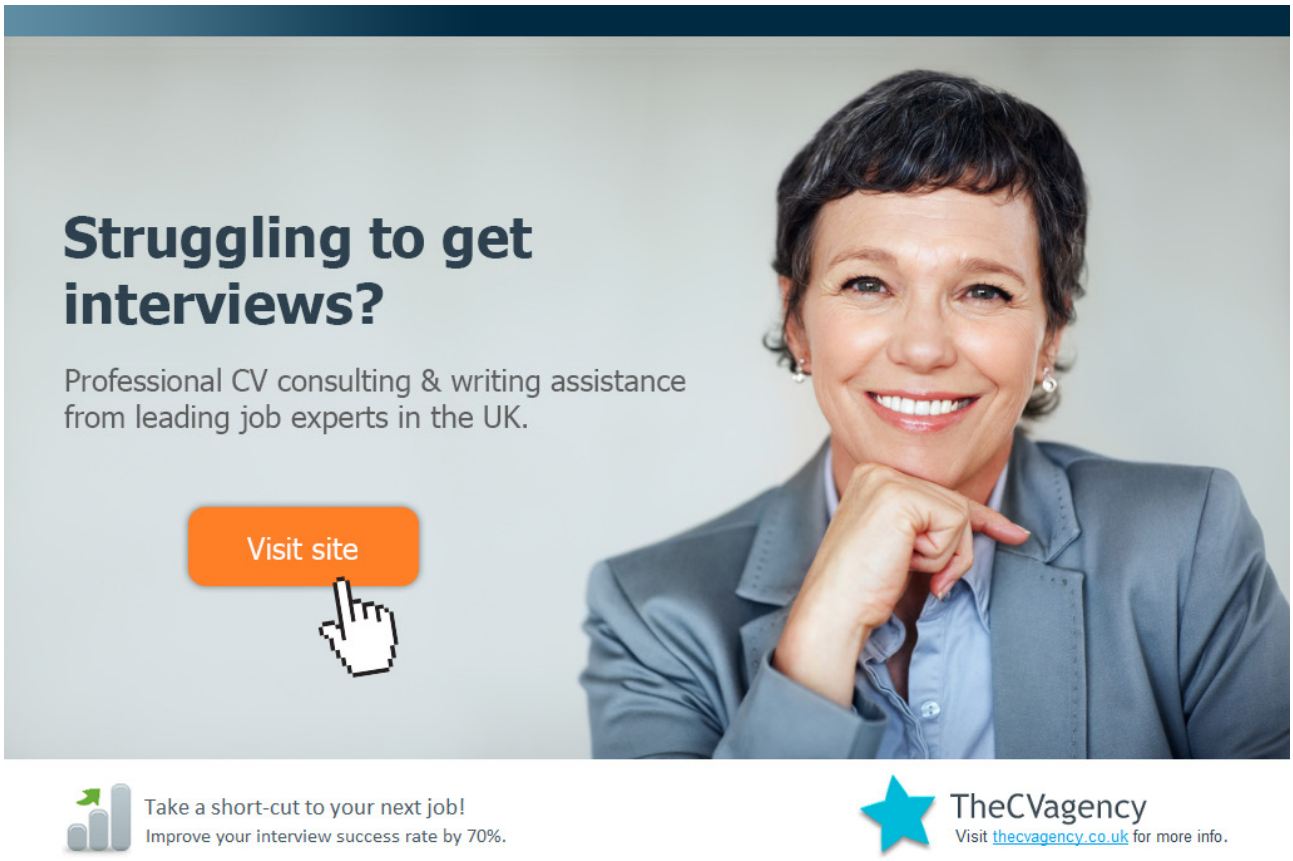
- Good digital hygiene practices and don't know what should be done
- Why it should be done
- How it should be done

Then there are those who don't want to know and don't really care (until things go wrong).

What you should do about it

To the readers that got this far, thank you for your patience. This book has 39 sections describing generally accepted good practices. Many of them are simple and quick to apply and Chapter 3 lists those considered to be the ones to start with.

Chapter 4 presents items to reflect on and implementing them may require the reader to change their approach to disclosures, assess how much privacy they wish to retain and become aware of the many parties interested in their personal data.



Download free eBooks at bookboon.com

Chapter 5 describes the main landmines you are likely to encounter in cyberspace and describes how to avoid them – if they appear as restrictions, it is because they are. The precautionary principle of "better safe than sorry" should be considered good advice.

Chapter 6 describes somewhat more advanced things to do. Not necessarily the highest priority but it's good to be aware that once implemented, you can feel more secure.

Chapter 7 is an attempt to predict how things under development now may impact on our social and personal life. As Nobel Prize Niels Bohr is alleged to have said "it is difficult to make predictions particularly about the future". There are so many developments towards what is generally known as The Internet Of Things that trying to predict which will become a successful product is no more than a gamble.

Chapter 9 presents a short list of other publications addressing the same issues and websites that provide good guidance. The list is nowhere complete but consists of trustworthy sources.

Is this book a complete guide to good digital hygiene?

Certainly not, and to a large extent deliberately so as publishing guidelines running to hundreds of pages would be a deterrent to getting started. Two domains beyond the author's knowledge and experience are:

Protecting children in cyberspace: this would include the effective use of parental controls, guidance on potential predators, online purchases, unsuitable sites, disclosures, addiction to video games and so much more. Such guidelines are available thorough the use of a search engine and government issued guidelines should be considered reliable.

Cybersecurity for Silver Surfers: in Europe there are constant reminders about the changing age profile of the population as life expectancy increases and these Silver Surfers have to accept that initiatives in e-government, facilities such as online video and audio telephony, e-commerce and so on have left them no option but to use the World Wide Web and mobile devices. From personal experience from older friends, it is clear that their level of awareness of cybercrime, malicious software and other risks is low. It is also difficult to try to explain these things in a way that makes sense to them.

Download free eBooks at bookboon.com

Can we learn anything from the past that points towards the future?

Those of us who enjoy the creative ideas of science fiction writers and film makers should recall that there are many books, magazine articles and movies on how future technologies will impact society. Many were written well before such technologies (perhaps their research was inspired by their ideas) became available. Here are a few examples:

- The concept of geostationary satellites, by Arthur C. Clarke in a communication to the editor of Wireless World (1945) – followed by many other ideas (see 2001 below)
- Nineteen Eighty Four, by George Orwell (1949) – on an intrusive state that monitors individuals and more
- I, Robot, a series of short articles by Isaac Asimov (1950)
- 2001 (movie) – released in 1966 – in which an artificial intelligence computer named HAL who communicates in natural language decides that completing its mission requires it to dispose of the astronauts
- Star Trek – the original TV series, 1966 to 1969 in which a "communicator" is used. Many cellular phones (shell phones or flip fold models) currently available look almost identical to it
- Cyborg, book by Martin Caidin, 1972. Provides the basis for the TV series The Six Million Dollar Man 1974 to 1978 where a former astronaut is "rebuilt" using bionic implants. This theme has been used in several other TV programs and movies since
- Star Trek – The New Generation TV series 1997 to 1984 where the computer communicates in natural language, touch screens and devices that look very much like tablets are in evidence. Advanced medical electronics, universal translators, etc. are also shown

This list could be extended considerably. The main lesson that can be drawn from it is that the creative ideas of the world of fiction can successfully migrate to the real world – it may take many years and many failures. The impact of successful initiatives on society and individuals can introduce significant change as well as undesirable and unpredictable side effects.

Download free eBooks at bookboon.com

9 Other publications and websites

The list in this chapter does not attempt to be comprehensive and is limited to the author's research for material issued by trusted sources in the last three years. The absence of other publications in this list is indicative of the author's ignorance…

Publications available on line and free of charge

Protecting Yourself Online – What Everyone Needs to Know, Australian Government
http://www.staysmartonline.gov.au/__data/assets/pdf_file/0005/19598/Protect_yourself_online.pdf

Cyber OPSEC USA Interagency Support Staff
http://www.dodea.edu/Offices/Safety/upload/15_Cyber_Protecting_Yourself_Online.pdf

Online Safety How to Protect Yourself and Your Family (Ministry of Education, Trinidad and Tobago) – advice about children online
http://www.moe.gov.tt/laptop_info/Online_Safety_Tips.pdf

Staying safe on the Internet (Interpol) – available in English, French and Spanish, possibly more
www.interpol.int/content/download/…/Education-SafeInternetEN.pdf

Mobile security survival guide for journalists
https://www.aswat.com/files/Mobile%20Journalist%20Survival%20Guide.pdf

Websites

http://www.fbi.gov/scams-safety/computer_protect (the FBI, USA)
http://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer (State of California, USA)
http://www.usa.gov/topics/family/privacy-protection/online.shtml (USA Government)
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/ (French Government)
http://www.ico.org.uk/for_organisations/data_protection/security_measures
(UK Government Information Commissioner)
http://www.nidirect.gov.uk/be-secure-online (UK Government services)
http://www.staysmartonline.gov.au/news/news_articles/regular/protect_yourself_online
(Australian Government)
http://www.saferinternet.org/web/guest/home (co-founded by the European Union)

It is reasonable to assume that there are many more such publications in many languages.

Download free eBooks at bookboon.com

10 Acknowledgments

The author wishes to express his appreciation to the many people and organisations that supported and encouraged him during the preparation of various publications, in particular, this book.

A publication with a similar name ("Good hygiene for data and personal computers") was part of a collection of booklets called The Information Society Library, published by the Diplo Foundation (www.diplomacy.edu) in support of the first World Summit on the Information Society held in Geneva in 2003. The Mindmap diagram of the original "Hygiene" book is included with the kind agreement of Diplo Foundation.

The MIS Training Institute (Europe, Middle East and Africa) (www.mistieurope.com) gave me the opportunity to attend and speak at several conferences on Information Security, Governance, Risk and Audit and the Chief Security Officers Summit. This in turn, allowed me to meet many key players in these domains, some of whom have, over the years, become good personal friends.

The Geneva Centre for Security Policy (www.gcsp.ch) for allowing me to join several of their workshops on information security.

Then come the many professional colleagues and friends who willingly gave their time to review and give candid comments on the drafts of this document. Special thanks are due to those who generously gave their time to discuss, comment and make suggestions, in particular (in alphabetical order):

Stefano Baldi, Director, Istituto Diplomatico, Ministry of Foreign Affairs, Italy;
Paul Dooley, CIO, United Nations Joint Staff Pension Fund, U.S.A.;
Keith Inight, Technology Strategy Director, ATOS, UK;
Gerben Klein Baltink, Secretary of the Cyber Security Council, The Netherlands;
Dr. Gustav Lindstrom, Head of the Emerging Security Challenges Programme, Geneva Center for Security Policy, Switzerland;
Esa Paakkonen, Certified Information Systems Auditor, World Health Organisation, Switzerland
Charles V. Pask, Managing Director, ITSEC Associates Limited, U.K.

The author also wishes to thank:

Steve Hathaway for his permission to use his photograph of a wolf in Chapter 1; and,
Ben Finio for his photograph of a robotic bee in Chapter 7.

Download free eBooks at bookboon.com

All the photographs and drawings in the book include the appropriate copyright notice. The author also acknowledges the goodwill of those uploading photographs to Flickr under the Creative Commons regime and with few restrictions on their use.

Finally, this book would have never been written if the author had not met over the years so many people who have no idea of what digital "hygiene" means and fail to protect themselves better. These are the equivalent of the Great Unwashed of past centuries range from the rather young who still have to learn to the Silver Surfers who tend to be put off by the jargon and apparent complexity of digital hygiene. Then there is the crowd in between these two.



Click on the ad to read more

Download free eBooks at bookboon.com