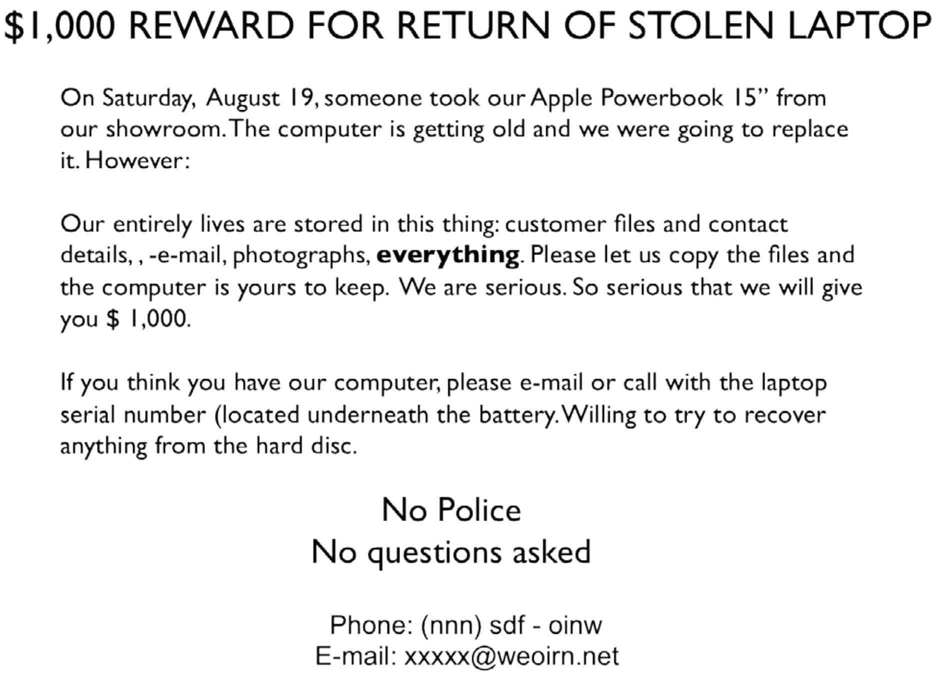
3 Good digital hygiene: the essentials



$1,000 REWARD FOR RETURN OF STOLEN LAPTOP

On Saturday, August 19, someone took our Apple Powerbook 15" from our showroom. The computer is getting old and we were going to replace it. However:

Our entirely lives are stored in this thing: customer files and contact details, , -e-mail, photographs, **everything**. Please let us copy the files and the computer is yours to keep. We are serious. So serious that we will give you $ 1,000.

If you think you have our computer, please e-mail or call with the laptop serial number (located underneath the battery. Willing to try to recover anything from the hard disc.

No Police
No questions asked

Phone: (nnn) sdf - oinw
E-mail: xxxxx@weoirn.net

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.

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

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.

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?

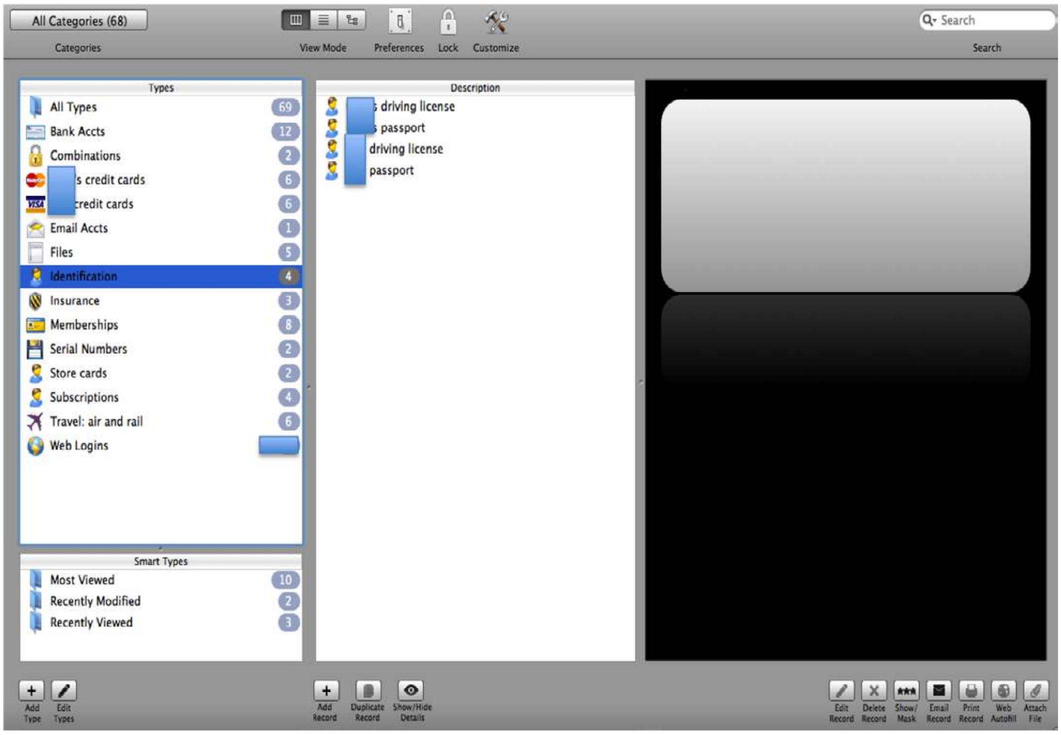
In the same way as a bank vault can be used to reduce the risk of loss or damage to valuables and important documents, there are software products that perform the same function by creating an electronic vault in your computer or smartphone.

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.



Types	
All Types	69
Bank Accts	12
Combinations	2
[redacted]s credit cards	6
[redacted]redit cards	6
Email Accts	1
Files	5
Identification	4
Insurance	3
Memberships	8
Serial Numbers	2
Store cards	2
Subscriptions	4
Travel: air and rail	6
Web Logins	[redacted]

Smart Types	
Most Viewed	10
Recently Modified	2
Recently Viewed	3

Description

[redacted]s driving license
[redacted]s passport
[redacted] driving license
[redacted] passport

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…

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.

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.

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.

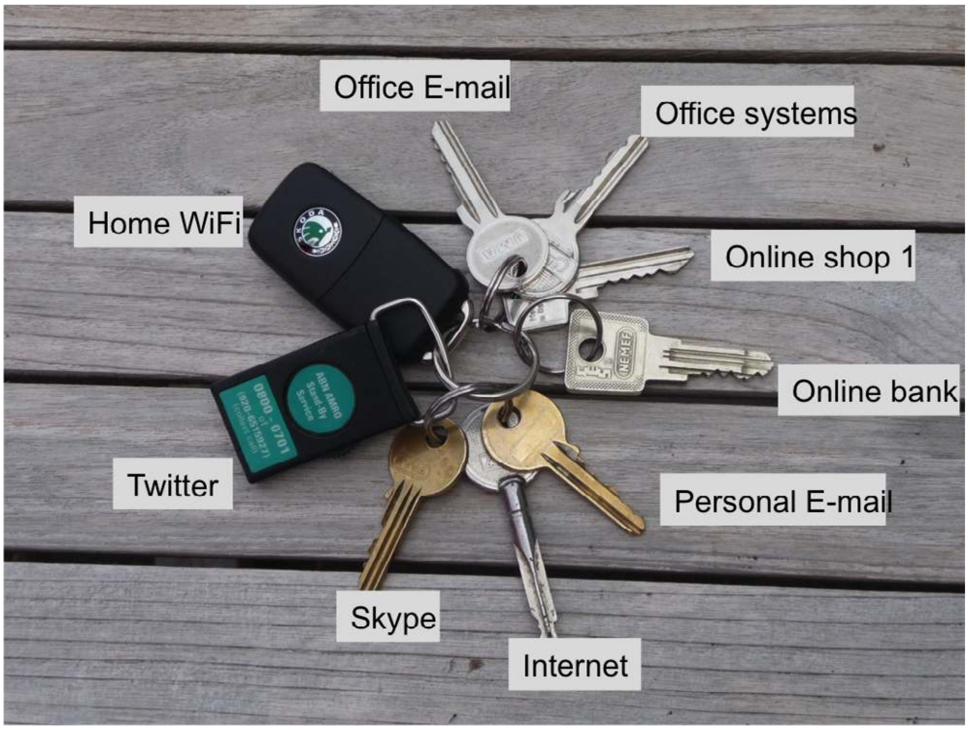


Figure 8: You have many keys – you should have many passwords for the same reason
© E Gelbstein, All Rights Reserved

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.

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.

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.

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).

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.

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?

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/

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.

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.

"I studied English for 16 years but... ...I finally learned to speak it in just six lessons"
Jane, Chinese architect
ENGLISH OUT THERE
Click to hear me talking before and after my unique course download