

Basic Information Systems

Free University of Bolzano Bozen – Dr. Paolo Coletti - Edition 10.0 (11 February 2021)

Introduction

This book is an overview of basic information systems for university courses, designed for students who start from a very naïve computer knowledge and experience. It contains in particular:

- computer introduction,
- Microsoft Windows,
- networks,
- dangers and security.

This book is usually updated every year, please take a look at the edition's date.

Disclaimers

This book is designed for very novice computer users. It often contains oversimplifications of reality and every technical detail is purposely omitted. Expert users will find this book useless and, for certain aspects, partially wrong.

This book supposes that the user is using Microsoft Windows 10 or macOS Catalina 10.15 operating system in English. However, it is perfectly readable with other versions, while some menus and procedures can be rather different if the language is not English (Windows language may be changed on multi-language installations).

The novice user in this book is, for simplicity, always considered male. This is not meant to be gender discrimination.

Table of Contents

Introduction.....	1	3.2. Communication	14
1. Computers.....	2	3.3. Internet connections	17
1.1. Hardware.....	2	4. Security	19
1.2. Software	3	4.1. Cryptography	19
2. Microsoft Windows	5	4.2. Passwords.....	22
2.1. Versions and editions.....	5	4.3. Viruses	24
2.2. Regional and language settings.....	6	4.4. E-mails	26
2.3. File system.....	7	4.5. Navigation.....	28
3. Networks	13	4.6. Attacks from outside	29
3.1. Technical aspects.....	13	4.7. Backup	30

1. Computers

This chapter presents a brief description of the most common storage devices and the typical software features for a novice user.

1.1. Hardware

Hardware are those parts of the information systems that can be physically touched, i.e. computer, tablet, smartphone, monitor, printer, keyboard, camera, etc.

1.1.1. Measure units

Computers have a very elementary way to store data: they can remember only 0 or 1. A value of 0 or 1 is called bit and all computer data are stored as sequences of bits. A sequence of 8 bits is called a byte, which is a quantity large enough to store usually a letter or a digit (even though often 4 bytes are necessary). Modern computers are able to deal with enormous quantity of bytes, forcing us to introduce other units of measure:

- Kilobyte (KB), approximately 1,000 bytes,
- Megabyte (MB), approximately 1,000 KB or one million bytes,
- Gigabyte (GB), approximately 1,000 MB or one billion bytes,
- Terabyte (TB), approximately 1,000 GB or one trillion bytes.

Usually, the unformatted text of a whole book can fit in some KB, while for an image in a good resolution (let's say ready to be printed on A4 paper) or for a song some MB are required, while a film in high quality needs some GB.

1.1.2. Moore's law

Over the last 60 years, computer hardware has been continuously improving its performances with an exponential growth. This growth is summarized by the famous Moore's law which says that the number of transistors in a processor doubles every 18 months. This law can be extended to several other hardware parts and we may say that the performance (be it speed or capacity) of hardware doubles every 18 months, thus leading to a general exponential growth. Unfortunately, software's performance does not increase in the same way.

1.1.3. Storage devices

The computer uses several devices to permanently store and move data, which vary a lot in terms of capability, cost, speed and portability.



The most used one is the internal hard disk, which is inside the computer box and cannot be moved easily. Its size currently ranges from 1 to 4 TB. On the other hand, an external hard disk is outside the computer, has the same size and obviously can be moved. Its only disadvantage is being slightly slower.

SSD Solid State Drives are starting to invade the market and will replace traditional hard disks. They are not disks at all, but very large memory cards shaped like a hard disk which can entirely replace the internal hard disk. Their main advantages are that not having moving parts (they do not rotate at high speed like hard disks) are more robust and that in most situations they are up to 10 times faster than traditional hard disks. Their disadvantage is the limited size which currently is maximum 1 TB and their high price.



USB flash stick or USB pen drive is the most used way to temporary store and move data. Its size is now up to 500 GB, however, its reliability is not perfect, therefore it is used mostly to move data.



Another common way to store and move data is through a memory card, used by devices such as photo cameras or to expand mobile phones' memory. From a technical point of view, they are identical to SSD or USB sticks.

1.2. Software

Software are all those products which cannot be physically touched and have therefore to be stored as information in storage devices. The software can be divided into three big categories: operating systems, programs, and data.

The operating system takes care of controlling device's hardware and human-computer interaction. Currently the most widespread operating systems are:



Microsoft Windows, which is the market leader for computers,



Macintosh computers have their own operating system macOS,



Linux (it is a family of very similar operating systems), which is a costless operating system for computers,



Android, a family of Linux-based operating systems for mobile devices,



iOS, for Apple mobile devices.

Programs are software which is used to do particular tasks, e.g. Word for document writing, Chrome for Web navigation, the Calculator for mathematical operations.

Data is everything which is produced either by the user or by programs (sometimes even by the operating system) to store information, e.g. a document file produced by Word is data, a downloaded web page is data.

1.2.1. Software licenses

The software can be divided, from a commercial point of view, using two features: the market cost and the permission to be modified.

Subdivision by market cost is:

- freeware, software which is completely costless. The producers of this software are either public institutions such as universities, or developers who do it for personal interest or advertisement or private company who do it for marketing reasons. Some examples are Skype communication program (the program itself it free, the service depends), 7-zip compression program or Linux operating system;
- shareware, software which is initially costless but after a certain period the user is asked to pay a fee or delete it. It can also be a software which has two versions: a free one, but incomplete or with advertisement banners, and a complete advertisement-free one, for which the user must pay. The most popular examples are mobile phones apps;

- commercial, software for which the user has to pay a license to use it. A typical example is Microsoft Windows operating system;
- subscription-based, software for which the user pays a periodic fee to use it. This software often is also offered on the web and in this case the user does not have to care about installation nor updates. Examples are Microsoft Office 365 and Adobe Photoshop Creative Clouds;
- private, software uniquely built for a specific customer to fit his needs. Only the customer may use it. A typical example is the university's database that handles students, courses, exams and professors.

The market cost is the price paid to buy the software license and, eventually, to install it when it needs a technical intervention. However, complex software have also a maintenance cost, which can be explicit in case the owner has to pay updates or technicians. The maintenance cost, however, can also be hidden, whenever the owner has to change his procedures and retrain himself or an entire company on the new software, with a consequent temporal decrease in productivity. The sum of the market cost and actualized maintenance cost, including training and decrease in productivity, is called total cost of ownership and it is the cost which must be taken into account whenever deciding before buying a new complex software.

The permission to be modified can seem a trivial question for the novice user, however for program developers and computer experts being authorized to modify a software is a great advantage since it can be improved, tailored to specific needs, errors can be corrected and in particular what it exactly does is public domain. The “open source versus proprietary software” is a strong ethical and economical debate in the computer scientists' community. Subdivision by permission to modify, grouped in categories, is:

- open source software may be studied, used and, in particular, legally modified by anyone. The software developers at the same time legally authorize to modify and distribute the source of the software to put other developers in a condition to easily modify it. Open source software is also automatically freeware. The most typical example is Linux operating system;
- copyleft software is open source but carries the restriction that any modification must be distributed as open source and copyleft, thus impeding that software becomes, after a modification, proprietary. The most famous copy left contract license is the GNU Public License (see <http://www.gnu.org/licenses/gpl.html>);
- proprietary software is distributed (costless as Adobe Acrobat Reader, or as a shareware as WinZip, or most often sold as commercial software as Microsoft Office) with the explicit legal warning not to modify it and technically locked to prevent other developers to see or modify its source.

1.2.2. Software naming

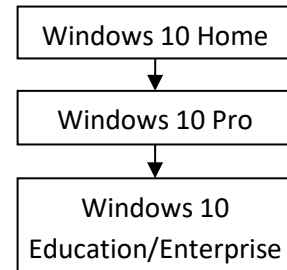
Software is usually identified by a name, for example “Linux” or “Microsoft Office”, sometimes by a distribution/edition name “Linux Ubuntu”, “Microsoft Office Professional” and very often by a version number, a sequence of numbers, points and letters (sometimes, as for Windows, commercial names) which distinguishes the changes made by developers with time, such as “Linux Ubuntu 17.04” or “Microsoft Office Professional 2016”. Obviously, the version numbers of open source software change rapidly, due to the many developers working on them.

2. Microsoft Windows

Microsoft Windows is currently the market leader operating system, it is the usual interface which appears when the user turns on a personal computer with Windows operating system. Its biggest competitors is Mac OS which is installed on 17% of worldwide computers (December 2020).

2.1. Versions and editions

Microsoft released Windows 10 in July 2015. It is available in only three editions. Education/Enterprise edition is currently (December 2020) installed on 73% of worldwide computers and on most UNIBZ computers.



2.1.1. Computer locking problem

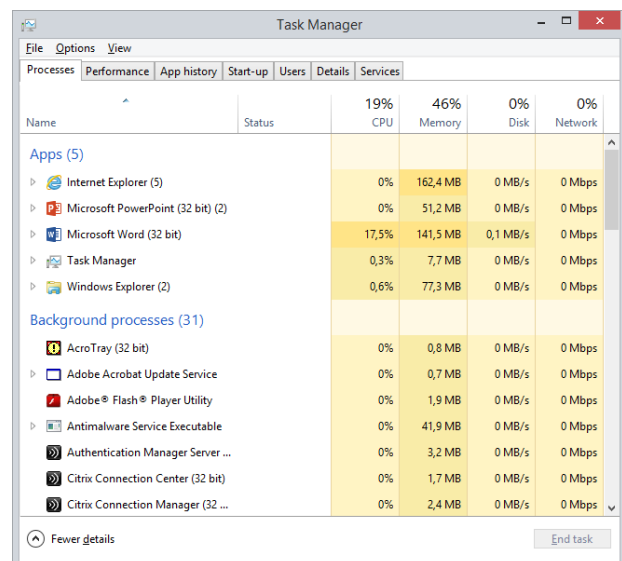
Microsoft Windows, and also Mac OS, sometimes becomes unstable: it can unpredictably, without any warning and when the user does not expect it and typically when he is doing something very important and urgent, lock and refuse to respond to user's actions. When this happens, it is usually caused by the program that is used and therefore the first thing to do is to try to close the current program. If this does not improve the situation, the only other solution left is to turn off the computer. The list of operations to try until the computer answers to user's commands is:

1. if the mouse works, click the X button on the program window or otherwise press ALT+F4. On the Mac $\text{⌘}+\text{Q}$;
2. press CTRL+SHIFT+ESC; press More details; select the program from the list and press End Program. On the Mac a similar window appears pressing $\text{⌘}+\text{ALT}+\text{ESC}$;
3. press for a long time CTRL+ALT+DEL and, from the bottom right icon, choose Shut Down. On the Mac $\text{⌘}+\text{CTRL}+\text{ALT}+\text{power}$;
4. press the computer on/off button;
5. unplug the electric power.

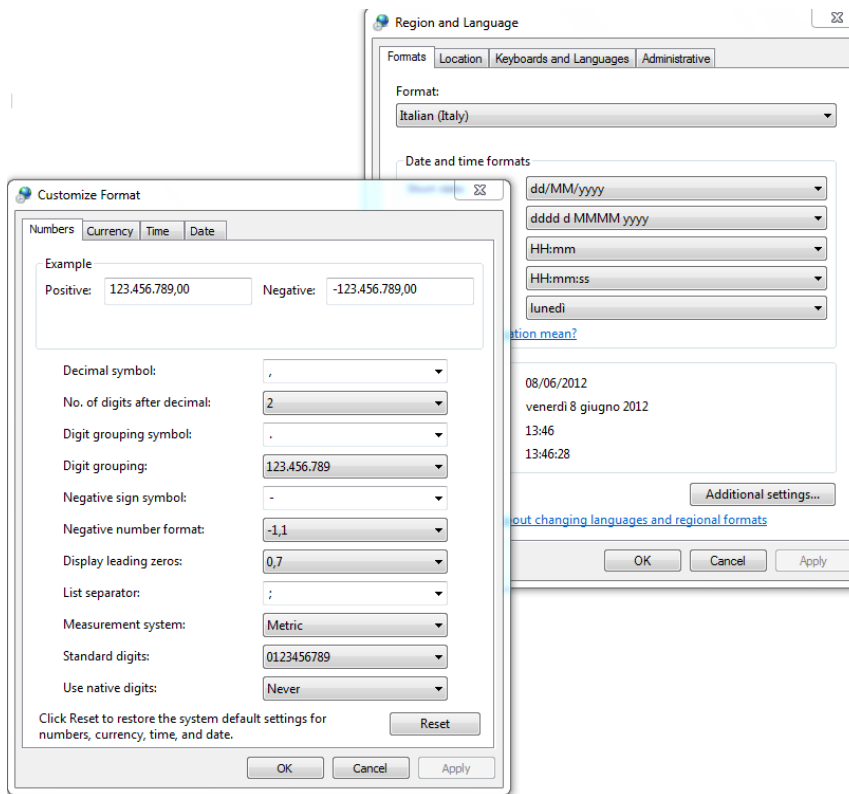
In any case, all the current unsaved work will be lost; in the last two cases the operating system can

sometimes be damaged but very often it will repair by itself the next time the computer is turned on.

Therefore, it is always a very good idea to save very often the current work, especially when it is important, urgent or difficult to redo.



2.2. Regional and language settings



Keyboard settings and number formats may be changed searching for Control Panel, then pressing Clock and Region -> Region -> Formats -> Additional Settings. Here the user is able to change the format of numbers, especially the decimal separator, the currency and the date format, especially the American (month-day) and European (day-month) and European (day-month) formats. Moreover, it is always a good idea to check that the list separator is set always to the semicolon, otherwise Excel's functions will not work properly. A similar menu can be accessed on the Mac going to System Preferences -> Language & Regions -> Advanced....

2.2.1. Keyboards and languages

Before starting this section it is necessary to take a close look at your keyboard. Locate these keys:

English keyboard	German keyboard	Italian Keyboard	Main function
CTRL	STRG	CTRL	
Windows	Windows	Windows	Activate shortcuts in Windows
ALT	ALT	ALT	
ALTGR	ALTGR	ALTGR	Produce character on the key's bottom right
F1 to F12	F1 to F12	F1 to F12	
DEL	ENTF	CANC	Delete character on the right
INS	EINFG	INS	Toggle insert/overwrite mode
HOME or	POS1		Go to beginning
END	ENDE	FINE	Go to end
PG↑ and PG↓	BILD↑ and BILD↓	PAG↑ and PAG↓	Go one page up or down
BACKSPACE or			Delete character on the left
ENTER or		INVIO or	Enter data
TAB or		TAB or	Move through the window
SHIFT or			Capitalize letters
CAPS LOCK or			Keep SHIFT pressed
			Move the cursor

Command ⌘	Command ⌘	Command ⌘	Only the Mac. It replaces some functions of CTRL
-----------	-----------	-----------	--

In this course book, the English name for keys will be indicated. When A+B is indicated, it means that the user must press key A, then press key B and then release both keys.

Another operation which can be useful in a multi language environment is changing the keyboard. While this can be done from the Language menu of the Control Panel, it is much easier to adjust it directly from the right side of the application bar, simply clicking on keyboard icon and selecting the appropriate one. If no keyboard's choice appears on the application bar, just press SHIFT with the left ALT key to toggle among available keyboard's settings.

2.3. File system

Before starting this section it is necessary to do the following operations:

1. search for Control Panel
2. Control Panel -> Appearance and Personalization -> File Explorer Options -> View
3. deselect Hide extensions for known file types.

In this way extensions (see section 2.3.3) are shown and file types can be better recognized.

In case you are using a Mac, it is even easier. Go to Finder -> Preferences menu -> Advanced tab -> check "Show all filename extensions".

2.3.1. Files and directories

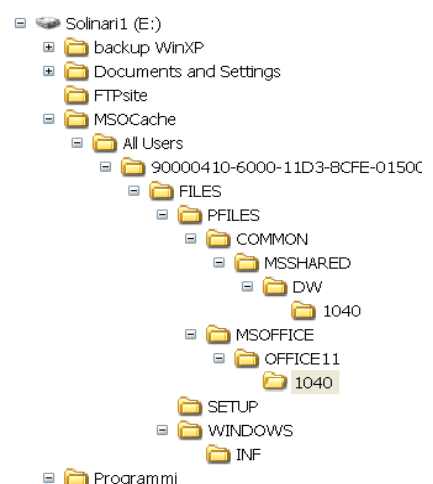
The software is stored on storage devices in a special container called file. The operating system uses a lot of files for itself and for its data, a program usually uses one file for itself and other files for its data and the user uses some files for his data. A file is represented by a small picture called icon.



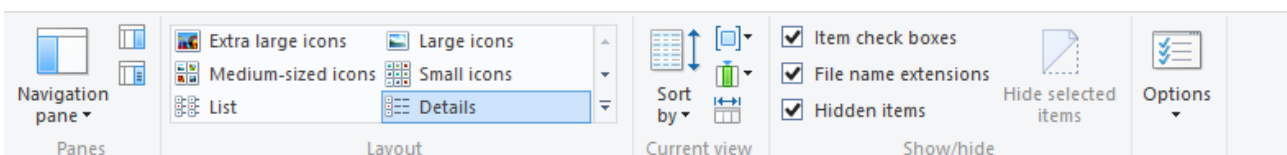
Another special object is the directory or folder, which is basically a container for files and other directories and is represented with an icon depicting a yellow closed or open folder. Double clicking on a directory opens a new window which presents the directory content.



Each storage device is a big directory, accessible from My Computer window, which contains directories and files. Each of these subdirectories may contain other files and other sub-subdirectories, and so on in a hierarchical way, forming a tree with the hard disk (or another storage device) as the root, directories as branches and files as leaves. Local disks are usually indicated with a letter and a colon, such as C:.



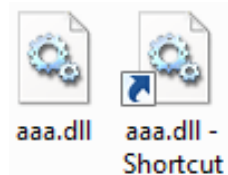
Choosing the "View" menu of a directory's window provides the user with several different ways to look at files and directories, the most important way being the Details which can show interesting information on files and directories such as their size and date of last modification.



Each file and directory can be univocally identified by its absolute path or address. For directories it is the path which appears on the address bar of the directory window, while for files it is the path of their containing directory followed by “\” and the file name. For example, the absolute path of directory “System32” in “Windows” directory on the C: hard disk is “C:\Windows\System32\” as can be seen from the address bar. While, the napipsec.dll file has the absolute path “C:\Windows\System32\napipsec.dll”.

Note that Windows operating system is not case-sensitive: capital or small caps letters in paths are perfectly equal. For Mac OS it depends on how hard disk was configured.

A special and tricky object is the link or shortcut. Although its icon looks like a file icon, the small curved arrow on the left corner clearly indicates that this object is a link. A link is simply an address to a file or directory, it is not a real file or directory. When the user double-clicks on the link, the computer behaves exactly as if the user is double-clicking on the real file or directory (if the operating system can find the real one, which is not the case if in the meantime somebody deleted or moved it). Instead, any copy/move operation on the link will simply copy/move the link and not the real file or directory; especially copying/moving the link to another disk will probably cause it to malfunction. Therefore it is a good idea for novice users to avoid using links at all.



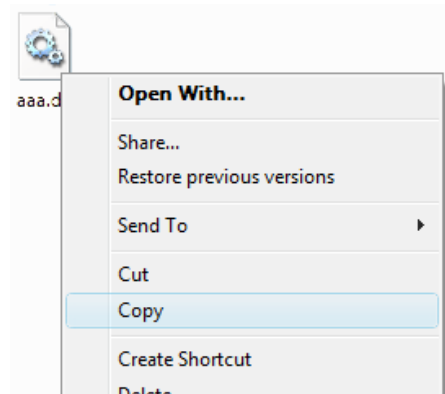
2.3.2. Files' operations

When double clicking on a file, the operating system usually starts a program. The user is often unaware of an important difference:

- double clicking on a program runs the program which was double clicked
- double clicking on a data file calls the program associated with that file type and runs it, at the same time telling the program to open the file. If no program is associated with that file type, Windows asks the user which program should open the file.

Copying a file means reproducing it to another location or to the same location with a different name. Copying a directory means reproducing it to another location, or to the same location with a different name, together with its entire tree of subdirectories and files. To copy a file or directory, the operating system offers several methods, the most used being:

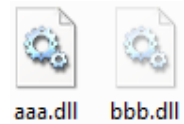
- drag the object to the destination. If a symbol + does not appear, press CTRL key to have it appear while dragging. On the Mac press ALT. Release the object in the destination;
- select the object and click the right mouse button. Select Copy. Point the mouse to the destination and click the right mouse button. Select Paste (Paste Item on the Mac). If the destination is the original directory, the file name changes to “copy of ...”;
- select the object and press CTRL+C. Point the mouse to the destination and press CTRL+V. If the destination is the original directory, the file name changes to “copy of ...”. On the Mac use command key ⌘ instead of CTRL.



Moving a file means moving it to another location losing the file in the original place. Moving a directory means moving it to another location together with its entire tree of subdirectories and files. To move a file or directory the operating system offers several methods, the most used being:

- drag the object to the destination. If a plus or a link symbol does appear, press SHIFT key to remove it. Release the object in the destination;

- select the object and click the right mouse button. Select Cut (Copy on the Mac) and the icon becomes lighter. Point the mouse to the destination and click the right mouse button (pressing also ALT on the Mac). Select Paste (Paste Item on the Mac);
- select the object and press CTRL+X and the icon becomes lighter. Point the mouse to the destination and press CTRL+V. On the Mac the only way to do it is to press $\text{⌘} + C$ to copy, then right click and press ALT until you see “Move Item Here” and select it.



To create a link to a file or directory:

- drag the object to the destination of the link. If the curved arrow symbol of the link does not appear, press CTRL+SHIFT or ALT until it appears. On the Mac press $\text{⌘} + \text{ALT}$. Release the object in the destination;
- select the object and click the right mouse -> Create Shortcut. On the Mac it is “Make Alias”. The link is created in the same directory.

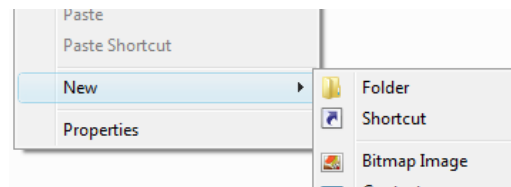
Deleting a file means often putting it into the Recycle Bin (called Trash on the Mac) where it can be recovered unless the recycle bin is emptied. Deleting a directory means putting it into the recycle bin together with its entire tree of subdirectories and files. To delete a file or directory the operating system offers several methods, the most used being:



- drag the object onto the Recycle Bin and release it;
- select the object, right-click and choose Delete. On the Mac choose Move to Trash;
- select the object and press DEL key. On the Mac press $\text{⌘} + \text{DEL}$ instead;
- select the object and press SHIFT+DEL. This operation deletes the object without passing through the Recycle Bin. On the Mac press $\text{⌘} + \text{ALT} + \text{DEL}$.

To rename a file or directory, simply select the object, click on the name and retype it. Alternatively, right-click and choose Rename. Usually, the operating system accepts most names, but novice users should stick with only letters, numbers, and spaces, since other characters may be forbidden.

To create a new directory, simply right-click the mouse and choose New and then Folder. After the creation, rename it.



Sometimes files occupy a lot of space and need to be reduced to save disk space or to be sent by e-mail; other times files must

be put in a package to remain together or to be sent as a single file via e-mail. These two operations are accomplished compressing a set of files and directories, which means using a special program (7-Zip or IZArc or the operating system itself) to reduce (from 0% to 90% depending on the file type) the file size and produce a new single file called zip-archive containing all the selected files and directories.

To compress a set of files and directories:

1. select the files and directories together,
2. click the right mouse key,
3. select 7-Zip or IZArc or the installed compression program and select something like Add to Archive File...,
4. a dialog box appears asking you to choose the zip-archive name and its destination;
5. in this dialog box, you must also choose the compression method, which is strongly suggested to be ZIP to be compatible with other programs;
6. in this dialog an encryption method (see section 4.1) may be chosen. If your zip-archive should be opened by anybody, then choose “None”. Otherwise, if you want the zip-archive to be uncompressed

only by people knowing a proper password, choose any of the encryption methods with at least 128 bits, such as “AES 256”, and provide the password.

Other files or directories may be added later to the zip-archive simply dragging them on the zip-archive file (this is a copy and not a move operation) if it is not encrypted.

On a Mac you start Keka, choose zip as the compression format, write any password if you want to encrypt the archive and drag the files and directories on the program window.










To extract files from a zip-archive file, simply click the right mouse key on the file and from the drop-down menu choose the appropriate extract option: the content will appear in the location you have chosen, together with all its directories' structure.

When double clicking on a compressed file, if the compression program is properly installed, it will open in a window as if it were a directory. But it is not a normal directory, it is simply a window produced by the program, with the list of the zip-archive's content: the user should not open files from this window since it is a very unreliable way to modify files! Files can be copied from this window to a real directory simply dragging them to the directory. When the entire content of the zip-archive has to be extracted or when the user wants to preserve the original tree structure, it is better to use the Extract button of this special window.

If you are using Keka for Mac, usually double-clicking the archive file immediately uncompresses it recreating the directory structure, without displaying the content.

2.3.3. File types

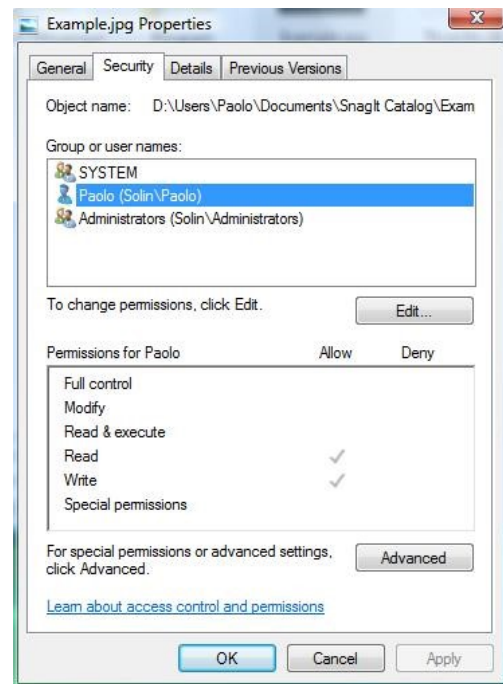
Windows identifies the file's type by its extension, which is everything appearing after the last dot in the file's name. Usually, it is an acronym of 3 or 4 character. Using the file extension, Windows knows the file type and decides which program will open that file. If the file extension does not show up, follow the instructions at section 2.3. The most important file types are:

File type	Program that typically opens it	Typical extensions	Typical icons
Program	itself	.exe .com .bat	
Compressed	WinZip / 7-Zip / IZArc	.zip	
Text	Notepad	.txt	
Document	Word / Acrobat Reader / PowerPoint	.docx .doc .rtf .pdf .ppt	
Sheet	Excel	.xlsx .xls .csv	
Image	Windows Photo Viewer / Photo / browser	.jpg .jpeg .gif .bmp .png	
Video	Windows Media Player / VLC	.avi .mov .mpg .mpeg	
Audio	Windows Media Player / WinAmp	.mp3 .wav	
Web page	the default browser	.html .htm	

2.3.4. File permissions

For each file and directory the operating system assigns permissions. Click the right button of the mouse on a file or directory and select Properties and then Security. On a Mac choose Get Info and then Sharing & Permission. The dialog box shows the list of users or groups of users who may access this object, while not listed users may not access it. For each user or group this dialog box displays the permissions, the most important in Windows being:

- read, to copy and open the object. Note that this includes creating a copy with a different name and then modifying it;
- read and execute, same as read, plus run the file if it is a program;
- list content (for directories), to see the content;
- write (for directories), to create files and subdirectories;
- modify (also called, when referred to a file, write permission), same as read and execute, plus delete, move, rename, modify;
- full control, same as modify, plus change and assign permissions.



The creator of the file usually has full control on it and may change permissions or add new authorized groups or users. A special group is the Administrators group (containing the users involved in the technical administration of computer) which has full control on every object.

2.3.5. Network folders at UNIBZ

On UNIBZ LAN there are shared hard disks on which common data are stored, so that it is accessible from every computer. These are called network folders. Some of them are:

- \\ubz01fst.unibz.it\courses\course_coletti which contains files that will be used during the course. These files must never be opened double-clicking from here, otherwise they will be locked for other users. They should be copied on each user's Desktop before opening them;
- \\ubz01fst.unibz.it\courses\exam_coletti\, followed by user's login name or the user's last name and first name, which will contain exam files and which is accessible only by the user;
- \\user.unibz.it\unibzhome\ and \\user.unibz.it\unibzredir\ followed by your login name contain your Documents and Desktop of UNIBZ computers. I do not know which one exactly, as I do not have a student's account unfortunately. Try!

While connecting to these directories from a UNIBZ computer is straightforward, if you are using your own computer you must take care that you are either connected to ScientificNetwork WiFi or using a VPN connection through Cisco AnyConnect (use vpn.scientificnet.org as server). When asked for login name and password, digit unibz.it\login name instead of simply your login name. Finally, Mac users may find it much easier to map it permanently: make sure you are connected to ScientificNetwork WiFi or are in VPN, Finder -> Go -> Connect to Server, use as address \\ubz01fst.unibz.it (try smb://ubz01fst.unibz.it, if that one does not work) then enter unibz.it\login name and your password and click OK.

2.3.6. Virtualization at UNIBZ

Whenever the user logs in on Windows 10 a Desktop computer at UNIBZ, the computer connects to a server on which the operating system Windows 10 is effectively running. Thus, the computer is acting as a mere terminal. This is called virtualization (see 3.1.2). In this way the user always finds his configuration and all his files as they have been left on the last used computer. The configuration is saved on the server, while the user's files are saved on network disk \\user.unibz.it (see 2.3.5). Whenever the user enters his Desktop or Documents, he is entering this network directory instead.

This mechanism works fine only if the user is not using too much disk space (which is usually 300 MB). If the user is over quota, the system sends a warning via e-mail to the user and, if the user remains over quota, the user may be forbidden from saving any other file. Therefore, it is a good idea to always save large files on a USB stick (and copying them later to another personal computer) and to periodically check the disk space looking at the properties of this directory. If a warning e-mail has been received, files need to be deleted, possibly not from the current computer but directly from the network directory.

3. Networks

Nowadays a computer is very likely to belong to a company's or home network. Without entering too much into the technical details, this section will explore the situations in which a novice user can find himself in troubles and how he can try to survive dialoguing with network administrators in their own strange technical language.

3.1. Technical aspects

A computer network is a set of devices which communicate and share resources. These devices are mostly computers or smartphones and sometimes stand-alone hard disks, telephones, printers and terminals (see 3.1.2).

3.1.1. Server and client

A network interaction is based on the client-server architecture: one device is the server and the other one is the client. The server is the device which is offering its resource, usually programmed to wait until someone asks for its resource. The client is the device which uses the resource, which sends the request to a waiting server.

For example, when sending a document to the printer, the user's computer is the client while the printer is the server; when retrieving personal e-mails, the user's computer is the client which connects to the mail-server asking for available e-mails.

The same device may act as client for a service and server for another service. For example, a library computer may have data shared to the other network users (server) and may be at the same time used by a user to print his own documents (client for the printer).

3.1.2. Virtualization

Virtualization is a technique which is rapidly growing, in particular in large organization, thanks to the arrival of powerful multi-processor computers. It consists in not having standard personal computers with their own operating system but in using these computers as terminals, running their operating system (called virtual machine) on another very powerful computer. The terminal itself simply provides screen, keyboard and other user's input/output devices, while all the memory and computation efforts are on the computer where the operating system is really running. This system has several advantages for large organizations:

- old computers can be recycled as terminals, increasing the amount of available computers;
- everybody has exactly the very same operating system with all the programs installed in the same way;
- software maintenance is centralized, i.e. it needs to be done only on the main computers used for running the operating systems and not on hundreds of different computers;
- users can use programs without having to install them on their own computers.

This is the technique adopted by UNIBZ for all computer rooms and for notebooks: whenever you switch the computer on, you log in on the virtualization program which offers you the possibility to use some operating systems or even some specific programs without loading the entire operating system. A similar system is offered to every UNIBZ user through VMware, simply connecting to <https://Desktop.scientificnet.org> and either choosing to install the client program or simply using it via web however without access to your local hard disk.

Another usage of virtualization consists in creating a virtual machine running on your very same computer, using for example Hyper-V for Windows or VirtualBox for Mac. This has the advantage that you can have another operating system on your own computer (for example a Mac computer with the Mac OS operating system running and on it a virtual machine with Windows 10) but in particular that you can easily make a copy of the virtual machine (it is just a huge file), test some new dangerous software on the copy and in case simply delete it and return to your clean original virtual machine.

3.1.3. Areas

Each network usually distinguishes three areas:

- Local Area Network (LAN or Intranet), usually the network of devices in the same building or belonging to the same owner. Inside the LAN every device is well identified and usually every user is known. It is considered a trusted area.
- Wide Area Network (WAN or Internet), which is everything which connects LANs. Devices' and users' identification is very hard and anonymity is possible. It is considered a dangerous area.
- Virtual Private Network (VPN) is a technology to recognize a device in the WAN as a trusted device: the user is identified with a password and his computer, even though connected via the Internet, will be considered as part of the LAN, for as long as it remains connected. VPN is typically required to identify portable computers connected from remote sites.

3.1.4. Transfer speed

The network connecting components are cables, which determine the speed of the LAN. Cables have a speed measured in bps (bits per second) which indicates how many bits can flow through the cable in one second.

- Ethernet cables have a speed of 10 Mbps and can thus carry 1.25 MB each second, meaning that, for example, a 6 GB movie can be transferred in about 107 minutes from one device to another one, supposing no one (neither users nor autonomous devices) is using that network tract for other purposes during the transfer.
- Fast Ethernet cables have a speed of 100 Mbps.
- Gigabit Ethernet cables have a speed of 1 Gbps.
- A wireless network, a cableless network where devices use radio signals to communicate, has a speed up to 300 Mbps.

To find out how much time does it take to transfer a file with a size expressed in bytes, divide by 8 the connection speed in bps to find out the byte rate per second and then divide the file size by the speed to find out the number of seconds it takes for the file transfer. For example, to transfer a 600 MB file through a Fast Ethernet connection, find out the speed of 12.5 MB per second (12 500 000 bytes per second) and then divide 600 MB (or 600 000 000 bytes) by 12.5 (or by 12 500 000) to find out the time of 48 seconds. Pay special attention whenever the file size is expressed in units (KB, MB, GB, TB) which are different from speed (Kbps, Mbps, Gbps).

3.2. Communication

Inside a network, many communication programs are installed on Intranet devices to connect to the Internet or even to internal devices.

3.2.1. World Wide Web

The WWW is a part of the Internet organized as an hypertext and accessible through a browser. It is not, as commonly believed, the entire Internet, as other things are going on on the Internet, such as e-mails, direct communication between computers, file transfers (e.g. for cloud services), chats and calls (e.g. WhatsApp).

A particular part of the WWW is the Deep Web, which consists in all those pages and documents which are not linked by other publicly available pages. The result is that these pages are also not indexed by search engines and are accessible only by users who know their direct address. Usually these pages include personal pages, reserved information or services for which a payment is required.

A subpart of the deep web is the Dark Web, which consists in pages which cannot be accessed using a standard browser. Whenever you connect with a standard browser you communicate your IP number to the visited website and you know the website's IP number. With the IP number your provider and the website's provider are identified and therefore you and the website are easily identified by local authorities. The Dark Web requires you to use browser Tor, which does not connect directly to the website but hops on 6 different sites thus losing track of your and of the website's IP numbers, but with a general connection's slowdown. This guarantees anonymity to the user as well as to the website real location.

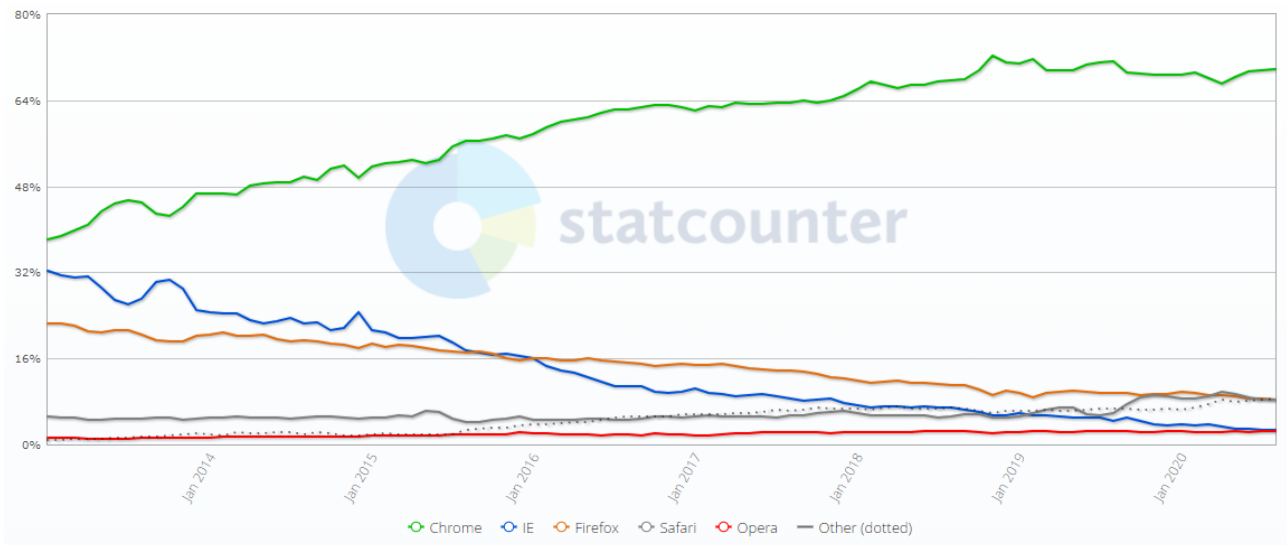
Most of the Dark Web content runs around illegal activities, from drug selling to counterfeited or stolen identities up to child pornography and weapons. However, it is also used by journalists who want to remain anonymous for their own safety and by libertarian activists.

3.2.2. Web browser

A web browser is a client program to navigate the WWW and retrieve web pages. It runs directly on the user's device as a client and connects to external web-servers, identified with the www prefix in the Internet name.



The market leader with more than 60% is Chrome, the browser from Google, followed by Safari, the Mac native browser, and with the two once popular Internet Explorer/Edge, a freeware proprietary software, and Mozilla Firefox, an open source software, now in decline.



Source gs.statcounter.com

3.2.3. Posta Elettronica Certificata PEC

When sending an e-mail, the sender has no proof that it has been sent, for example, to be used in a court of justice, and no guarantee that the e-mail has been dispatched. Some mail readers use a receipt system, but the receiver is not obliged to send back the receipt. In order to overcome these problems, many solutions have been proposed. The Italian Posta Elettronica Certificata (PEC) system is one of the few implemented solutions, thanks to law 82/2005 which determines that PEC receipts are legal proves.

A PEC address is a special e-mail box which is handled by a provider with specific technologies and which is identified by the presence of the word “pec” in the address. When an e-mail is sent from a PEC address to another PEC address, the sender receives two receipts: the first one is a proof that the e-mail has been sent with date and time, while the second one is a proof that the e-mail has been dispatched to the mailbox of the receiver. This does not represent a proof that the e-mail has been actually read, but from the moment the e-mail is dispatched to the mailbox, it is the receiver’s responsibility to read it. Under these circumstances, it is perfectly equivalent to “Raccomandata con Ricevuta di Ritorno” (“Certified Mail with Return Receipt Requested” in USA, “Registered Mail” in Canada).

E-mails can be sent also from a PEC address to a non-PEC address and, in this case, the sender gets only the sent proof but not the dispatched proof, like the “raccomandata semplice”. When an e-mail is sent from a non-PEC address to a PEC address, no receipt is produced and this is equivalent to a standard letter.

Another issue of standard e-mail is that the sender’s identity is not certain, as the e-mail address in the From field can be very easily changed, even by unskilled user. Moreover, the e-mail can be intercepted and altered, even though this is usually much harder to do. Therefore, even though it is not officially required by the PEC standard, many providers apply to PEC also encryption and digital signature (see section 4.1.1 **Error! Reference source not found.**) to guarantee automatically that content be not altered and that the sender’s e-mail address is really the indicated one.

3.2.4. Search engines

A search engine is a special program running on a website which offers to the user the possibility of searching other websites for specific web pages. The user needs to connect to the search engine website and digit the keywords, or sometimes even a complete question, and the website returns the list of relevant web pages.

Search engines use a crawler technique on the visible web: they continuously go through the known web pages memorizing their content and trying to discover other web pages through the contained links. In this way, they are able to memorize the visible part of the World Wide Web. The non-linked websites, the Deep Web, can remain unknown to search engines.

The most popular search engines are Google, the current market leader, Yahoo! and Bing. According to 2020 data, the percentage of use of these engines are Google 92%, Yahoo! 2%, and Bing 3%. In order to choose the order in which web pages are displayed to the user, search engines use a page ranking algorithm. The most famous one is Google’s PageRank which relies on the idea that a page which received many links is very important and useful; therefore a web page receives a score proportional to the number of web pages which put a link to it.

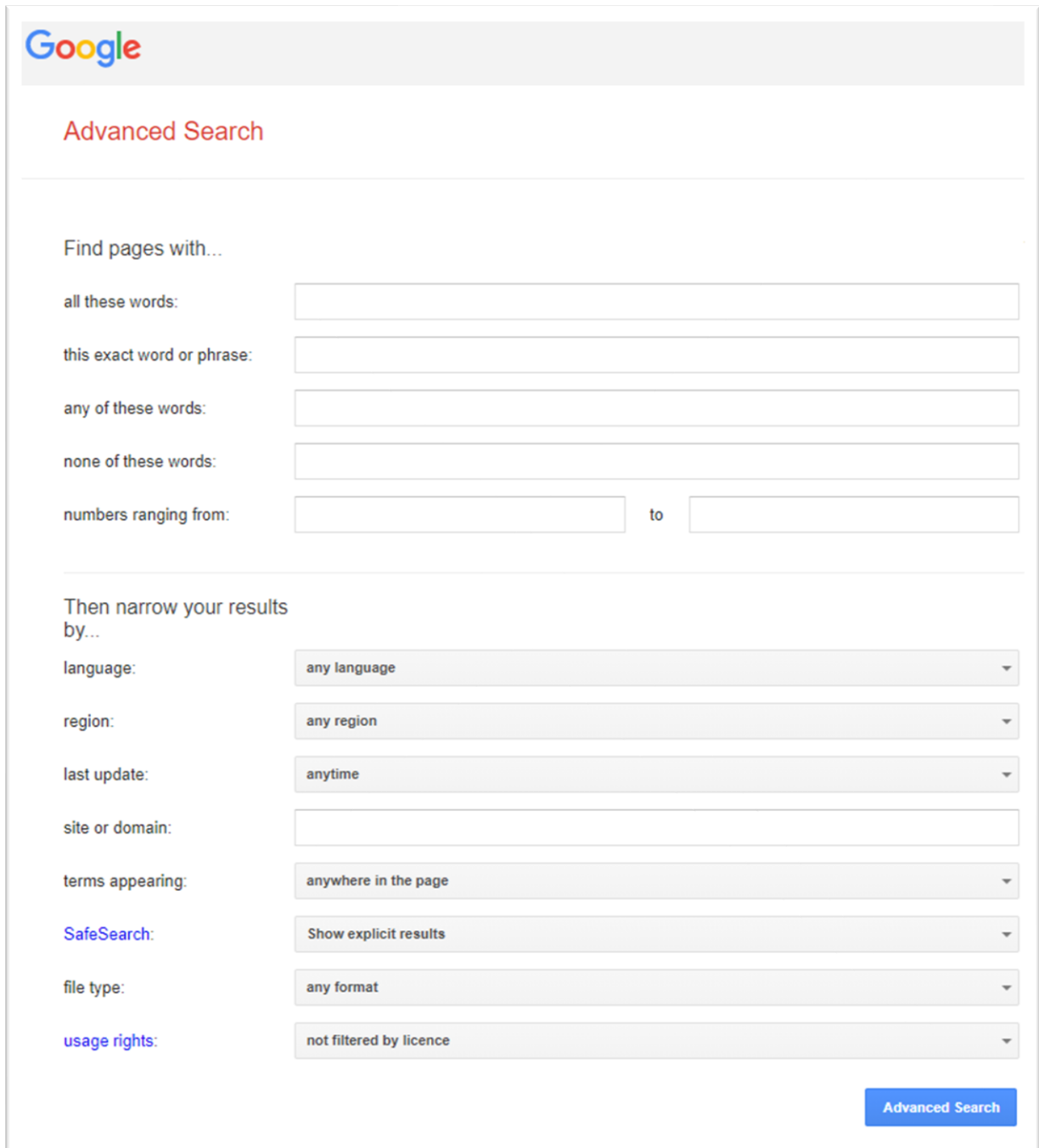


There are many tricks to speed up the web search and arrive quickly to the desired result:

- most novice users search the WWW using only a single keyword, which often produces the right result but, in some cases, can result in long lists of wrong results, for example when looking for Java

Island web pages typing simply “java”. Using as many keywords as possible often avoids wrong results, even though sometimes returns no pages if too many words are used;

- putting some words between quotation marks forces the search engine to look for the exact phrase, i.e. exactly for those words in that order and with no words in between;
- in the Advanced Search menu often there are very interesting options, such as the search of pages only in a specified language or only in a specified format, for example .doc or .pdf;



The image shows the Google Advanced Search interface. At the top left is the Google logo. Below it, the text "Advanced Search" is displayed in red. The main section is titled "Find pages with..." and contains five search criteria, each with a corresponding input field:

- all these words: [input field]
- this exact word or phrase: [input field]
- any of these words: [input field]
- none of these words: [input field]
- numbers ranging from: [input field] to [input field]

Below this section, the text "Then narrow your results by..." is followed by several filter options, each with a dropdown menu:

- language: any language
- region: any region
- last update: anytime
- site or domain: [input field]
- terms appearing: anywhere in the page
- SafeSearch: Show explicit results
- file type: any format
- usage rights: not filtered by licence

A blue "Advanced Search" button is located at the bottom right of the form.

3.3. Internet connections

There are many different ways to connect to the Internet. Some are old technology, rather slow and used right now only when no other means is available, such as the old telephone line or the ISDN or GPRS technologies. Modern connections are called broadband:

ADSL (Asymmetric Digital Subscriber Line)	telephone line modem	1 Mbps in upload 20 Mbps download	
Fibre optic	telephone line modem	1000 Mbps	
UMTS (Universal Mobile Telecommunications System) 3G	3G mobile phone	5 Mbps in upload 40 Mbps in download	
LTE (Long Term Evolution) 4G	4G mobile phone	100-1000 Mbps	
5G	5G mobile phone	1-10 Gbps	Still under development in 2021

4. Security

Being connected to the Internet means giving anybody access to the device. Despite the traditional novice user's belief that he is the one who goes outside, it is instead the Internet world which is coming inside, with all its benefits and dangers. Knowing a little bit of security is nowadays necessary even to the non-expert user, to avoid being lured into traps or adopting potentially dangerous behaviors.

Personal data is one of the most important security aspect to take care of. The European GDPR 679/2016 on data protection has cancelled the previous Allegato B of the Italian law 196/2003 which contained the minimal security techniques which must be adopted. Now there are no more specific rules for handling personal data, but the decision of security level is left to companies and professional users which must be able to prove to use all the up-to-date security measures depending on which kind of data are handled. This law applies clearly to companies and professionals, while it does not apply to users who handle data exclusively for personal use.






Good security measures include

- each employee must be authenticated by a personal username and a password or a biometric device or a personal token;
- each employee must have its own permissions, limited only to the data he needs for his work, and the permissions must be revoked when the employee does not need them anymore;
- employees must receive specific training or instructions to be able to use their authentication and to be aware of their responsibilities, duties and the possible dangers;
- all data must be constantly backed up (see section 4.7);
- software must be updated as frequently as possible;
- sensitive data (race, sexual preferences, genetic, religious belief) must be kept encrypted or in such a way that subjects are not identifiable.

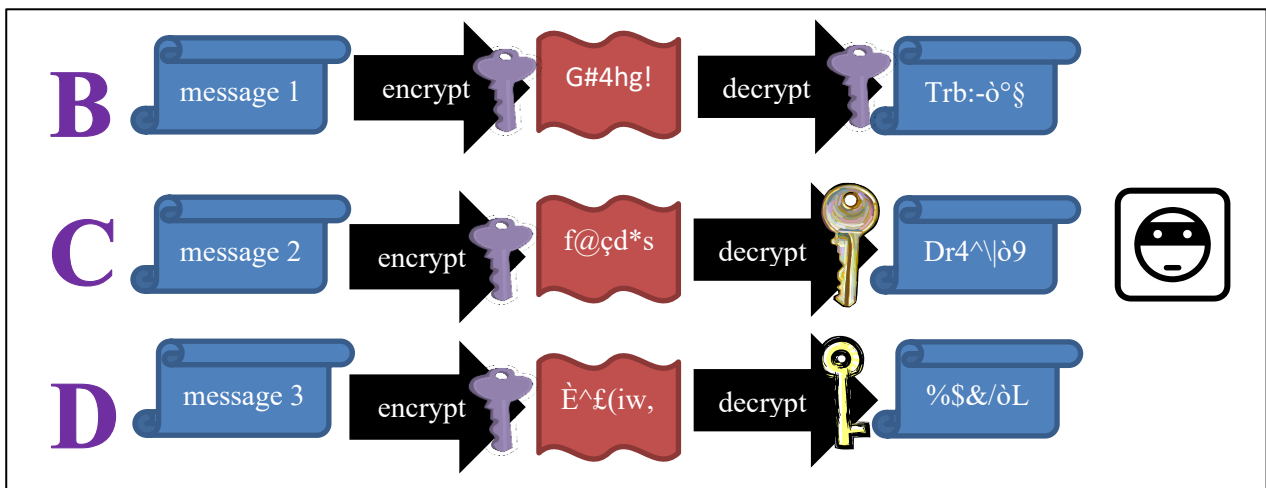
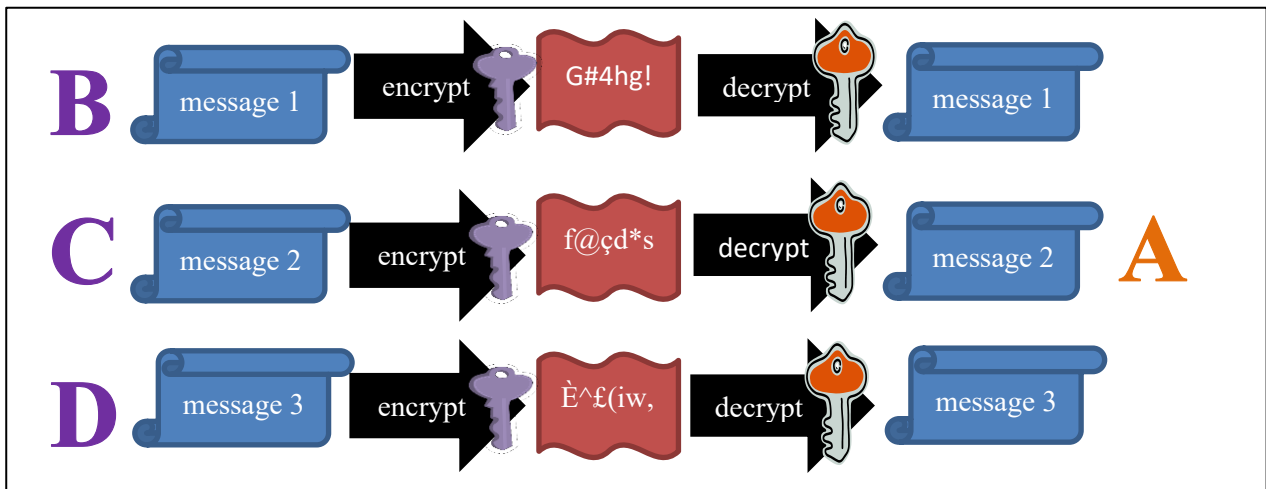
4.1. Cryptography

Cryptography are text masking technologies, derived from military use, which transform information in such a way that it may be correctly read only with a special password called key. They typically use a set of rules to change the text and a parameter to determine how to change it. For example, COMPUTER can be scrambled into FRPSXWHU moving each letter three positions ahead in the alphabet. For practical reasons, the algorithm is usually well-known while the parameter (+3 in this case for encrypting and -3 for decrypting) is kept secret. An algorithm like this one, used since the time of Julius Caesar, suffers from two major drawbacks. The first one is that a computer can easily try all the possible parameter combinations (in this easy example they are only 26) until it finds a readable text. The second one is that someone who knows a key can easily deduce the other one.

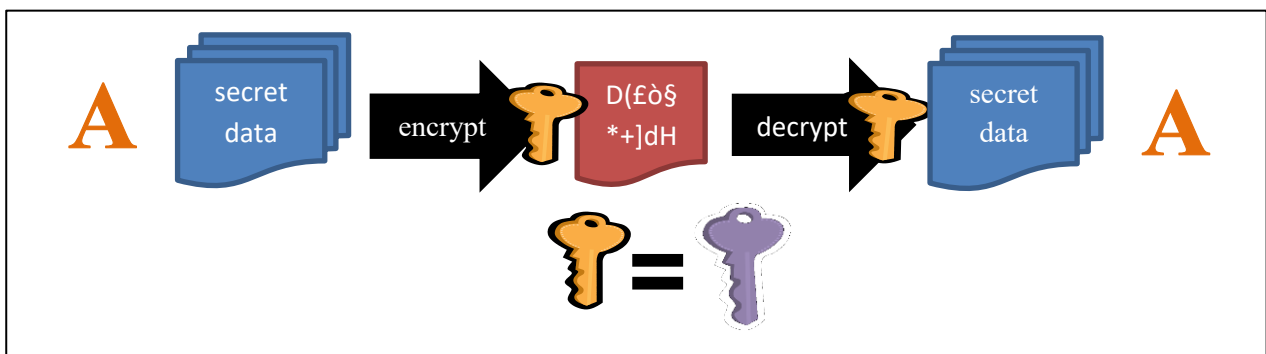
In 1978 Rivest, Shamir and Adleman invented the RSA algorithm, an asymmetric encryption method. It uses two keys, a public key for encrypting, usually known by everybody, and a private key for decrypting, usually known by only one person or organization. Both keys are generated using huge prime numbers and are very hard for computer to be guessed through random attempts.

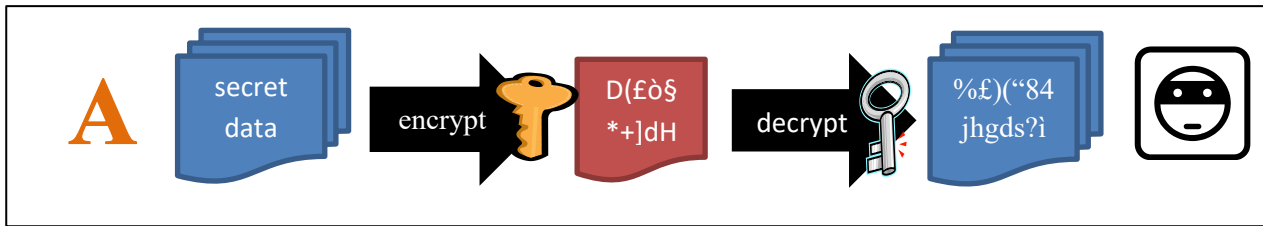
The two following schemas illustrate how B, C and D can send secret information to A using A's public key . The sent messages are encrypted and later decrypted by A with his private key . In case somebody  intercepts a message, he is unable to decrypt it correctly since he does not have A's private key , which is known only to A. If somebody  uses the public key to decrypt, it produces non-sense text.

The same process happens whenever a browser sends a password or secret information to a website using a secure connection (see section 4.5): the website tells the browser its public key and the browser uses it to encrypt information which can be read only by the arriving website.



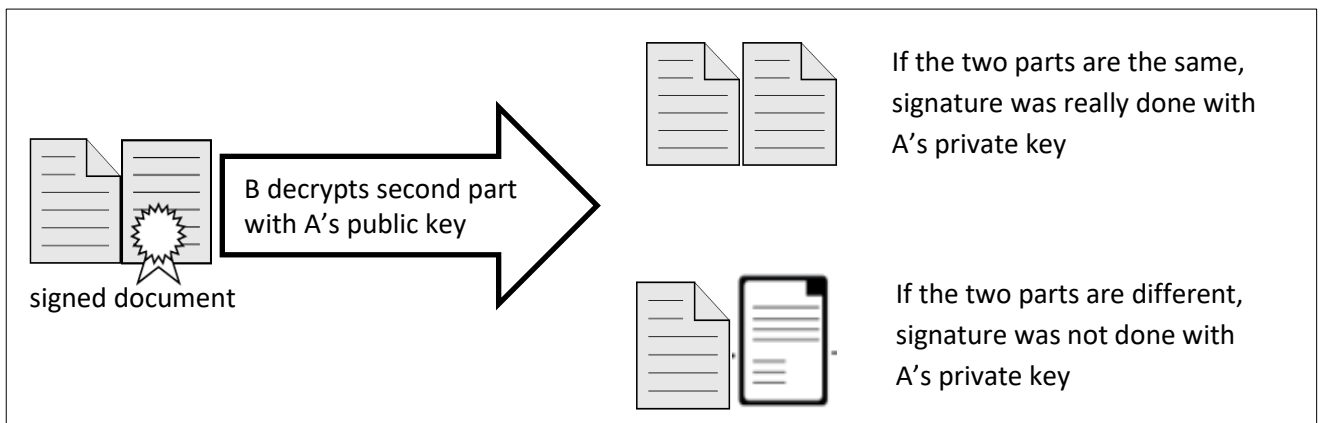
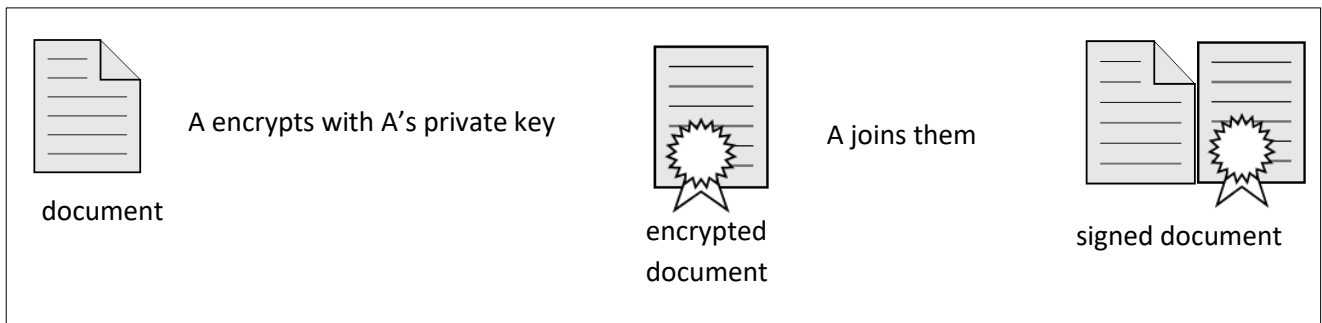
Another analogous usage of cryptography is to make stored data unreadable except by the owner. In this case private and public keys coincides and are kept secret. The encryption and decryption process is done automatically by a program (for example see section 2.3.2) or even by the operating system (if the entire disk is encrypted), which asks the key to the user every time.





4.1.1. Digital signature

A digital signature is a cryptography technique for documents which guarantees, at the same time, the document’s author’s identity and that the document’s content has not been altered. According to Italian law 82/2005, a digital signature is equivalent to a handwritten signature.



These two schemas illustrate the usage of asymmetric cryptography for digital signature. A wants to publish a publicly available document with its signature. First of all, A generates two keys, keeping one of them private and publishing the other, e.g. on his website. A then encrypts his document using his private key and publishes the original document together with the encrypted one. All the users can decrypt the second part using A’s public key. If the result of decryption is identical to the first part of the document, it means that it was really encrypted with A’s private key and thus comes from A. On the other hand, if the result is something else, it means that encryption was not done with A’s private key or that the original document was modified after A’s signature.

Digital signature can be used in combination with PEC to guarantee also sender’s identity and that e-mail’s content was not altered.

While cryptography to receive secret messages or to hide information simply requires the user or the program to create its own couple of private and public keys (programs, for example browsers, do this operation automatically without the user’s intervention), for digital signature it is not so simple. Since everybody must be sure that the public key is really the author’s public key, some government require that official digital signature pass through a certification authority which generates private and public keys. Even

though theoretically a simple password is enough, to be sure that the user does not give the private password around, the certification authority gives him, after having identified him through a governmental identity card, a password usually together with a two-factors identification tool (see section 4.2.2), which, when used together, correspond to his private key. An automatic digital signature program takes care of automatically encrypting documents.

4.1.2. Keys expiration

The major problem of cryptography's keys is that if a computer is put to work trying to encrypt a text with many private keys in sequence and then to decrypt it with the correct public key, within some years it might manage to find the right private key. Therefore, each couple of private-public keys has a time limited duration, usually some years, after which it is necessary to change them and encrypt again all the past documents.

Documents for which it is important to determine the exact date of the signature have moreover a temporal mark signed directly by the certification authority.

4.1.3. Comparison with handwritten signature

	Digital signature	Handwritten signature
Who can sign	Needs keys from certification authority and proper tools	Everybody instantly
Who can verify	Everybody (with proper program)	Handwriting analysts
Verification reliability	Sure for some years	Subjective in dubious cases, no time limit
Temporal duration	Some years (can be renewed)	Until other reliable signatures are available
Mass signatures	Some seconds for all documents	Some seconds per document
Date reliability	Objective if temporal mark	Based on uncertain elements (paper's and ink's age)
Content alteration	No possibility	Words can be added in blank spaces

4.2. Passwords

On most information systems the user is identified only by his username, known to everybody, and his password, known only to him. The password is what makes an unknown person an authenticated user, with all his privileges and his identity's responsibilities. If somebody else uses the user's password, for the information system this other person is exactly the user. It is a very bad idea to give a password to other users, even when it seems to be necessary. These are some, often underestimated, malign actions a passwords' thief can do:

- steal personal information: the thief can read the user's e-mails and personal information;
- steal privacy protected data: the thief can gain access to data about other people protected by privacy, or read e-mails received from other people. The legal responsible of this privacy violation is the thief as well as the user who did not protect other people's data;
- steal money: the thief can find the user's bank account numbers and passwords, sometimes directly from the user's web browser's history;
- delete and modify data: the thief can delete user's important data, or even worse he can modify these data without the user being aware (bank numbers, friend's e-mail addresses, degree thesis content, add illegal pictures);

- steal identity: for the information system the thief is now the user, and therefore he can act to the outside world exactly as if it were the user, for example answering to e-mails, subscribing to websites, withdrawing from exams;
- start illegal activities: anybody who wants to start an illegal Internet activity will obviously use somebody else identity, so he will not get into troubles when the activity is discovered.

Therefore it is absolutely necessary to keep your own passwords secret. Unfortunately, many people use very trivial passwords. This is the list of the most common passwords in 2020: picture1, password, 12345678, senha, qwerty, abc123, Million2.

There exist automatic programs which are able to try 4 billion passwords each second, and they usually start trying combinations of words and numbers (the complete set of all Italian, German and English words can be tried in less than 1 second). Check on <https://howsecureismypassword.net> how much time does it take to one of these programs to discover your easy passwords.



Best practices are:

- change your password often if it deals with important things;
- avoid words related to yourself, such as names, dates, places and addresses;
- use minimum 8 characters.
- use as a password a good mix of numbers, strange characters, small caps and capital letters, avoiding any common word (other people's names or words which can be found in a dictionary);
- use different passwords for different purposes. Unfortunately, every website asks the user to register with a password and users who use always the same password are giving it away to every website they register, even untrustworthy ones. It is a good procedure to have at least three passwords: one for important use (bank account), a second one for everyday use and a last one for unimportant use (registering to unknown websites or to services that will not be used anymore);
- beware of passwords stored on device: mail-readers, browsers, and even your own smartphone store your password masked with asterisks. They seem to be unreadable, but often computer experts can reveal them instantly. Store passwords on device only if it has a single user and if access is restricted, but never on public or shared devices.

Account name:	username
Password:	xxxxxxxx
	<input checked="" type="checkbox"/> Remember password

4.2.1. Remembering passwords

While several years ago it was fine to remember all the password by hearth, in a modern world this is surely impossible. Each website requires a password with different requisites or, even worse, assigns a random password impossible to remember. Users have various techniques to remember passwords. Some are very dangerous, such as writing the password on a file which is kept on the computer hard disk or on the smartphone's memory. Anybody who gains access to the disk or the memory, for example simply opening the stolen computer, can read the file. Other less dangerous strategies are writing the password on a paper handbook, which is very impractical, and sending the password to the user's own e-mail or chat account, leaving them in the trust of the company owning the servers.

One of the best strategies for remembering the passwords and having them easily accessible is storing them in a password manager. It is a program which runs on computers and smartphones which keeps all your

passwords in an encrypted file. The user just need to keep a copy of this file on his cloud space or on any portable device and remember that file's password which will be asked everytime the file is opened.

4.2.2. Alternative password devices

Current technology offers methods to replace the password authentication with personal devices or with biometric identification and some other techniques to add extra security to existing passwords.

To replace the password, biometric identification is considered to be very secure and thus it is used to replace completely the password system. It can be fingerprint recognition, face recognition, iris recognition and voice identification.

For very important activities, such as a digital signature or bank operations, the password is instead coupled with a personal device. This is called two-factors authentication. The usual password is remembered personally by the user and a personal device provides the second part of the password. This device can be a smart card, such as the national health card, which is inserted into a card reader.



Alternatively, the second part of the password can be an OTP One Time Password, generated every time on an app installed on the user's smartphone or through a telephone call from user's mobile phone or sent through a text message or simply activating an app notification on the smartphone.

This big advantage of OTP systems is that, even if both parts of the password are intercepted or guessed, the second part can be used only that time and will expire after a few seconds.

4.3. Viruses

From the WAN many unauthorized connection attempts arrive. Some of these are mistakenly authorized and manage to reach the LAN or at least to come in contact with programs which are behind the firewall (see section 4.6.1). If these connections carry malign intentions, usually their aim is to explore and use the LAN computers, to destroy data or to stop some services (which is a severe attack if these services are managing essential public services). Defense against these kinds of attacks is in charge system administrators.

While ordinary external attacks do not involve users, the virus is a special attack which arrives directly on the user's computer and must be prevented and stopped by him. The virus is a little program which has this name because its life cycle is the same of the biological organism: survive and duplicate.

1. It arrives on the computer through e-mail attachments, downloaded files, CDs, DVDs and USB sticks or directly through your browser. It is often hidden inside other good files or programs, which are called infected. In the last years, many freeware programs deliberately install small advertisement programs without the user's explicit consent; this kind of behaviors is considered borderline between a virus and a way of financing the program's development.
2. As soon as the user mistakenly runs it (often trying to run the good program or to open the good file), the virus orders the computer to run itself every time the computer is turned on, thus assuring its survival.
3. It starts duplicating itself, infecting other files and USB sticks and trying to send itself around by e-mail's attachment or on the Intranet.
4. Most viruses are programmed to do damage to the computer and to the user, altering or deleting files, sending e-mails with user's personal data, preventing firewalls and antiviruses from running or turning the computer off. No viruses are known to be able to damage hardware.

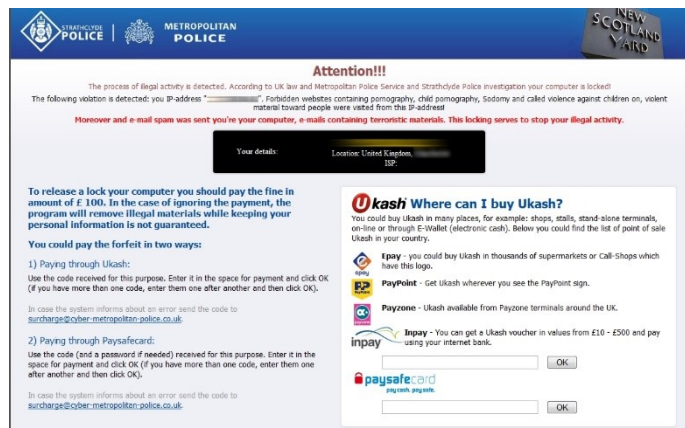
Many names are used for viruses' types according to their different behaviors.

- trojan horse is a virus which looks like a good program and, when downloaded and run by the user, it performs the user's wanted task but at the same time does other actions;
- keylogger is a virus which records keyboard's activity and then sends the keystrokes to its creator, mostly to get user's passwords;
- back door is a virus which opens a port on the computer to let external users in;
- adware is a virus which displays advertisement;
- spyware is a virus which spies user's activity to get passwords or to target the user with specific advertisement;
- ransomware is a virus which makes its presence public and demands to the user money to be removed, threatening to damage him in a variety of ways, such as encrypting files or pretending to be an authority's tool and asking the payment of a fine.

These types are not exclusive: for example a Trojan horse can be at the same time a spyware and an adware.

4.3.1. CryptoLocker/WannaCry

In 2013 a new terrible ransomware trojan virus called CryptoLocker and similar others called WannaCry appeared on the Internet. It arrives usually by e-mail with a double extension, such as document.pdf.exe and with an icon identical to the typical PDF icon. Since many people use operating system without activating extensions (see section 2.3.3), they see a PDF icon and the name document.pdf and open it directly, which for a program means running it (see section 2.3.2). Once run the program starts to encrypt (see section **Error! Reference source not found.**) all the documents on the current hard disk and on all the network hard disks it has access to. The program is soon stopped by an antivirus or by an administrator who discovers that files are starting to be unreadable, but in a few minutes it can encrypt tons of data. At this point the user receives a request for payment of some hundreds USD, through an anonymous pre-paid cash voucher or Bitcoin, to get the decryption key.



It is estimated that 3 million USD were paid in the first 6 months, even though 27 million USD were found entering the creators' bitcoins wallets. This problem was so severe that an international consortium of several police forces started investigations and found the database of decryption keys. However, several other similar viruses are appearing, some of them use a file downloaded from the web to circumvent e-mail protections. Currently, these viruses are very hard to stop as they begin to encrypt very fast as soon as they are clicked.

4.3.2. User's behavior

An infected computer can be recognized by some symptoms. These are the most frequent ones:

- when the computer is turned on, unwanted programs start, advertisements appear and the Desktop presents some new bars or features which were not present nor installed before;
- the computer starts very slowly and unknown programs give strange operating system errors;
- commercial or pornographic web pages appear on the web browser without the user's consent;
- the Task Manager window (see section 2.1.1) presents unknown programs.

Most of the time, a responsible user's behavior is the best weapon against viruses: it protects him from getting viruses, helps him removing them and prevents him from diffusing them. Responsible behavior means:

- never open downloaded files and e-mail attachments, especially when they come from a friend with a text such as "please open it, urgent!", since simulating to be a user's friend is a typical virus' tactic. To open these files, save them on the Desktop, check them with an antivirus and then open them;
- do not insert in your computer CDs, DVDs and USB sticks coming from other people or which were inserted in other computers, unless you have an antivirus running or unless you scan them immediately with an antivirus;
- avoid visiting strange websites, especially pornographic or hackers' website, or websites which open a lot of pop-up windows;
- have an antivirus always running or at least run an updated antivirus on your whole hard disks every week. Keep your antivirus always up to date: more than 50 new viruses appear every week;
- keep communication programs and the operating system up to date. Almost all software companies offer free updates and automatic updating tools;
- beware of freeware programs which often try to install adware programs, asking the permission very quickly during installation's steps, relying on the novice user's habit of clicking always "yes".

To check the computer for viruses and to try to remove viruses from the computer, the user can run a special program called antivirus. The antivirus basically has three possible different actions:

- it can scan all the storage devices (hard disks, USB sticks, the CD or DVD inside the reader) for viruses. If a virus is found, it tries to remove it and to repair damaged files. Some files can be unrecoverable. Complete devices scanning takes usually some hours;
- it can scan a single file or an entire directory for viruses. If there is an infected file, it tries to delete the virus and repair it. Some files can be unrecoverable. Single file scanning takes some seconds;
- it can be always running. In this case, whenever a virus or a suspect file is run, the antivirus prevents it from running and warns the user.

A lot of antivirus programs, freeware and commercial, exist. Their most important feature is obviously the possibility to be constantly updated through the Internet.

4.4. E-mails

4.4.1. Attachments

For viruses, e-mail attachments are a first class way of traveling, since they are very often opened by users without any precaution. Sometimes viruses hide inside files which were really sent by the sender, unaware of having an infected computer. Other times a virus takes control of the mail reader program and sends itself to the whole address book, counterfeiting the sender address (often using an address taken from the address book) in order to avoid that the real infected computer be identified and to gain the trust of the receiver, and writing in the e-mail text smart sentences pretending to be a regular friend of the receiver. The arrival of this kind of e-mail usually creates havoc, since the receiver is sure that the fake sender has a virus, while the original infected computer is another one.

The basic rule is never open any attachment directly from the mail reader program. Save the attached files on the Desktop and run an antivirus program to check these files before opening them. This applied even when the e-mail comes from a friend: he cannot know that to have got a virus or he can not be the real sender.

4.4.2. Spam

Spam messages are unsolicited unwanted bulk e-mails. They are unsolicited, meaning that the user did not ask to receive them, they are unwanted, meaning that the user did not want to receive them, and they are bulk, meaning that they are sent to millions of addresses. They are used mainly for four different purposes:

- advertisement e-mails are the most innocuous version. The e-mail message contains commercial information usually on gambling, medicines, pornography, software or investments. Sometimes these messages are purposely written with orthographic mistakes or with strange characters, to avoid being intercepted by antis spam programs;
- frauds are usually long letters proposing the user a semi-legal bargain or a big lottery prize. Their only aims are to get the user's bank coordinates for further illicit activities and to lure him into paying small expenses hoping to get the promised imaginary money;
- phishing e-mails look as completely plausible e-mails from a bank, a credit cards issuer or financial website, asking the user to enter their website to perform some urgent actions. They often carry real logos, seem to address to the correct website and even cite the real website's anti-phishing campaign! However, this website address is a trap, and the user will be sent to a false website, who looks exactly like the original one, whose only scope is to get passwords or credit card numbers. Phishing has become a big problem for Internet banking system, and the user's best defenses are entering any crucial website always typing the address directly in the web browser without clicking on addresses contained in e-mails. Call immediately his own bank at the telephone whenever believing of having been a victim of phishing.

Da: Gralnick
Data: martedì 21 febbraio 2006 12.59
A: aditn@ing.unitn.it
Oggetto: ATI-Network: probabile SPAM *** Best love dr@gs at best store!

Hot Weekly Specials			
1	Cialis	\$89	BUY NOW
2	Viagra	\$69	BUY NOW
3	Valium	\$99	BUY NOW

World Wide Shipping Save Up to 80%
 Discreet Shipping
 Complete Order Tracking
 Best Pricing
 World Wide Shipping

Da: miccam@marfino.net
Data: venerdì 24 febbraio 2006 13.55
A: miccam@marfino.net
Oggetto: Equity in Friendship

Phone: +234 802 554 9993
 reply to adioms@marfino.net

I am the chairman of the contract award committee of the National Petroleum Corporation here in Nigerian, for security reasons, I may not wish to disclose how I got your email address for now.

After due deliberation with my partner, I decided to forward to you this business proposal, we want you to assist us receive the sum of Twenty eight million, six hundred thousand united state bills(us28.6m) into your account. This fund resulted from an over-invoiced contract awarded by us under the budget allocation to my ministry and the bill was approved for payment by the concerned ministries. The contract was executed, commissioned and the contractor was paid his actual cost of the contract. Now, we are left with the balance of us28.6m as the over invoiced amount, which we have deliberately over estimated for our own use. Please note that the law forbids civil servants to operate or own foreign accounts hence this contact, we have agreed to share the money in the following percentages: 30 for you, 60 for us 10 for tax as may be required by your government.

Note that this transaction is very much free from all sorts of risk hence the business was carefully planned before it was successfully executed and we the officials involved in the deal have put many years in service to our ministry. We have been exercising patience for this privilege for so long

The best behavior to adopt against spam messages is to ignore them. Complaining is worthless since their sender address is always false; clicking on their links, especially if they suggest clicking there to be removed from their lists, usually has the only effect of letting the spammer know that the user's address is really read by someone.

The best ways to defend from spammers are to avoid using the user's main e-mail address during registration in forums and unimportant websites, and to avoid publishing it on the personal or the company's website.

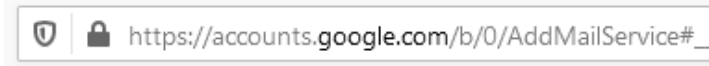
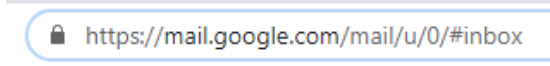
These are the places where spammers get their millions of addresses. If it is really necessary, a good strategy is to have an alternative e-mail address for registrations, which will receive all the spam.

There are antispam programs, which put the supposed spam messages in a separate junk e-mail folder, but they are not completely reliable and sometimes they trash even good messages. These programs rely on analysis of the e-mail's content and on blacklists, which contains the Internet mail-servers which are supposed to let spammers send their e-mails; it may happen that a good mail-server ends up into those blacklists and that e-mails send from customers or employees of that Internet site are marked as spam by other sites.

4.5. Navigation

Navigation is the second most dangerous Internet activity. It has more or less the same dangers as e-mails: the user's computer can get viruses if he does not run an antivirus before opening downloaded files, and the user can be lured into phishing websites if he does not type personally the bank's address in the web browser. Moreover, the computer can get viruses even when simply visiting some websites, and therefore two good suggestions are to avoid visiting strange (pornographic websites, websites with a lot of pop-up windows and illegal websites) or untrustworthy websites and to keep browser and operating system always up to date.

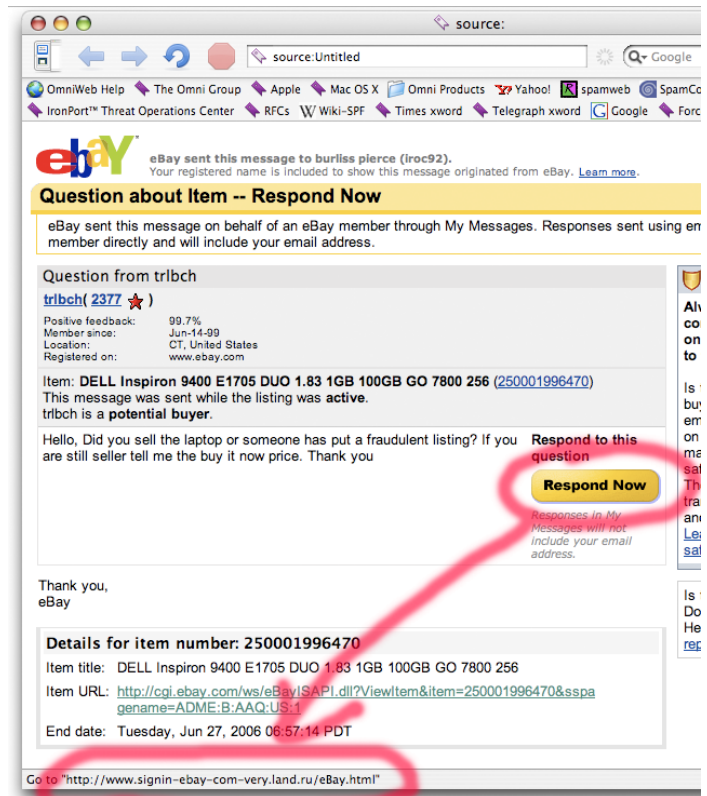
The other security problem while navigating is data interception. When connecting to a website, the user's data travels long distances, passing through a large number of computers (to connect from unibz.it to www.athesia.it the data go to Padua, Milan and Bologna passing through at least 13 computers). Data on the Internet travel without any protection, any computer administrator can read them. Therefore, when sending passwords and other private data to a website, the user should take special care that the address in the address bar starts with https:// (instead of http://) and that a closed lock symbol appears in the bar: these



indications mean that the connection is secure (SSL Secure Socket Layer) since data are traveling encrypted. Beware that the SSL connection guarantees only that data are not intercepted and that the user is connected to the same website from which he started the connection, while it does not guarantee this website is the right one.

4.5.1. Fake news

Even though not a direct attack, fake news can be considered as a plague of modern WWW.



Initially they originated by misbeliefs or superstitions which spread on the web using the fact many social network users trust the people they are connected with, without checking the source, and thus propagate wrong news. At this point fake news were just a form of nuisance.

Unfortunately, recently, fake news have found a way to be a source of profit, exactly the same that happened for spam when phishing was invented. Several web sites deliberately distribute fake news in order to attract visitors to their site and, in particular, to their advertisement banners which represent their main income. Therefore, forwarding a news which appear on a social network without checking personally whether its source is correct or, at least, whether there are some other people who have already proven it as a fake news, is a very good way to feed these misinformation sites.

NEWS ECONOMY ENTERTAINMENT HEALTH PEOPLE SCIENCE SOCIETY SPORTS WEIRD

HOT TOPICS AUGUST 5, 2019 | LOTTERY WINNER BUYS HIS FORMER WORKPLACE AND FORCES HIS FORMER BOSS TO WEAR MASCOT

For

22 P
FOOD

NEW JERSEY BROTHER AND SISTER ALLOWED TO MARRY AFTER 10-YEAR-LONG COURT BATTLE

A New Jersey brother and sister have won the right to marry after a landmark ruling by the Supreme Court of the United States. In...

READ MORE

4.6. Attacks from outside

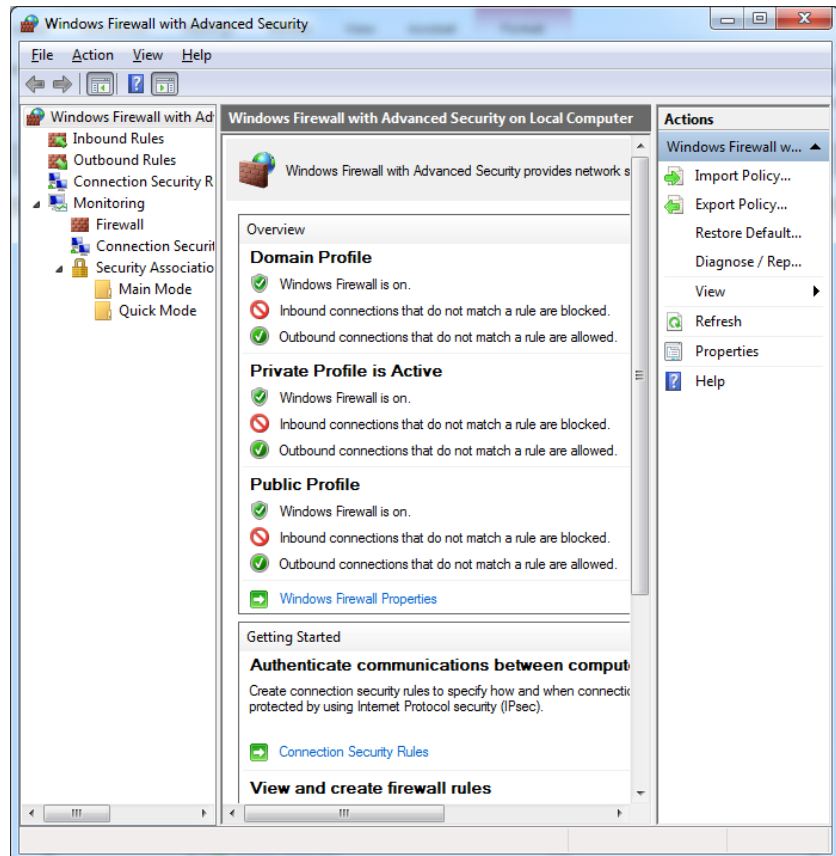
Any computer attached to the Internet, even from inside a LAN, is subject to attacks from the outside WAN. The typical attack consists of external computers trying to gain access to the computer using the operating system's known problems or hoping that the user is currently running programs which open computer's ports to outside connections. From the user's side, the best defense is keeping the programs always up-to-date, especially the operating system and communication programs.

The most famous attack from outside, and the one from which it is very difficult to have an appropriate defense, is the DDoS Distributed Denial of Service attack. It is an attack which does not strike private users, but organizations offering services over the Internet. It consists of sending millions of incoming connections which pretend to use the service but stay simply connected, in such a way to overcrowd the server and drain all its resources (bandwidth, speed, memory) until the server crashes. The attacker clearly does not use his own computer to carry on a DDoS attack, otherwise his computer would probably crash well before the server, but uses computers of unaware users around the world, called zombies, which have been hacked in the past days. In this way, the attacker has the power of several hundreds computers connected from many different parts of the world and, at the same time, it is difficult to trace the responsibility up to him.

4.6.1. Firewall

Often programs' security problems once discovered need some days to be fixed and somebody can take benefit of them in this short time, before the security update is installed on the user's computer. Therefore on every LAN, usually in the point where the LAN connects to the Internet, or more often on every computer a special program called firewall is running. The firewall examines all the incoming and outgoing traffic, using the following analysis techniques:

- which internal program is originating/receiving the traffic,
- from/to which external address is the traffic originated/directed,
- what amount of traffic is passing from/to the same program to/from the same external address,
- which kind of data are passing.



Making an analysis of these data clearly slows down the connection but lets the firewall stop potentially unauthorized connection.

Windows operating system comes with a firewall preinstalled, which lets the user customize which programs are allowed to make or receive connections and determine rules to approve or deny automatically connections.

4.7. Backup

Backup is the process of copying important data to another location to prevent their loss. There are three very good reasons to do regular backups:

- against the user, who can accidentally delete some files or who can modify files and then change his mind. Having a recent backup handy can often save hours of work;
- against the system, which can suddenly break due to hardware or software problems. Hard disks tend to become unreliable after some years of continuous activity. A recent backup saves the user from redoing all the work of the previous months;
- against viruses and other users, which can delete and alter files.

Usually, the operating system's and the programs' backup are done by system administrators, even though for the personal computer it is a good practice keeping a backup of all the non-freeware programs. However, there are some files which should be taken in charge by the user himself:

- personally created data files, including all documents, images and videos created by the user and any other file which is a result of the user’s personal work. An often forgotten thing are pictures and videos from your own smartphone;
- in case these are not handled by an online system: the contacts, calendar and the e-mails;
- some programs require a lot of configuration and store their configuration in configuration files, which are usually in the program’s directory;
- all the stuff which is difficult to find again, such as documents from other people or downloaded from forgotten websites.

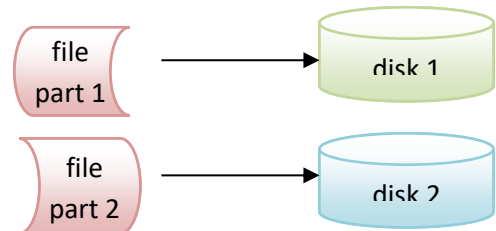
The place where the files are copied determines the reliability of the backup. It should be a large, cheap and fast storage device. It should also be handy, since the typical problem with backup is that the user does not take the time to do it regularly and, when the backup is too old, it is worthless. For home or simple office users, the Friday morning backup is a good timing solution. Good storage devices to be used are:

- a second hard disk, used only for backup, which is very fast and very large and always ready to be used;
- online backup systems, where user’s data are uploaded and are ready from anywhere in the world, such as Dropbox, Google Drive, Microsoft OneDrive, iCloud, Box and Amazon Drive which offer some GB of space for free;
- USB stick, to be used only in emergency when no other appropriate storage device is available;
- big companies usually have special tape devices for backups.

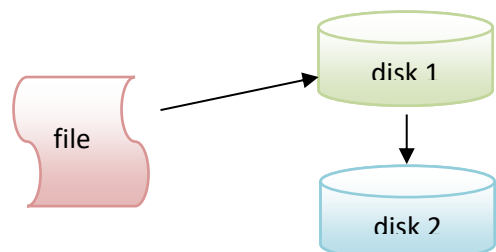
4.7.1. RAID

A very popular backup solution is RAID (Redundant Array of Independent Disks) technology, which consists of several identical hard disks. There are different types of RAID implementations, which vary a lot in functionalities and security.

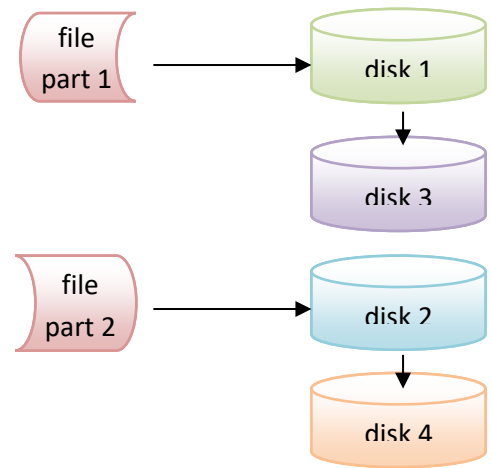
RAID0 uses two identical disks which are seen by the user as a single disk. Every time he writes a file, the first part of the file is written on the first disk while the second on the second disk. This strategy has the big advantage that writing speed doubles, with a total available space equal to the sum of the size of the two disks. But if a disk breaks, all the content of both disks is lost, since the user will lose half of all the files and half file is worthless.



RAID1 is the most common implementation of RAID. It uses two identical disks but the user sees only the first one. The second disk is simply an identical and instantaneous copy of the first one. The disadvantage is that the speed does not improve and the available space has the size of one disk only, but in case a disk breaks, no file is lost since the other one is its identical copy. This is a very good backup solution to protect data against physical failure, especially suited for 24h services. However, it is not a backup solution against viruses or user’s incidental cancellations, since any modification on the first disk is immediately replicated on the second one.



RAID10 is an overlay of RAID1 and RAID0. It uses four identical disks writing files on the first and on the third as if they were on RAID0 and then duplicating their content on disks two and four. This technique has the speed of RAID0, the reliability of RAID1, but gives the user a space equivalent to the sum of two disks sizes, while four disks are effectively used.



All the RAID techniques are good at either improving the speed or improving the reliability against hardware failure, but are not good against other threats and therefore they must always be coupled with another form of backup, such as daily copy of data.