



# DIGITAL SURVIVAL

Essential Information for Getting Started with  
Computers, the Internet and Mobile Phones



# Table of contents

Introduction	3
<b>Chapter 1 The Computer</b>	<b>5</b>
Introduction	5
Protecting the health of your computer	6
Computer hardware	11
Operating systems	13
Connecting peripheral devices	15
File management	19
Software applications	24
Keeping your computer and data safe	29
Computer viruses	35
Internet café security checklist	39
<b>Chapter 2 The Internet</b>	<b>47</b>
Introduction	47
Connecting	49
Browsing Web-pages	55
Searching Web-pages	59
Working Online	61
Engaging Communities Online	63
Establishing a web-site	65
Keeping track of web-pages	66
Using email	67
Real-time messaging	73
Online Voice-Calls	74
<b>Chapter 3 The Mobile Phone</b>	<b>77</b>
Introduction	77
How mobile phones work	78
Creating and sharing content using mobile phones	80
Choosing a mobile phone	82
Connecting to your Computer	87
Making the most of your mobile phone's multimedia capabilities	88
Travelling with your mobile phone	93
Mobile security & privacy	95

# Digital Survival

Essential Information for Getting Started With Computers,  
Internet and Mobile Phones

## Introduction

To survive in the digital age, with constantly changing technologies, it's important to learn the basics of how things work.

For this guide we have organised information about the three most widely used digital technologies: 'The computer', 'The internet' and 'The mobile phone'. We aim to explain the essentials of these technologies to make them accessible and easy to understand. We have also highlighted security issues. The more you use digital technologies, the more vulnerable you become and it's important to understand the risks.

There's no need to read the entire guide cover to cover, you can scan the chapter titles and go to whatever topic you'd like to, or need to, learn more about. This also means that you can use it as a reference and come back to it whenever you want to learn more.



# 1

# The Computer



## Introduction

Computers are complicated. There's no getting around it. And they were designed by people who find their inner workings – circuits, wires and coding – utterly fascinating. This means that sometimes computers are not well-designed for people who just want to turn them on and use them to do tasks. Nevertheless, computers have become much more user-friendly over the last decade, and this chapter will help you understand and use them even better.

After reading this chapter, you should understand:

- How to keep your computer healthy and running smoothly
- The different components that make the computer work
- How to connect devices to your computer
- The varieties and types of software applications
- How to protect your computer and its data

# Protecting the health of your computer



If you use a computer you know how challenging it is to keep it running smoothly, avoiding crashes or loss of processing speed. Inevitably though, problems arise: systems develop bugs, software becomes corrupted – your computer may even come down with a virus! The following points will help you keep your computer and data in good condition and working smoothly.

- ❑ Never cut off the power supply to your computer without shutting down the system first. If you shut your computer down properly every time, your software is less likely to become corrupted.
- ❑ Install an anti-virus programme. Make sure it will automatically scan your files, and make sure it updates itself at least once a week. This is particularly important for Microsoft Windows users.

- ❑ Back up your system at least once a week. It's not a question of if you will have a system or hard-disk failure, but of when it will happen. If you aren't prepared, then you are very likely to lose some or all of your valuable files.
- ❑ Avoid software copies and pirated software.
- ❑ If you have a broadband internet connection, update your software regularly, because developers are making improvements all the time. Most applications will alert you when updates become available on the internet and you can then choose to install them.
- ❑ Remove software applications you no longer use. Uninstall and remove the programme files.
- ❑ Don't install too much software on your computer, as it can slow your system down and cause problems.
- ❑ Don't let your hard drive get more than 75% full or your computer will slow down.
- ❑ Keep your desktop folder as clean and empty as possible. Desktop clutter contributes to slowing your computer down.
- ❑ When in doubt, restart your computer. A simple restart can solve many problems. Always restart your computer before attempting any complicated trouble-shooting.
- ❑ If you have more than one person using a computer regularly, consider setting up separate accounts for each user.

## Tips for Windows OS Users

Windows OS users should regularly do the following:

### 1. Disk clean-up

There are probably plenty of files on your computer which you don't need. These can slow down your operating system. To clean up your Hard Disk Drive (HDD), you should:

- Uninstall applications – and delete the programme files – that you don't use any more.
- Regularly check the Temporary Files (tmp) folder (you can find this in your C drive), and delete any unnecessary files.

### 2. Disk error checking

From time to time the hard drive of your computer may malfunction; for example, if a virus attacks your computer, or if you don't close down an application properly. Usually, the application 'Scandisk' will already be installed on your Windows OS computer. You should run it periodically. If you have recently bought the computer, it will probably be running Windows Vista and in this case disk checking requires a bit more work:

- 1 Go to 'Start', then 'Computer'
- 2 Right click on the hard disk drive icon, and then on 'Properties'
- 3 A new window opens up. Click on the 'Tools' tab
- 4 Under 'Error Checking', click 'Check Now'

Remember: Before you run a disk error check, you must first close all other applications.



### 3. Disk defragmenting

Disk defragmenting is like tidying up a messy cupboard so that you can find what you want quickly. It involves moving all the computer files around to create order on your hard disk.

Afterwards, files will load on your computer much more quickly than before.

To do this, you can use Windows Disk Defragmenter (Start → programmes → Accessories → System Tools → Disk Defragmenter).

In Windows Vista follow steps 1–3 from Disk error checking (above) and then click on ‘Defragmentation’ below ‘Error Checking’.

## FAQs

Why does my computer slow down sometimes?

The most likely reason is that there are too many applications and programmes running at the same time. Usually closing down a few applications will speed things up. You may have unseen programmes, such as anti-virus software, running in the background. Check your system tray (in Windows, this is in the lower left-hand corner) to see if you have any programmes running in the background. A slow computer may also be infected with a computer virus.

Why does my computer screen go off while I’m working?

This is more likely to happen on a laptop but is still possible on a desktop computer. It’s largely due to your energy-saving settings. Change your ‘System standby’ setting, under ‘Power options’ in the Windows Control Panel, to ‘Never’ if this is an problem.



# Computer hardware

This is what you would see if you opened up a computer.



What's inside a computer:

- ❑ Central Processing Unit (CPU): the 'brain' of your computer. The CPU performs calculations and tasks that make programmes work. The faster the CPU, the quicker the computer's performance.
- ❑ Random Access Memory (RAM): RAM can be understood as the computer's 'memory'. It stores information that is needed quickly by the programmes and applications running on your computer. More memory lets you run more applications at the same time without slowing down your computer.

- ❑ Hard Disk Drive (HDD): all your main data, including your operating system, your software programmes and your personal files, is stored on the computer's HDD. A typical HDD is only slightly larger than your hand but it can hold over 100 GB of data. The larger the hard disk, the more information you can fit on the drive.
- ❑ Video Card: the video card helps the CPU to process and display graphics. Most computers have built-in video cards which are adequate for day-to-day use.
- ❑ Sound Card: like a video card, the sound card helps the CPU to process sound. Most sound cards give you the power to plug in speakers and a microphone in order to play music, watch videos or have voice chats. As with video cards, many computers come with sound cards already installed; you only need to buy one separately if you need better sound quality for your work.
- ❑ Motherboard: everything is connected through the Motherboard. It acts as a circuit board bringing all the different parts of the computer together.
- ❑ Optical drive: for playing and writing CDs and DVDs. These are becoming less common, particularly in laptops.

To learn more about how your computer works, see:

How Stuff Works: How PCs Work:

<http://www.howstuffworks.com/pc.htm>

# Operating systems

Your operating system (OS) is an essential part of your computer – it controls the most basic running of your hardware. It allocates memory, performs tasks and acts as the interface for the applications you use. Without an OS, software applications will not work and your hardware is basically useless. The most common operating systems are Microsoft Windows, MacOS, and Linux. Generally any OS is compatible with any computer, with the exception of MacOS, which can only be used on a Macintosh computer.

It is more than likely that when you bought your computer the operating system was already installed, and it was probably Windows, although Ubuntu Linux is also gaining in popularity. In order to ensure that the applications you want to use on your computer are compatible with its operating system, you need to know what OS your computer is running. If you are only using a computer for web-browsing, email and creating text documents you needn't worry too much, because all operating systems come with programmes that will allow you to do these things. However, if there are programmes and applications that you prefer to use, you should make sure that they will run on the operating system that comes with your computer.

It's important to keep up with updates to your operating system. It is inevitable that some of the software coding that makes the operating system work will contain undiscovered errors, and it is likely that some of these errors could undermine your computer's security. Software developers continue to find these errors and periodically release updates to fix them. It is therefore essential that you frequently update all of the software on your computer, including the operating system.

If Windows is not updating itself automatically, you can configure it to do so by clicking the 'Start' menu, selecting 'All programmes' and clicking 'Windows Update'.

If you ever need to do an actual upgrade to a newer version of your operating system, there are two things to keep in mind:

- 1 Will the software you've already got installed on the computer be compatible with the new version of the OS? Most developers will release new versions of their software that are compatible with new versions of operating systems, but often they are not ready until after the new OS is released.
- 2 Will your computer meet the system requirements of the upgrade? Every new OS version requires greater hardware capacity and will be designed to take advantage of the latest components. Always check the system requirements for the upgraded OS and if your computer doesn't meet them, don't upgrade.

## Connecting peripheral devices




You've probably noticed that there are a few ports on the body of your computer – these enable you to connect other devices to your computer, to help you with various tasks, from storage to printing. Some of the most common peripheral devices that can be connected to the computer are:

- Keyboard
- Mouse
- Printer
- Scanner
- Digital Camera
- USB Flash Drive

Today most peripherals, like the keyboard, scanner and printer, connect to your computer via external USB ports.

Some of your peripherals will need special software, which you install on your computer so that your operating system will be able to communicate with and send instructions to the device. These sorts of software are called drivers and you should receive instructions on how to install the driver when you acquire the peripheral. These are often contained in the 'Quick Start' guide.



Universal Serial Bus (USB). On your computer the USB port is marked with a little logo like this  and the USB plug is a squarish flat piece which fits into the port. After you have finished using a USB device, you need to eject it from the 'Remove Hardware' option on your computer.



## FAQs

Why doesn't my printer work?

If your printer was working and then inexplicably stopped, the first thing to do is to check your cable connections. If you are still experiencing the problem, and you are running Windows, it's quite possible that the driver for the printer has become corrupted: uninstall your printer driver and reinstall it. If you are receiving specific error messages when attempting to print, you can also do a search on the internet using the error message and printer model name and number (e.g. Deskjet 2000i); you will probably find instructions on how to rectify the problem.

What's the difference between a Megabyte and a Gigabyte and why should I care?

Computer data is measured in bytes. A byte is one unit of digital information.

1 kilobyte (KB) = 1000 bytes

1 megabyte (MB) = 1000 kilobytes

1 gigabyte (GB) = 1000 megabytes

1 terabyte (TB) = 1000 gigabytes or  
1,000,000,000,000 bytes

If you are trying to determine the capacity of any storage device, these terms are quite important to understand. Any external storage device or hard drive should be measured in Gigabytes, or, if they are very big, in Terabytes. Anything smaller than a gigabyte is now considered quite small. The same applies to RAM.



# File management

File organisation is very important and learning how files are currently organised on your computer can save you time when you are looking for specific files.

As your hard drive acts like a digital filing cabinet, your computer files are the digital equivalent of paper documents. Computer files are organised in computer folders. Each folder can also contain any number of sub-folders.

Your operating system will have a tool built in to browse through your files and folders and keep them organised. In Windows, this will usually be done via an icon called 'My Computer'; in Ubuntu Linux it will be called 'File Browser'; in MAC OS X you would use the 'Finder'. The most common method for moving and organising your files and folders is known as 'drag and drop'. This means you use your mouse to select a file and then drag it into a folder.

## Tip – how to drag and drop:

- With your mouse navigate over the file and click and hold down the right button on your mouse.
- Keeping the mouse button held down, move (drag) the file to a folder in your browser (you can use two browser windows if necessary).
- Drop the file in the folder by releasing the mouse.
- For multiple selections hold down the 'ctrl' key on your keyboard while clicking with the mouse button. Hold down the shift key to group more than one adjacent file and drag them all together.

You can also open a file directly from the file browser by double clicking on it. This will first open the required application; for example, Microsoft Word or Open Office, and then the file will open in that application. The computer selects the correct application via the file extension, which is the three letter abbreviation that comes after a full stop in the file name; for example, if the file is called 'mystory.doc', then '.doc' is the file extension, which tells your operating system that this file needs Microsoft Word to open.

For more information on file management:

<http://www.uwec.edu/BITS/filemanagement.htm>

## FAQs

I just saved a file and want to copy it to my USB drive but I can't find it when I browse for it in 'My Computer'. Where is it?

The very first time you save a file, the application will open up a dialogue box (usually called 'Save As') that will ask you if you want to 'Save in' a particular folder. It's important to pay attention to which folder this is. Often applications have a default folder that they will save to; for instance, Word will save automatically in 'My Documents'. If in doubt, click on 'Save As' and this will show you the folder where your file is being saved. You can then browse to the folder via 'My Computer'.

Alternatively, you can always use your operating system's "search" or "find" functions.

What is the difference between 'My Computer' and 'My Documents' (in Windows)... or my 'hard drive' and my 'Home' folder? (on Linux and Mac OS X)

Your operating system will create a hierarchy of folders and files when it is installed on your hard disk. In Windows, the top-level, most comprehensive folder can be found as the C:\ Drive when you open 'My Computer'. In it, you will find the system folders

and the programme files . Other operating systems will call this location the hard drive. On Windows, 'My documents' holds all the files and folders that you will personally create. Putting all your personal files and sub-folders within one folder makes it very easy for you to back up your files or move them to another computer. On other operating systems, such as Linux or Mac, this location may be called your 'Home' folder.

How can I create shortcuts to the files I use most often?

Clicking on 'My Computer' in Windows allows you to browse through the folder hierarchies and find the file you need. If you click on the file with your right mouse button you will see an option to 'create shortcut' in the drop down menu. After you click on 'create shortcut', a new highlighted icon will appear with a small arrow on it to indicate that it is a shortcut. This icon can be dragged anywhere you would like (most people put them on their desk top). Then you just click on the newly created icon when you want to open that file.

Where are my actual music files located?

Most music files are organised and stored by your music player in a folder, in your Home folder, called something like 'Music'. This can be confusing because most music players, such as iTunes, allow you to browse through and play your music within something called a 'Library'. Most music players are designed to prevent the copying of music files and so you can't actually copy the music file from the 'Library' itself. You have to find the music file using your file browser rather than your music player.

How can I transfer files from one computer to another?

The easiest and most popular way of transferring files from one computer to another is with a removable storage device;

- USB Flash drive: also known as flash stick, pen drive and USB stick. These terms all refer to the same thing: a small thumb-

sized drive that you attach to your computer via its USB port. They have replaced the old floppy disks.

- ☐ External hard drive: computers are made with an internal hard drive but if this gets full or if you have a lot of information you want to back up (especially sound and video files, as they take up a lot of space), you can temporarily or permanently add another, external hard drive. These, like the flash drive, connect to your computer via USB. They come with different amounts of memory (although all in gigabytes, or 'gigs'). Some are designed to be portable.

USB drives can be helpful if you use internet cafés – you can write your emails on a home (or other trusted) computer, load them onto the USB drive, send them from the computer in the café, and then use the same device to store emails you've received. USB drives even allow you to run the software applications you use at home on the internet café computer. See section 2.4.6: Portable Applications.

#### TIP

Be careful when using USB drives or external hard drives; it's very easy to transfer viruses along with files. Make sure your anti-virus programme is configured to automatically scan any device attached to your computer.

How do I back up my files?

Backing up is incredibly important. Try to designate one day a week where you make copies of all of your files and store them on an external source such as a flash drive, external drive, CD-R or DVD-R disc. The easiest way to do this is simply to copy your 'User' folder. In Windows this is the folder, found in 'Documents and Settings', that carries your user name.

The free programme Cobian for Windows can help you back up all your files at once and store them together. One handy thing about using a programme like Cobian is that it will allow you to do an 'incremental' back-up. This means that only new and recently modified files will be saved afresh, and not files which haven't changed since the last time you ran your back-up. To find out more about this option and how to install it, look at [http://security.ngoinabox.org/cobian\\_main](http://security.ngoinabox.org/cobian_main)

# Software applications



Software applications are designed to help you perform a particular task. Typical examples of this are ‘word processors’, such as Microsoft Word or OpenOffice Writer, ‘email clients’ such as Outlook or Thunderbird, and ‘photo editors’ such as Adobe Photoshop or GIMP. Essentially software can be classed in two categories: either Free and Open Source (FOSS) or Proprietary. The most important difference between the two, for our purposes, is legality. It is illegal to copy proprietary software, while FOSS software can be copied freely and legally.

Some examples of proprietary software:

Adobe Photoshop

Microsoft Office



Internet Explorer

iTunes

Some examples of FOSS software:

Firefox – web-browser that is considered to be very stable and secure.

GIMP – a Graphics Image Manipulation Programme that is an alternative to Photoshop.

OpenOffice – a suite of programmes which includes a text editor, spreadsheets, presentation software and database.

VLC – a media player

Be very wary about installing ‘shareware’ or ‘freeware’. These are small applications that are available via the internet. They have the potential to clutter up your system, and may also change your system without warning. These applications are often referred to as ‘Malware’ because of the damage they can do.

Things to remember about any software before installing it:

Is it legal?

Is it from a trusted source? Will it harm your system?

Do you really need it, or will it just clutter up your computer?



### TIP - Portable Applications

There are some computer software programmes which can be installed onto a USB drive and then run from different computers. This is useful if you are moving from one computer to another.

PortableApps is an entire office suite of different applications which you can run from your USB drive on any Windows computer. Think of it as having your own computer (in the form of a USB drive) with you all the time, even when you use public computers.

The list of portable applications is growing daily. Some of the Portable Apps currently available are:

- Thunderbird (email)
- Firefox (internet browser)

☐ VLC media player

☐ GIMP (image and photo editor)

See the PortableApps website for the full list of what is available, and take your software on the move with you! <http://portableapps.com/>

## FAQs

If I am using pirated software, are there any steps I can take to protect myself?

The short answer is no. If possible, you should only use legal software. Pirated software is not uncommon and in quite a few places it's easier to obtain than legal versions of proprietary software. Pirated software is often compromised and may include hacks, viruses and other malware; this makes your data extremely vulnerable to security breaches. With pirated software you do not have any access to support or updates. What's more, the authorities in a growing number of countries have begun to verify that organisations possess a valid license for each piece of software that they use. Police have confiscated computers and closed down organisations on the basis of 'software piracy'. The best way to make sure you are not at risk of data vulnerabilities or legal measures is to use Free and Open Source software.

Where can I find computer software products?

There is a lot of software out there and sometimes it can be hard to choose an application to suit the job at hand. You can learn more about proprietary software on websites such as Microsoft.com and Adobe.com. For Open Source software, there are the websites of the main software releases, such as OpenOffice.org, GIMP.org and Mozilla.com (for Firefox and Thunderbird). A repository of Open Source software can be found at Sourceforge.net. Tactical Tech has several toolkits available,

which include Open Source Software tools selected by a team of international experts and designed to meet the needs of NGOs, human rights advocates, independent journalists and community organisations. See <http://www.tacticaltech.org/toolkits>

How can I set my application to automatically save the document I am working on?

Most office suites, such as Microsoft Office and OpenOffice, have an auto-save option which can be found in your preferences. This will save your document as you work, without your having to remember to do so or interrupt what you're doing. The auto-save function is not a default setting, it needs to be turned on after you install the software.

## Keeping your computer and data safe



Any connection in to your computer can be a source of vulnerability: your office or home network, the internet, a USB flash drive or even someone who has just walked into your office.

### Assess your risks

Security risks differ according to the user and the context of use. What's the last thing you'd want to see happening to your data? Who are the last people you'd want to see getting their hands on it? Think about how to prevent these fears from being realised. Remember that one piece of information may be vulnerable on many different levels.

Think about:

- The communication channels you use and how you use them
- How you store important information
- The physical location of your computer, your external drive and any printed documents containing sensitive information

For more on assessing your risks see: [http://security.tacticaltech.org/chapter\\_2\\_1](http://security.tacticaltech.org/chapter_2_1)

Other important things to consider:

## Firewalls

A firewall is the first programme on a computer to receive incoming data from the internet. It is also the last programme to handle outgoing information. Like a security guard posted at the door of a building to decide who can enter and who can leave, a firewall receives, inspects and makes decisions about all incoming and outgoing data. Most operating systems have a built-in firewall, which should always be switched on. In addition, many anti-virus programmes also come with a firewall.

## Passwords

If you have information you want to keep private, you can save documents or files with a password which only you know. There is an option to create a password on your computer system itself to restrict or limit other users of the computer. You can also save your documents with passwords. In Microsoft Office applications click Save As>Tools>General Options, and then a window will pop up where you can type in your password. In Open Office, go to File>Save As, and then tick the 'Password' option.

Physical security still affects your digital security. You might think your anti-virus software is protecting the information on your USB stick, but if you are carrying that USB stick in your pocket and it starts pouring with rain, you would probably be better off with a sealed plastic bag! Even if you encrypt the data on the hard drive of your computer, you won't be able to use it anymore if someone breaks in and steals your computer.

An 'intruder' can gain access to the information on your computer or portable storage devices remotely, by reading or modifying your data over the internet, or physically, if they manage to get access to your hardware. It is best to have several layers of defence, which is why you should also protect the files themselves. That way your sensitive information is likely to remain safe even if your other security efforts prove inadequate.

There are two general approaches to the challenge of securing your data in this way: you can encrypt your files, making them unreadable to anyone but you, or you can hide them in the hope that an intruder will be unable to find your sensitive information.

## Password tips

1 Pick one really easy password and use it only for nuisance logins - those sites where you know you won't really care if someone gets hold of your account. Yes, someone could steal your password - but what are they going to do with it? If you're worried about protecting your privacy, use a better password, but if you aren't, use the same plain word over and over again and don't think twice about it. Good examples of nuisance logins are:

Newspapers and other online content

Travel sites or airline sites

Email lists, online communities and photo sharing sites

2 Pick one password for private things that aren't life or death. Find a random password or invent a semi-random password. Passwords you should be able to keep to yourself:

Your email account(s)

The FTP login for your website

3 You might need a few passwords you can share – these should change at least as often as staff changes. They should be random passwords, but they shouldn't be the same as any password you use for personal logins. Server passwords and shared websites often fall into the shared category.

4 Your last password category is for really sensitive stuff. Ideally, you wouldn't reuse these passwords, but more importantly, this should be a truly random password, and you should change it from time to time. For example:

A web-based membership database

Remote access to your desktop computer

Banking websites or anywhere your information is stored

Passwords are strongest when they have a combination of letters, numbers and symbols. Easy-to-remember passwords can be made stronger by incorporating numbers in place of letters, for instance: “f@6u1ou5”

For more on password-protecting your computer please see:  
[http://security.tacticaltech.org/chapter\\_3\\_1](http://security.tacticaltech.org/chapter_3_1)



## FAQs

Should I protect my computer with a password?

As standard practice you should password-protect your computer. This is to safeguard it from unwanted eyes or someone walking up to your computer and quickly copying files to an external USB stick. However, password-protecting your computer won't prevent someone having access to your data if your computer is stolen or falls into the wrong hands. To create a password to protect your computer, make it long, make it complex and make it difficult for anyone to guess. But also make it practical for you to remember, and always keep it secret.

Should I encrypt my hard drive?

If you keep any information on your hard drive that is sensitive, you should keep your hard drive encrypted. This will prevent the information from falling into the wrong hands if your computer is stolen.

For more on encrypting your hard drive please see: [http://security.tacticaltech.org/chapter\\_4\\_1](http://security.tacticaltech.org/chapter_4_1)



## Computer viruses

If you use a computer, the sad fact is that you need to know about computer viruses. There are many different ways to classify viruses, each with its own set of colourfully named categories. Worms, macroviruses, trojans and backdoors are some of the more well-known examples. Many of these viruses spread over the internet using email, malicious webpages or other means to infect unprotected computers. Others spread through removable media, particularly devices like USB memory sticks and external hard drives that allow users to write information as well as reading it. Viruses can destroy, damage or infect the information on your computer, including data on external drives. They can also take control of your computer and use it to attack other computers.

To protect yourself from these threats, you need to install an anti-virus application, and run it regularly. There are both proprietary and FOSS versions of these. If you buy a computer, it will probably not have anti-virus programmes pre-installed, so you need to decide which to use. Whichever you choose, ensure that it scans your computer for viruses as well as spyware. Some programmes combine the two functions, while others are separate. A good combination is the two open source applications: Avast anti-virus and Spybot anti-spyware.

You can find out more about these and download them free of charge in the Hands-on Guides in the Security in-a-box toolkit.

Avast: [http://security.tacticaltech.org/avast\\_main](http://security.tacticaltech.org/avast_main)

Spybot: [http://security.tacticaltech.org/spybot\\_main](http://security.tacticaltech.org/spybot_main)

Internet café security note: If you're working in internet cafés you are not going to know if the computer you're working on is infected or not. That's why Avast virus cleaner has a portable application which you can run straight from your USB flash disk. You can download it from the Avast website here: <http://www.avast.com/eng/avast-virus-cleaner.html>

## Tip - Preventing virus infection

- ❑ Be extremely cautious when opening email attachments. It is best to avoid opening any attachment received from an unknown source. If you need to do so, you should first save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the programme's File menu to open the attachment manually, rather than double-clicking the file or allowing your email programme to open it automatically, you are less likely to contract a virus.
  
- ❑ Consider the possible risks before inserting removable media, such as CDs, DVDs and USB memory sticks, into your computer. You should first check that your anti-virus programme has the latest updates and that its scanner is running. It is also a good idea to disable your operating system's 'AutoPlay' feature, which can be used by viruses to infect your computer. Under Windows XP, this can be done by going inside My Computer, right-clicking on your CD or DVD drive, selecting Properties and clicking on the AutoPlay tab. For each content type, select the **Take no action** or **Prompt me each time** to choose an action options then click OK.
  
- ❑ You can also help prevent some virus infections by switching to Free and Open Source software, which is often more secure, and which virus writers are less likely to target.

## FAQs

How do I know if my computer has been infected with a virus?  
If your anti-virus programme is working properly and its virus definitions are fully up to date, you will get a warning window, informing you of the existence of the virus and prompting you to

take action. However, if you aren't so lucky, here is a list of things that should cause you to suspect that you have been infected:

- Applications crash while using them
- Programmes will not load what you start them
- Your computer seems much slower than usual
- You see the 'blue screen of death' when you are try to perform tasks
- You can only start your computer in 'safe mode'
- Accessing or downloading anything on the internet seems to take a really long time
- Random pop-up ads suddenly appear on your desktop, even what you are not at your computer or surfing the internet
- You receive complaints that you are sending infected e-mails (although this can sometimes be a result of spoofing).

What should I do if a virus infects a device such as an external drive?

Your anti-virus programme should be able to scan and clean the external device.



## Internet café security checklist

Internet cafés can be very useful for people who do not have their own computers or internet connections. You pay to use the computer by the minute or the hour, and you don't have to deal with any day-to-day computer maintenance, as you would with your own machine. However, internet cafés present security risks of their own. There are many users coming in and out every day, which means a greater chance of virus infection and even the possibility of others spying on your activities. Nevertheless, internet cafés can be useful for avoiding internet surveillance but you have to know what steps to take to ensure that you remain anonymous and do not leave any trace of your activities behind when you leave. Your aim should always be to leave the computer in the state you found it – as if you've never even been there.

- Make informed choices; make sure the internet café you use is well-known and recommended. Look to see if lots of people are using it, and consider asking for recommendations from friends or locals in the area.
- Check if the computers have anti-virus software running. Also note whether users are allowed to plug their own devices into the computers; for example, digital cameras. The more interaction between the computers and other devices, the higher the risk of coming into contact with viruses.
- Use Firefox rather than Internet Explorer: at the moment there are fewer viruses made for Firefox because it is newer software than Internet Explorer. Take a look at [GetFirefox.com](http://GetFirefox.com) and see what it looks like so that you can recognise it in an internet café. If the computers do not have Firefox installed, consider using it as a portable application.

- ☐ Check for malware: to start your session securely, you need to check that the computer you are using is not already infected. It's a good idea to run the Avast portable application from your USB drive. Otherwise, use an online malware tool to check the computer for malware. A good tool for this purpose is Housecall which is free and only requires a small download (<http://housecall.trendmicro.com/>)
  
- ☐ Leave No Trace
  
- ☐ Protect your personal details: when logging in to your various internet accounts, make sure that you don't select the option to save your details. When you have finished, click the 'log out' option; if you just close the browser window of Gmail, for example, the next person who tries to access Gmail will be taken straight in to your email account. Make sure that any information you fill in on any internet forms is not saved. To do this, go to: Tools > Internet Options > Content > Autocomplete > Clear Forms and Clear Passwords > Ok.
  
- ☐ Delete your internet history. When you've finished your session, clear your cookies (small text files saved on the computer that can identify you and what you did) as well as the internet history which lists the sites you visited. In Internet Explorer, go to: Tools > Internet Options > Delete Cookies and Clear History > Ok. Deleting the files may take a few minutes so make sure you leave time for this at the end of your internet session.
  
- ☐ In Firefox versions 3.5 or later there is an option for 'Private Browsing', where none of your history or information will be retained, or there is an option to 'Clear Recent History'. You'll find both of these options under Tools.



- ☐ Delete any saved documents: if you have saved anything to the computer, make sure that you delete your files, both from the folder you saved them in and from the recycle bin of the computer.

## Troubleshooting



Don't PANIC! There is a direct correlation between the amount of stress a user is under and the number of times a computer will crash. When you are in a rush to get a document finished, you may forget to close open applications or to save your work, and you might well send too many commands (like printing, spell-check, etc.) at once. If you're moving fast on the computer, it pays to take a moment, take a deep breath, close unnecessary programmes and save your work. Also, if you are trying to solve a computer problem, you will need your full mental capacities. So if you're feeling frustrated and tired while trying to troubleshoot – take a break! You'll solve your problems faster if you have a fresh mind and attitude.

## Some Initial Steps

- Reboot the computer, and try to reproduce the problem. If the problem is still happening, write down any error messages you get.
- If the problem involves a peripheral device, check all your wire connections and make sure they are connected properly.

## Finding the problem

- Have you recently installed any new programmes or utilities? For example, if you downloaded and installed a new game and then later noticed that Microsoft Word wasn't working, the problem may be due to the new game.
- Did you have a blackout/brownout/sudden surge in power, or a thunder-storm? Power fluctuations can affect computer equipment, especially if your equipment is plugged in to a surge protector that's overloaded, or isn't plugged into a surge protector at all. Maybe you were cleaning your office and moved or unplugged some equipment and/or cables – double-check that everything is plugged in properly.
- Is the problem affecting only your computer, or is it affecting everyone in the office? If the issue you're dealing with is only affecting your computer, you may be able to see what's wrong by checking the settings on another machine. For example, if you can't print from your computer, but from another computer in the office (with the same operating system and software), printing works fine, then you can look at the other computer's printer settings to see if yours is configured correctly.

- ❑ Is your software up to date? Many software companies will periodically release software updates that fix problems with their software. It's possible that the problem you're having would be fixed by applying an update.
- ❑ If your problem involves your network or your connection to the internet, think about how this connection works:
- ❑ If you get internet access through your office network, see if other people in your office are having the same problem.
- ❑ Check that your hub, server, and firewall are working – can other computers in the office connect to the server? What about connecting to the internet? Is the server on? Can you try rebooting the server? If you have a firewall, is it working? Can you try rebooting the firewall?
- ❑ If you use a dial-up modem for internet access, check to make sure that your modem is plugged in and working – do you hear a dial tone? Does the modem actually dial a number? Do you hear any connection noises?

### Finding a solution

If you still have internet access, try searching the web. Bear in mind that when you're looking for information about a computer problem, either on the web or by telephone, it saves time for everyone if you can accurately describe the problem you're having.

Saying or searching for 'Windows is broken' or 'My email is broken' doesn't really help because it's not a precise description of what the problem is. Saying 'When I try to download my email, I get a "connection to server failed" message in Outlook' is much better because it narrows down the range of possible problems. Clearly articulating the steps you've taken in your attempts to

solve it will also help give a better sense of what the problem is.

Go to the website of the company that makes the product you're having the problem with. If it's a software problem (if your email programme won't open, for example), check the site of the software company. If it's a hardware problem, go to the hardware manufacturer's site. Most companies have a support section on their website where you can search for a description of your problems and possible solutions. Maybe someone else has had the same problem and there's a fix for it, or maybe there's an update that solves it.

It's very likely that someone else has had the same trouble, and you'll be able to find some helpful pointers online. If you find information or examples that suggest solutions, try them! There is a good chance that they'll fix the problem. Please be aware, though, that it can be hard to find exactly what you're looking for – sometimes the search terms that seem obvious to you aren't so obvious to everyone else, so if nothing turns up with your first search, try different search terms. Also bear in mind that solutions will differ for different versions of the same programme or operating system, so be sure to pay attention to those details.

Finally, remember that there may be bad information online too, which will not fix the problem. If you come across a solution that seems extreme or just doesn't sound or feel right, don't try it – research it and see if other people are suggesting the same thing. You are the person responsible for fixing the problem, so take as much time as you need to be certain that the solutions you try make sense to you and to other credible sources. For example, it may be unwise to heed advice about Windows from a Mac website.

Other sites to search:

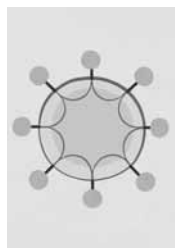
☐ Microsoft knowledgebase: <http://support.microsoft.com>

☐ Apple Support: <http://www.apple.com/support>

☐ Ubuntu Linux Forums: <http://ubuntuforums.org/>

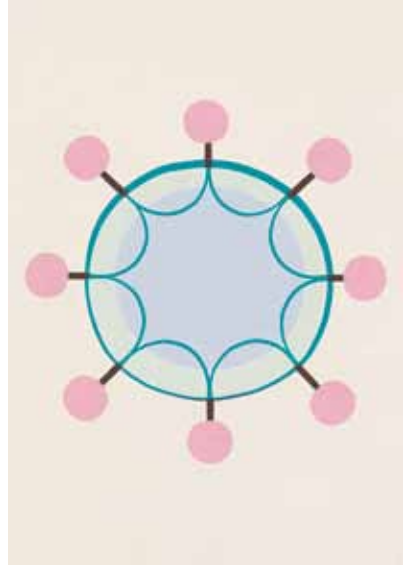
If you've exhausted these strategies, and still haven't found a solution, then reach out to your consultant or a benevolent technology assistance provider. Be sure to have a detailed description of the problem and the steps that you took to try and resolve it.





# 2

## The Internet



### Introduction

The internet can't be bought or owned by an individual, the way a computer or a software programme can. It is made up of millions of computers connected to each other, all around the world, constantly sharing, swapping and storing information.

This section covers simple ways of getting the most out of the internet. It will also introduce you to some of the basic security precautions that you should follow in order to use the internet safely.

After reading this chapter, you should understand:

- How to connect to the internet
- How bandwidth affects what you can do on the internet
- How to use these tools effectively and safely:
  - browsers
  - search engines

online applications

social networking

email

Instant Messaging and VOIP



## Connecting

If you don't have your own computer the easiest way to access the internet is to visit an internet café which provides computers connected to the internet for customers to use. If you do have your own computer, and you plan to use the internet a lot and don't want to sit for hours a day in an internet café, you can set up your own internet connection.

To do this, you will need:

- ☐ To open an account with an Internet Service Provider (ISP)
- ☐ Some extra equipment to help your computer make the connection. This may include: a modem (sometimes these are built into a computer and sometimes they are externally connected), a phone line or a wireless router
- ☐ Software, such as an internet browser and email program (see later sections on email and browsing)

What you can do with your connection to the internet depends largely on how much bandwidth your internet connection gives you. Internet connections are often delivered in the following ways:

Via wires:



- ❑ Dial-up: your computer dials a telephone number using an internal modem to connect. This is slow and limits you to email and light web-browsing.
- ❑ Broadband or DSL and Cable: your computer will use an external modem (often provided by your Internet Service Provider) to connect to the internet via your phone line (it doesn't dial) or via the cable for your television. This provides medium-to-high speed and will allow you to do email and heavier web-browsing, and watch video.
- ❑ Super-fast or Fibre Optic: also done using an external modem, the difference here is that you are connecting to a special wire provided by your ISP. This is fast and will allow you to do just about anything on the internet, but current availability is limited to developed countries.

Wirelessly:



- ❑ Satellite: often used in areas with no existing telephone or television cable infrastructure. A satellite dish is positioned on the outside of a building; it connects to a modem inside the building which provides an internet connection. The speed of the connection will depend on a number of factors. This is an expensive way of getting an internet connection.
- ❑ Wifi: many commercial establishments, including cafes and hotels offer wifi (wireless) connectivity for their customers. Your computer will need its own wifi receiver (now built into most laptops). These connections often operate at medium-to-high speeds.
- ❑ Mobile phones: also called 'Tethering.' Your computer can use your mobile phone as an internet modem if your mobile network provides this service. This is often slow, though some locations may offer higher speeds. Mobile phone network

providers also sell and provide USB peripheral devices called dongles, which will allow your computer to connect to the network's internet signal.

If you have a faster connection, you are able to do much more. If your connection is slower you can speed it up by setting your web-browser to read text only and by not downloading email attachments. These options can be adjusted in the settings of your browser and email programs.

## Security



All data travels through the internet in a readable format unless it is encrypted. SSL stands for Secure Socket Layer; this is the technology which allows your computer to communicate over the internet privately. SSL turns the information into a code (encrypts it) so that it cannot be read by unauthorised people. You may have seen SSL on banking websites where you are required to enter private financial information. You will know when you are on an SSL-supported website because you will see a little padlock sign on the lower frame of the browser window, and the internet address of the site will begin with HTTPS rather than HTTP. It is a good idea to use SSL for your email too, if possible. It will encrypt your login details (so that no one can get hold of your password) and your outgoing email so that it cannot be intercepted on the way to the recipient. If you are using email software (where your email messages are downloaded straight to your computer) such as Thunderbird or Microsoft Outlook, it should be set to use SSL – this needs to be agreed with your server. For webmail accounts, such as Gmail and Yahoo, you will probably also have to enable SSL, either as a preference in your account settings or by typing in the HTTPS manually (by logging in to <https://gmail.com> instead of <http://gmail.com>). You should always make sure that your connection is secure before logging in, reading your email, or sending a message.

## Tips

If your internet connection has recently slowed down, it is worth investigating. Sluggishness can be caused by anything from a virus to a bad configuration on your hardware. Some useful information about troubleshooting for slow internet connections can be found here: <http://compnetworking.about.com/od/speedtests/tp/slow-network-connections.htm>



# Browsing Web-pages

A web-browser is the main way for you to view information on the internet. If you are reading this guide on the web, then you are using a web-browser to do it. The most commonly used browsers are Internet Explorer, Mozilla Firefox, Apple Safari and Google Chrome. Most of what you do on the internet can be done via the web-browser.

This includes:

- Reading web-pages
- Research using a search engine
- Reading and composing email
- Creating and editing documents and spreadsheets, using online applications
- Interacting with online communities and networks
- Creating and updating your own web-pages
- Communicating in real time via text and voice.

Things you will find in a web browser:



- An address bar where you can type the address (or URL) of a website (such as [www.tacticaltech.org](http://www.tacticaltech.org)).
- A search window (in which you can type keywords) that connects to a search engine
- A home button which will take you back to a designated web-page that is opened every time you restart your browser (this can be changed in the 'preferences' or 'options' menus).
- A stop button which will stop a web-page from loading. This is helpful if the page seems to be taking a while to download into your browser
- A reload/refresh button which will start downloading the page again from the beginning
- Forward and Back buttons which make it easy to navigate through pages you have already browsed.
- A bookmark bar, where you can store website addresses which you might want to visit again.

## Troubleshooting web-browsers

There are a lot of reasons why your web-browser might have problems loading a web-page. The first thing to try is clicking the 'reload' button. If that doesn't work, then:

- If you get an error message that says 'this page can not be found', check that you have typed the address correctly.



- ❑ If you get an error message that says ‘Unauthorised’ or ‘Forbidden’, the page you are looking for may be censored. See below, under Security, for more information on this.
- ❑ If you are seeing a screen with a funny-shaped box and some x’s on it, or if there is no content on the page at all, you might be missing an add-on component which extends the capabilities of your browser; for example, by allowing you to watch a video. Your browser should give you a message about installing what’s missing and usually it’s safe to follow these instructions.
- ❑ If the page won’t finish loading, your internet speed might be too low for the amount of graphics and other content on the page in question. Click the stop button and see if the page offers a link for a text-only option. Alternatively, you can set your browser preferences so that it does not load images.

## Security



Many countries have installed software to prevent people from accessing certain websites and internet services. Companies, schools and public libraries often use similar software to prevent employees, students and patrons from accessing material that they consider distracting or harmful. Some filters block sites based on their IP addresses, while others blacklist certain domain names, or search through all unencrypted internet communication, looking for specific keywords.

If you suspect that the page you are looking for is being censored, you may want to consider using an anonymity tool like Tor ([www.torproject.org](http://www.torproject.org)). You can learn more about bypassing censorship in Security in a Box (<http://security.ngoinabox.org/en/chapter-8>)

## Tips

- ❑ **Don't use Internet Explorer.** Internet Explorer is the most common web browser, but it has many flaws and vulnerabilities that viruses and spyware take advantage of. Instead, consider Mozilla Firefox which is recognised as being safer and more secure than Internet Explorer. It's free to download and install, and it has a number of add-ons which enhance the security and privacy of your internet browsing. You can find out more about it and download it in the Security in-a-box Hands on Guide ([http://security.ngoinabox.org/firefox\\_main](http://security.ngoinabox.org/firefox_main))
  
- ❑ **Beware of Pop-Up Scams.** Viruses, adware and spyware. They will trick you into thinking that you're downloading or installing things that are good for your computer. Often when you're surfing the web, ads will pop up on your screen, saying things like, "Your computer may have viruses – click here to protect your computer!" Sometimes these pop-ups look just like messages from Windows or another legitimate program. Don't respond to these prompts.
  
- ❑ **Use Bookmarking!** It's easy to lose track of all the great stuff you see on the web, and bookmarking is one way both to record addresses and to organise them. Every browser has a bookmark menu. If you use internet cafes, you can use a service like Delicious which will provide you with a place on the web to store your bookmarks.
  
- ❑ **Never ever give up your account information** if you have doubts about security. Although it is very helpful and easy to buy things and do your banking online, be sure to check the security of the online stores you wish to use, as well as that of any banks you may have transactions with. They should always use SSL.

# Searching Web-pages



The web-browser is a great tool for research. To find information on the web, you can use a search engine to look for relevant words (keywords) that are embedded in web-pages.

Search engines store information about web-pages, which they gather using automated systems known as 'web-crawlers'. When you enter keywords into a search engine, they search their own databases for web-pages containing those keywords. The search engine lists the results, with the more frequently visited web-pages at the top of the list.

The most commonly used search engines are Google, Yahoo and Bing.

## Security



If you are concerned about someone monitoring your search keywords, you can use an SSL connection with Google. Just type in <https://www.google.com>. This doesn't prevent Google from logging your search requests, but it does ensure that your search is not being monitored by a third party on the internet.

If you are also concerned about Google logging your search requests, you can use a search engine like Scroogle <http://scroogle.org>), which uses Google's search database but doesn't log your keywords.

## Tips

When using a search engine, make your searches as simple as possible and use as few words as possible — 'weather bangalore' will give better results than 'weather report for Bangalore, India'. Think of how things might be written on the page you are looking for: 'Stomach ache' will yield better results than 'my stomache hurts'.

## Working Online



As bandwidth and access to the internet increase, there are a growing number of web applications which can be used as substitutes for traditional software which you have to install on your computer. The advantages of using web applications are that you don't need to do any installation and there is little or no cost involved in using them. They are very helpful if the majority of the computer work you do is in an internet cafe. The negative side of this is that it's quite easy to lose control of your content, and you can't access these applications if your internet connection goes down.

You can use these applications to do things like creating text documents and spreadsheets and editing photographs. However, in order to do this you need to have at least a broadband connection; dial-up is simply too slow.

Popular Web Applications include:

- ☐ Google Docs, Spreadsheets and Calendar
- ☐ Microsoft Office Live
- ☐ Adobe Photoshop Express

## Security



All the content that you are creating and working on within an online application is being stored somewhere on the internet and not on the hard-drive of your computer. This can be a real problem if your account becomes compromised and someone else gains access to your user name and password. Never include sensitive information when using an online application.

## Tips

- ☐ Online applications are great for short and small projects, especially if you need to collaborate with people in other geographic locations.
- ☐ Remove your files after you are finished, to ensure that they are not accessible to others. After you have downloaded your files, follow the on-screen prompts to delete them from the online application's storage.

# Engaging Communities Online



In recent years the web has been increasingly used to allow communities and networks of people to share content and connect. The most well known of these are Facebook, Twitter, YouTube and Flickr but there are more being created all the time and millions of people are using them.

They are a great way to find, and keep in contact with, people with whom you have lost touch. They are also very good for building and maintaining an online community with common interests. Many NGOs use Facebook groups and pages as a way to stay in touch with their members and keep them informed about their activities and events. It is often easier and more engaging to communicate and share information with large groups through a social network site rather than by email. Activists use YouTube and Flickr to share and publish online video and pictures.

Facebook, YouTube and Flickr, along with other social network sites, feature the option to email you whenever a comment is

made on one of your posts. In this way you can track people's uptake of and response to your message, which will help you make decisions about the value and effectiveness of using different online platforms and services.

## Security



You should maintain your security awareness on these sites just as you would on any other. Beware of clicking on unknown links posted by other users, and of suspicious messages to your account. Also, remember that the information you put into a social networking site may not be private and many different people may look at it, including people that are not trusted friends. You can usually tune your privacy settings in your account options and control who can see your profile, but you might also consider signing up under a pseudonym to avoid divulging too much private information.



## Establishing a web-site



It's very easy to create content that is accessible to anyone on the internet, particularly if it's text-based. Weblogs or Blogs are websites which use a diary or log format. They are easy to set up and configure and are also easy to maintain over time. Using Blogs, you can easily establish a web presence for yourself or your campaign.

Blogs are good for posting updates about events or if you want to allow many people to contribute individual posts about a particular topic. You can incorporate into your blog other content that you've posted on sites like YouTube or Flickr.

Popular blogger services are: Wordpress, Blogger and Blogspot. A great place to get started with using a blog is the 'Plan your blog' Web-page at Message-in-a-box - <http://messageinbox.org/planyourblog>

## Keeping track of web-pages

RSS (Really Simple Syndication) feeds are an easy way of keeping track of new content and headlines on your favourite websites and blogs. Once you've subscribed to a website's RSS feed, you can receive notices about new content and a summary of this content. This means that instead of checking each individual website for new content, you just check your RSS feeds.

Most browsers have an RSS aggregator function built in and you can easily subscribe to a feed on a website by clicking on the RSS icon that appears in the address bar. In Firefox, this is called 'live bookmarking'. Popular email software such as Thunderbird will let you subscribe to and view RSS content in a format similar to email. You can also use web-based tools like Google Reader, which will show you your RSS feeds on a dedicated page.

The disadvantage of aggregators and RSS feeds is that you can become overwhelmed with updates and information. Subscribe only to things you absolutely need to follow.

For more on RSS feeds, see <http://messageinbox.org/RSS>

## Using email



Email is a fast and efficient way to communicate. It is very useful for sending messages to which you need a timely reply, it's a great way to keep people informed about developments and it also makes it easy for people in different geographical locations and time zones to discuss topics and issues. It can be used as a tool for planning, and for content creation. However, email is not ideal for more nuanced discussions, and because it is text-based it can be easy for the tone of comments to be misunderstood.

You can access an email account in two ways, either using an application dedicated to receiving, sending and managing your messages, such as Outlook Express or Thunderbird, or via your web-browser, using online services like Gmail, Yahoo Mail, or Hotmail. Before doing anything, you will need to open an account with an email provider (see below).

The main thing to remember about email is that all data travels on the internet in a readable format, so if someone intercepts your email along the way, they can read the content easily. You

would be surprised by just how many people could view this content if they wanted to. The internet is a huge, worldwide network of computers, all directing traffic among themselves, so there are very many different people who have the opportunity to intercept a message in this way.

## Security



Few of the webmail providers available offer SSL access to your email. Some of them give you a secure login to protect your password but the messages you send and receive are not secure. Some even insert the IP address of the computer you are using into all of the messages you send. Two providers which are worth considering are Gmail and Riseup.

- GMAIL: can be used entirely through a secure connection, as long as you login to your account from <https://mail.google.com> (with the HTTPS), rather than <http://mail.google.com>. To

ensure ultimate security, you also need to set a preference that tells Gmail always to use SSL in sending and receiving mail. However, we don't recommend relying entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom.

- ☐ RISEUP: If you don't have an email account yet, or wouldn't mind switching, the best we can recommend is Riseup <https://mail.riseup.net>. RiseUp offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. Unlike Google, they have very strict policies regarding their users' privacy, and no commercial interests that might conflict with those policies. In order to create a new RiseUp account, however, you will need two 'invite codes' which can be given out by anyone who already has a RiseUp account.

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. Even if you are accessing your email account securely, your recipients may not be using a secure email account when reading and replying to your messages. To ensure private communication, you and your contacts should all use secure email services. If you want to be certain that messages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. In this case, RiseUp is a good one to choose.

If you suspect that someone is monitoring your email, you should read 'Tips on responding to suspected email surveillance' at [http://security.ngoinabox.org/en/chapter\\_7\\_2](http://security.ngoinabox.org/en/chapter_7_2)

## Tips

- ❑ Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.
- ❑ You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is Tor. You can find out more about this in chapter 8 of Security in-a-box at <http://security.ngoinabox.org/chapter-8>.
- ❑ If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.
- ❑ You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.
- ❑ You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked. A list of sample words blocked by spam filters can be found at <http://www.mequoda.com/articles/subject-line-spam-trigger-words/>
- ❑ Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut

down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.

- ☐ Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.





## Real-time messaging

With Instant Messaging (IM), you can have a real-time conversation with someone living miles away from you, without spending money on expensive phone bills and calling cards. You may have heard of some of these services: Skype, Yahoo Messenger, Google Talk or MSN to name the most popular ones. With these programmes you can create a contact list (like a list of email contacts) of people who use the same service. You can be alerted when they come online and then you can initiate text chat with them. Some of these services allow you to transfer files, such as documents or images, across the chat. Some of them also offer the added benefit of using web-cams so you can see the person you are chatting with, and some even allow you to have voice conversations using a microphone and your computer's speakers.

### Security



With IM, it may seem as though you are having a 'private chat' with someone, but because it's transmitted via the internet this may not be the case. Unfortunately IM programmes don't offer good security so you need to use other programmes to do this. You are more secure if both you and your instant messaging contacts use the same software and take the same security precautions.

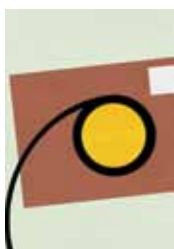
## Online Voice-Calls

Thanks to voice over internet protocol (voip) technology, you can have telephone-like communication via the internet. Many chat and instant messaging clients now support making VOIP calls and often provide this service free of charge.

A popular VOIP service is Skype. With this you can call another Skype user anywhere in the world at no cost – as long as they also have an internet connection. Skype also allows you to buy credit to make inexpensive international calls to landline phones.

Other VOIP applications include:

- ☐ Qute.com (<http://www.qutecom.org/>)(formerly known as WengoPhone)
- ☐ Adium (ver. 1.0.2 -> 1.3.2; <http://www.adiumx.com/>)
- ☐ Colloquy (ver. 2.1 -> 2.1; <http://colloquy.info/>)
- ☐ Pidgin (ver. 1.5.0 -> 2.5.2; <http://gaim.sourceforge.net/>)



# 3

## The Mobile Phone



### Introduction

Mobile phones provide individuals and organisations with access to a range of voice and data services. This chapter will show you how to make the best use of your mobile phone.

After reading this chapter, you should know:

- What features to look for when purchasing a mobile phone
- How to connect your mobile phone to your computer
- How to make the most of your mobile phone's camera, video and sound recorder
- What security issues you should be considering when using your mobile phone

## How mobile phones work



A mobile phone is actually a very advanced and complicated radio.

When you talk into a mobile phone, it converts the sound of your voice into radio waves. These waves travel through the air until they reach a receiver at a nearby base station (owned by the mobile network operator). The base station then sends your call through the telephone network until it reaches a base station near the person you are calling. That base station sends out radio waves that are detected by a receiver in the recipient's telephone, where the signals are changed back into voice or data. The sound quality of the call depends on the ability of the two phones to send and receive signals from the base stations.

Today the voice function is the least of a mobile phone's capabilities. Mobile phones may support services such as SMS (Short Message Service – for text messaging), email, internet browsing, video and still cameras, MMS (Multimedia Message Service – for sending and receiving photos and videos), MP3 players, FM radio, and even access to the internet.

## The SIM Card

If you remove the back of your mobile phone you will find the battery, underneath which is the SIM card. SIM stands for Subscriber Identity Model and this card is where information about your network provider and your phone number is stored. By moving the SIM card you can move your phone number and stored contacts from one phone to another. This is useful if your phone is broken or damaged, because you can remove the SIM and put it in another phone. You can also put a different SIM card in your phone, and thus use a different phone number. This can be useful when you are travelling and want to use a local number (see the *Travelling* section).

## Creating and sharing content using mobile phones

There are now many ways to create and share multimedia (videos, pictures and text) content from your mobile phone, either between phones or via the internet, and reach a broad audience.

Depending on the model of your phone, you can:

- Take photos or record videos to document events or provide evidence for advocacy work
- Record short interviews
- Share images with others via MMS
- Send text messages via SMS
- Send updates via the internet to micro-blogging sites, such as Twitter
- Upload content via the internet onto content-sharing sites, such as YouTube and Flickr, or onto Wordpress blogs

With mobile internet costs falling in some countries, mobile phones are increasingly being used to access the internet while on the move. Some mobile phone providers offer fixed monthly packages for internet use while others sell 'bundles' of mobile data. With a phone that has a wireless internet connection it is also possible to access the internet on your phone through free wireless 'hotspots'. NGOs can take advantage of this by creating specially adapted mobile versions of their websites. There are online services such as Wapple.net and MobiSiteGalore which can help you create mobile-friendly websites.

To read a selection of case studies, showcasing a variety of innovative ways that mobile phones have been used by individuals and organisations, visit the Mobiles in-a-box website at <http://mobiles.tacticaltech.org/taxonomy/term/4>

## Challenges

Updating a blog or website with content sent directly from your mobile phone often requires that you pay to sign up with a service outside your country; this means you may be charged the cost of an international message every time you use the service.

You may need to connect your mobile phone to a computer to be able to download photos and videos and share them through the internet.

The quality of video captured on most mobile phones remains low. Unless you or your organisation are prepared to invest heavily in a high-end mobile phone, the uses of video made on mobile phones may be quite limited.

Sending MMS messages (i.e. image or video files from your mobile phone to another mobile phone or to a website) is still extremely expensive in most countries and it doesn't always work.



## Choosing a mobile phone

Before buying a phone, consider what you are going to use it for. Someone who needs to take lots of photographs with it will need a different phone from someone who only wants to send text messages. With this in mind, we recommend that you spend some time looking at the features available on different phones, so that you can select one that meets your needs. You can use a website like Mobyedia (<http://www.mobiledia.com/phones/search/>) to help you research and compare the features of different mobile phones before you choose one to buy.

Below are some issues to consider when choosing a phone for individual or organisational use.

### Payment plans

#### Prepaid

Often called 'pay-as-you-go', this allows you to purchase credit to use on a mobile phone network as and when you need it. You can make calls, send SMS and MMS and use the internet until you run out of credit; you buy more credit when you need to.

- ☐ **Advantages:** No bills and no contracts! It is much easier to control your spending this way, and you have the freedom to swap to another mobile phone provider if you wish. If security is a concern, it's possible to obtain and use a prepaid mobile phone without establishing a link between your identity and the phone.
- ☐ **Disadvantages:** Calls, texts and internet use are often more expensive than on a contract. You also have to buy the telephone handset yourself.

## Contract

This usually involves undergoing a credit check, signing paperwork and being billed monthly for your mobile phone usage.

- ❑ **Advantages:** Cheaper calls and texts and greater freedom to use your mobile phone network in other countries (called 'roaming'). A monthly allowance of calling minutes, texts and internet time is often included in your plan. In most cases you pay off the cost of the handset over the period of your contract, and do not have to pay for it upfront.
- ❑ **Disadvantages:** It is difficult to keep track of your spending and you may end up with large bills at the end of the month. You are also locked into a contract, for which you must continue to pay for a fixed period of time (at least twelve months in most cases).

## Locked or un-locked phones

If you need to be able to use multiple SIM cards in your phone for security reasons, you will need a phone which is unlocked, which means you are free to use it with any service provider, not just the one you bought it from. Phones which are bought as part of a contract with a mobile service provider are often locked.

If you have a locked phone you can get it unlocked. You will need to contact the network provider for the unlock code.

## Battery life

Phones with advanced features such as video recorders may have a limited battery life. If you are likely to be away from a power supply for long periods of time, you should investigate the battery life of the phone.



## Bands

The Global System for Mobile Communications (GSM) uses four different frequencies for mobile phones, each in a different region of the world. A dual-band phone will work on two of the three frequencies which are used in Europe, Asia and most other places except the United States. A tri-band phone will operate on three of these frequencies, and a quad-band on all four frequencies. If you intend to travel widely with your phone, it's advisable to use a tri-band or quad-band phone. See the section below on *Travelling with your mobile*.

## Data Speeds

If you want to use the internet on your mobile phone you will need to understand data speeds. The current standard for mobile internet is 3G, which is often compared to the average broadband speeds you get for your computer, but in reality is usually a bit slower. It's fine for email and web-browsing and even watching video online. GPRS or 2G are the older speeds and are generally equivalent to dial-up internet speed, which is

fine for email and light web-browsing. If you want to use the internet on your phone, you must first find out if your phone is internet capable and at what speed, and then find out if your mobile network offers internet access (usually at an extra price), and at what speed.

## Storage capacity

Taking pictures using your mobile phone can use up your phone's memory so if this is a priority for you, it's advisable to consider either buying a mobile phone with a large memory or one that can take an external memory card (which is also helpful when it comes to transferring files to your computer).



## Connecting to your Computer

When choosing a mobile phone you should ensure that it is compatible with your computer operating system (e.g. Mac/Windows/Linux). You will need to connect your mobile phone to your computer to transfer multimedia files, and to back up information, such as your contacts.

In order to do this you will first need to install software on your computer that will allow you to manage your phone's content on the computer. This software is usually provided when you buy a phone. However, if you have acquired a second-hand phone or lost the package your phone came in, you can always check the manufacturer's website and download the software from there.

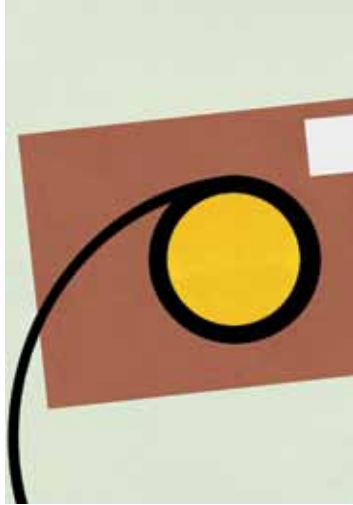
Once the software is installed, there are three ways to connect your mobile phone to your computer:

- Using the data cable supplied with your phone
- Using an external memory card in your phone which can be removed and placed in a memory card reader (some computers have these built in, or you can buy an external USB reader)
- Data transfer via Bluetooth, Infrared or Wifi

If you are buying a mobile phone and want to use Bluetooth for data transfer, make sure that the mobile phone actually supports this. Sometimes mobile phones have Bluetooth capability but do not allow actual data transfer. If your computer does not have internal Bluetooth capabilities, you can purchase a Bluetooth USB device (sometimes called a 'dongle') to plug into it.

# Making the most of your mobile phone's multimedia capabilities

## Photographs



A mobile phone camera can be a great way to document important events when you are in a difficult situation where a larger camera might attract unwanted attention.

If all you require is small images for use in emails or on a blog or website, then the camera function on most standard mobile phones should be adequate. If you want to print your pictures, you need to think about the number of megapixels the mobile phone camera offers.

Megapixels explained: All digital cameras capture images in pixels. A megapixel is equal to 1 million pixels. The quantity of megapixels is what determines the quality (resolution) of the picture the mobile phone can produce. A 2 megapixel camera will allow you to take an image which will print a picture 8 inches by

10 inches at fair-to-good image quality (150 pixels per inch). A 3 or 4 megapixel camera on your phone will produce a much higher-quality image, which means that even larger prints will be acceptably sharp.

If you are unsure about the capabilities of your phone's camera, it is worth testing it a few times, transferring a few trial images into the format you hope to use them in (email/print/web etc), before using the camera for anything important.

Taking pictures using your mobile phone can use up its memory quickly. If you want to use your mobile phone for taking photos it is a good idea to invest in a phone that has a large memory, or one that can take external memory cards.

## Sound Recording



Sound recordings are usually saved in mp3 file formats (the same as most music files). If you want to edit a sound recording, you



will first need to transfer it from your phone to a computer – see *Connecting to your Computer*, above.

The recording can be edited with a sound editing tool, such as the free software Audacity (read more about how to use this, and download it, in the *Message in-a-box Hands On Guide* <http://messbox.tacticaltech.org/viewtool/audacity>). Audacity includes many filters that can add effects to your sound recording or get rid of background noises. The process can work in the opposite direction as well: you can create recordings on your computer and transfer them to your mobile phone.

You can turn a sound recording into a ringtone and distribute it to raise awareness around a particular issue. In the Philippines, part of an alleged conversation about vote rigging between the Comelec Commissioner Virgilio Garcillano and President Gloria Macapagal-Arroyo became a hugely popular ringtone on mobile phones. For an explanation of how to use Audacity to create ringtones, see the tutorial at [http://wiki.audacityteam.org/index.php?title=Making\\_Ringtones](http://wiki.audacityteam.org/index.php?title=Making_Ringtones).

## Video recording

Video images recorded using your mobile phone will also need to be converted if you hope to edit them. Most mobile phones save video recordings in file formats called .mp4. These files can be edited using video editing software which may already be included in your Windows (Windows Movie Maker) or Mac (iMovie) operating system. For more on creating and editing videos, including links for free tools to edit and format videos see the video section of *Message in-a-box* <http://messbox.tacticaltech.org/section/10>



Mobile phone video quality is sufficient for creating short videos to upload on social media websites (such as YouTube, Daily Motion and Facebook) but some high-end phones are capable of producing high definition video which is 60 frames per second, 1280x720 pixels resolution.

## Sending multimedia messages

Multimedia messages allow users with MMS-capable phones to send text, photos and video to one another across a mobile network. MMS can be used to send images or videos to people, as part of a campaign, or to news sites to report on or publicise an event. Different phones compile MMS messages in different ways, but it essentially involves a similar process to email, through which pictures, video and sound files can be sent as attachments.

You should bear in mind that the cost of sending and receiving these files varies greatly between mobile phone service providers

and countries. Before you start using MMS as a way of exchanging images or video, it is worth finding out the cost! The MMS function normally has to be set up by the service provider – you can find out about this by calling your provider’s customer service centre.

If your intended recipient is unable to receive the MMS for some reason (perhaps the mobile phone is not MMS-enabled, or it is an older handset) then the user will receive a standard text message directing them to a website where they can view the message and attachments online.

## Travelling with your mobile phone



Mobile phones are incredibly useful to have when travelling – however, using your phone in another country (or even another region of the same country) can be expensive.

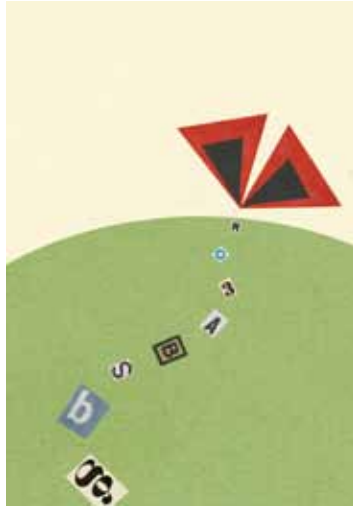
Here are some things to keep in mind if you are going to travel:

- ☐ Will your mobile phone actually work? If you have a quad band phone, this shouldn't be a problem (see the section on *Bands*, above, for more about this).
- ☐ What will it cost to use your phone on a different network? Your mobile phone provider will charge you a premium price for leaving their network and using another. Before you travel, check the per-minute price for receiving and making calls, and for sending and receiving SMS messages, at your destination. Any data or internet services will also be charged at a

premium rate. If these prices are prohibitive, you may want to consider using a local SIM card.

- ☐ Use a local SIM card. Many mobile phone providers sell SIM cards for pay-as-you-go services. If you are going to have a high volume of calls while you are abroad this is a very affordable option, particularly if people in the country you are visiting need to call you on your mobile via a local number. To do this you will need an unlocked phone (see section on unlocked phones). It is best to check to see if this an option before you travel but you will probably need to wait until you reach your destination to buy the SIM card and the number you will be able to use.

# Mobile security & privacy



Mobile phones carry a vast amount of data; not just your contacts but also logs of calls made and received, and of SMS messages sent and received. They can reveal a lot about you; for example, the list of all your contacts in your mobile phone shows exactly who you are working with. If you are working on a politically sensitive issue this can put you and everyone you work with at risk.

There are obvious security concerns for people who use mobile phones to record video or take photos in sensitive situations. If a phone is confiscated or found with footage in it that incriminates others, those people could be put at risk as well as the phone's owner. Great caution should be exercised at all times.

Special care needs to be taken if and when this content is transmitted over the mobile network as mobile phone service providers can be pressured to hand over records of activity on particular phones.

Networks also automatically track the location of each and

every active mobile phone – this is done for the purposes of routing calls and messages. This means that members of the public (or at least their phones) can be pinpointed to a specific location at a specific time. The only way to ensure your location cannot be identified is to turn your phone off and remove its battery.

Mobile phone cameras also routinely store the location where an image was taken, along with details of date, time and the type of camera or phone used. This information, or metadata, is stored as part of the JPEG standard which is the file format most commonly used for digital images. This information could be useful to you in some circumstances – to prove that you were in a particular place at a particular time to witness an event – but it could also get you into trouble, depending on the situation. Tools are available which enable this ‘hidden’ information to be viewed, and (in most cases) removed, before the image is forwarded to others. You can download a free tool called JPEG Stripper (<http://www.steelbytes.com/?mid=30>) which will help you remove metadata from your images.

## Mobile Security Checklist

- When using your phone, remain aware of your surroundings and do not use it in crowded areas or where you feel unsafe.
- Avoid displaying your phone in public. Keep it with you at all times and do not leave it unattended.
- Always use a PIN code to unlock your phone’s keypad and functions. See the phone’s security settings to set this. Use invisible ink to mark the phone and battery with your postcode and street number or the first two letters of your house name. This can be helpful in recovering your phone if it is lost or stolen.

- ☐ The 15-digit serial or IMEI number helps to identify your phone. This can be accessed by looking behind the battery of your phone – it should be visible as a 15 digit number. Make a note of this number and keep it separate from your phone, as this number could help the police to trace ownership quickly if it is stolen.

For more information, visit the Security section of the Mobiles in-a-box toolkit (<http://mobiles.tacticaltech.org/security>)






<http://survival.tacticaltech.org>

ISBN 978-93-80765-00-6

This guide explains the basics of the three most widely used digital tools: the computer, the internet and the mobile phone. We aim to make these accessible and easy to use for human rights advocates working in any environment.

This work is licensed under a Creative Commons Attribution-Share Alike 3.0 Unported License.



A project of

TACTICAL  
TECHNOLOGY  
COLLECTIVE

