



# Cyber Safety

Cover Fundamentals of protecting information and devices from online risks  
Syllabus version 2.0

### **Courseware Disclaimer**

European Computer Driving Licence, ECDL, International Computer Driving Licence, ICDL, e-Citizen and related logos are all registered Trade Marks of The European Computer Driving Licence Foundation Limited ("ECDL Foundation").

DM3 is an entity independent of ICDL GCC Foundation and is not associated with ECDL Foundation or ICDL GCC Foundation in any manner. This courseware may be used to assist candidates to prepare for the ECDL Foundation Certification Programme as titled on the courseware. Neither ICDL GCC Foundation nor DM3 warrants that the use of this courseware publication will ensure passing of the tests for that ECDL Foundation Certification Programme. This courseware publication has been independently reviewed and approved by ICDL GCC Foundation as covering the learning objectives for the ECDL Foundation Certification Programme.

The material contained in this courseware publication has not been reviewed for technical accuracy and does not guarantee that candidates will pass the test for the ECDL Foundation Certification Programme.

Any and all assessment items and/or performance-based exercises contained in this courseware relate solely to this publication and do not constitute or imply certification by ECDL Foundation in respect of the ECDL Foundation Certification Programme or any other ECDL Foundation test. Irrespective of how the material contained in this courseware is deployed, for example in a learning management system (LMS) or a customised interface, nothing should suggest to the candidate that this material constitutes certification or can lead to certification through any other process than official ECDL Foundation certification testing.

For details on sitting a test for an ECDL Foundation certification programme, please visit ICDL GCC Foundation's website at [www.icdlarabia.org](http://www.icdlarabia.org).

Candidates using this courseware must be registered with ICDL GCC Foundation before undertaking a test for an ECDL Foundation Certification Programme. Without a valid registration, the test(s) cannot be undertaken and no certificate, nor any other form of recognition, can be given to a candidate. Registration should be undertaken with ICDL GCC Foundation at an Approved Test Centre.

## Table of Contents

<b>Chapter 2-1 Protect</b>	<b>4</b>
2-1-1 Identity	5
2-1-2 Authenticate	10
2-1-3 Anti-Virus	12
2-1-4 Anti-Spyware	15
<b>Chapter 2-2 Secure</b>	<b>19</b>
2-2-1 Backup	20
2-2-2 Email	24
2-2-3 Wireless	26
2-2-4 Physical	28
2-2-5 Smart Devices	30
<b>Chapter 2-3 Beware</b>	<b>39</b>
2-3-1 Online Risks	40
2-3-2 Shopping Online	43
2-3-3 Paying Online	47
<b>Chapter 2-4 Think First</b>	<b>51</b>
2-4-1 Personal Identity	52
2-4-2 Sharing Devices	55
2-4-3 Social Networking	57
2-4-4 Spamming & Phishing on Social Networking Platforms	59
2-4-5 False Identities on Social Media and Grooming	63
<b>Chapter 2-5 Virtual World</b>	<b>71</b>
2-5-1 IM / Chat Rooms	72
2-5-2 Video, Blogs	75
2-5-3 Online Games	79
2-5-4 Be Responsible	81

<b>Chapter 2-6 Learn Together .....</b>	<b>87</b>
2-6-1 Discuss .....	88
2-6-2 Parental Controls .....	91
2-6-3 Online Addiction.....	102
<b>Chapter 2-7 Virtual Behaviour.....</b>	<b>108</b>
2-7-1 Communicating .....	109
2-7-2 Cyberbullying .....	112
<b>Chapter 2-8 Policy .....</b>	<b>119</b>
2-8-1 Usage .....	120
2-8-2 Copyright .....	123
<b>Chapter 2-E Exercises .....</b>	<b>126</b>
2-E-1 Facebook.....	127
2-E-2 Twitter.....	132
2-E-3 YouTube.....	136
2-E-4 Google+.....	137
2-E-5 LinkedIn.....	141
2-E-6 Blogs .....	146



# Goals

---

**Cyber Safety** provides Candidates with the skills and knowledge required to operate safely with computers and a range of mobile devices and to be aware of online threats. Candidates will recognise the need to safeguard personal information on computers and mobile devices and will recognise the threats posed by Internet criminals and scams.

Candidates will understand the threats posed by viruses and will know the importance of using anti-virus software and firewalls. Candidates will know about back-up procedures and good password practices as well as knowing how to filter email for spam and the importance of scanning email attachments before opening them.

Candidates will be aware of the information contained in smart devices and how it is shared online. Candidates will know how to set appropriate security features for smart devices to guard against security threats and prevent unauthorised access to the device and the data it contains.

Candidates will recognise the risks in everyday use of the Internet and know how to protect themselves when shopping online. Candidates will be aware of the implications of putting personal information on social networking sites and be aware of privacy issues. Candidates will be aware of the range of devices that can be used to share information and how photo and video features may be used to record and post inappropriate information.

Candidates will be aware of some of the dangers associated with social networking, including inappropriate content, age verification issues, access to profiles and the potential for predators. Candidates will understand the threats posed by social engineering attacks and the cyber threats posed to children by the use of false identities on social media.

Candidates will learn responsible behaviour practices when engaging in online activity: the importance of not circulating material that would be hurtful to others, knowing how to decline or block strangers and unwanted contacts, using a webcam solely with people you know, treating others online with respect.

Candidates will learn how to set parental controls in order to protect their children's online activities as well as selecting and using filtering and monitoring software. Candidates will understand the concept of online addiction and how to recognise the symptoms of the same as well as how to deal with the problem. Candidates will recognise and understand what cyberbullying is and understand the mediums through which it can occur. Candidates will recognise the warning signs of cyberbullying and know how to counter it. Candidates will understand why organizations develop and adopt Acceptable Usage Policies (AUP's) and recognise the components of effective policies.

## Chapter 2-1

### Protect

2-1-1 Identity

2-1-2 Authenticate

2-1-3 Anti-Virus

2-1-4 Anti-Spyware

## 2-1-1 Identity

### 2-1-1-1 Recognise that personal information contained on your computer needs to be safeguarded.

More and more people are using their PCs, laptops, tablets and smartphones to conduct their personal affairs online. Activities such as social networking, online shopping, job hunting and contacting government departments, are part of our everyday life. As we undertake these activities organisations collect and use our personal information, they have a responsibility to protect this information. There are also precautions we can take to protect our personal information and safeguard access to the information stored on our computers and phones.

To protect your computer, and therefore your personal information, some of the things you should do include:

- Installing security software to protect against attacks and viruses
- Keeping your software up to date
- Clearing your browser history and cookies on a regular basis
- Never sharing passwords
- Using caution when opening email attachments
- Frequently backing up your important files, documents, etc. to safe external device.
- Refraining from downloading unfamiliar software or programmes from the Internet.

Social media platforms have privacy and security policies, to protect your personal information when you communicate online, see Fig. 1 below that shows Facebook's Security page:




Fig. 1 Facebook Security page (<https://www.facebook.com/security/>).

## 2-1-1-2 Recognise the serious threats posed by Internet criminals and Internet scams.

Anyone who uses the Internet is at risk from Internet crime. The Internet is an easy way for criminals to deceive people out of money by stealing their personal information. Criminal exploitation of the Internet, sometimes referred to as Netcrime or cybercrime, happens when offences are committed against individuals or groups of individuals using modern telecommunications networks such as chat rooms, emails, social media platforms and text/SMS messaging. Common methods are:

- Virus programmes – corrupt or delete data files
- Identity theft - stealing someone's personal information
- Pharming - an attempt to redirect a website's traffic to another bogus website
- Hacking - accessing computer networks by bypassing the security systems
- Spyware - software that tracks and sends personally identifiable information to third parties
- Phishing a fake website that looks like the real website

Governments and businesses provide online help to users on how to avoid becoming a victim of cybercrime, Fig. 2 below is an example from the Illinois State Police that gives users advice on how to avoid being scammed out of their money. Access the website and click on the link for more information - this page is available in English only (<http://www.isp.state.il.us/crime/avoidscamtips.cfm>)



**ILLINOIS STATE POLICE**

Leo P. Schmitz, Director

### Tips to Avoid Being Scammed

The object of any con game is to entice an unsuspecting person to part with their money or other items of value. Most con games are initiated by people who approach potential victims on the street or call them on the phone.

Each person should be suspicious of ANY plan, idea, scheme, business deal, or any proposition that requires you to provide your money on short notice. The following tips are intended to improve your chances of not being a con's next victim:

- **REALIZE** scam artists are professionals - everyone is a potential victim.
- **SUSPECT** all "Get Rich Fast" schemes.
- **ALWAYS** lock your doors when doing yard work, getting the mail, or anytime you go outside - both the front and back doors.
- **NEVER** allow strangers inside your home.
- **ASK** "officials" to produce identification, and confirm their alleged employment.
- **CONTACT** the utility company by telephone if any purported city employee wants to enter your home, or requests you to go outside with him/her.
- **DISPLAY** "No Solicitation" and "Beware of Dog" signs near your residence door.
- **BE WARY** of any unexpected contact with strangers (in person or on the telephone).
- **SUSPECT** all "Door to Door" sales solicitations.
- **BEWARE** of unsolicited home repairmen. If you need the services of a home repairman, check first with the county, township, city building officials, the Better Business Bureau, or Office of the Illinois Attorney General to confirm they are legitimate. Be suspicious of anyone knocking at your door asking to make repairs to your home and/or asking to pave or seal your driveway.
- **CHECK** the Better Business Bureau to see if complaints have been filed against the person or business you are considering.
- **ASK** for references and call them.
- **GET** several repair estimates and compare prices.
- **TALK** with a trusted friend or relative before making major money decisions.
- **BE SUSPICIOUS** of high pressure sales tactics.
- **PAY BY CHECK** so you can stop payment if dissatisfied; **NEVER PAY CASH.**
- **PRINT "Deposit Only"** on the back of personal checks to create a "paper trail".
- **BE SURE** the work is completed to your satisfaction before you make final payment.
- **REQUIRE** a guarantee on the work.
- **REMEMBER**, you have **three days** to cancel a contract for home repairs if you signed the contract at your home.
- **NEVER** sign any contract or agreement without carefully checking it.
- **BE SURE** you understand and agree to all provisions in a contract or agreement.
- **WRITE DOWN** the license plate number of any suspicious vehicle(s) the suspect(s) may be operating.
- **CALL YOUR LOCAL LAW ENFORCEMENT AGENCY TO REPORT THE INCIDENT!!!**

Fig. 2 Illinois State Police - Avoid Being Scammed

### **2-1-1-3 Understand what identity theft means, and what the risks are.**

Identity theft occurs when your personal details (such as your name, date of birth, current or previous address) are stolen, and identity fraud occurs when these details are used by someone else in a criminal activity. If you are a victim of identity theft, it can lead to identity fraud which can have a direct impact on your personal life and make it difficult for you to conduct your day to day routine such as using your credit card until it is resolved. Fraudsters can use your personal details to open bank accounts, obtain credit cards or loans, order goods in your name, or take out mobile phone contracts. The first time you may be informed of this activity is when you receive bills or invoices for things you have not ordered, or when debt collectors want you to pay debts that are not yours.

To protect yourself make the following activities a regular habit:

- Shred any documents containing your personal or financial details before you throw them out;
- If you receive unusual emails from your bank asking for your security details never reveal your full password or login details;
- If you are concerned about the source of a telephone call claiming to be your bank, hang up and ring the bank back;
- Check your bank or financial statements carefully and report anything suspicious to your bank or financial services provider;
- Dispose of old computers/smartphones by physically destroying the hard drive or equipment;
- Comply with social networking sites' privacy rules;
- Be cautious when providing personal information online or on your smartphone;
- Be wary of anyone asking for your bank or credit card details;
- Only use secure sites when shopping online - secure sites should carry the padlock symbol or/and URL starts with (https), so that you know you can enter your details in confidence (see example in Fig. 3 on the next page);
- When choosing a password avoid obvious choices, such as your mother's name, a child's name, or other reference that someone could easily guess or find; try to use a random combination of upper and lowercase letters and numbers.

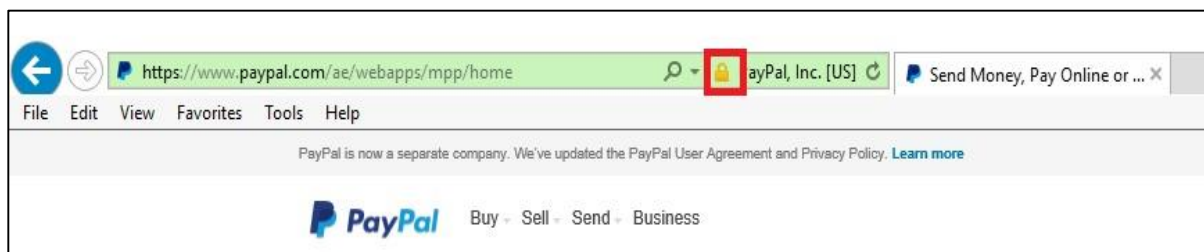


Fig. 3 Internet Explorer - example of the padlock symbol

#### **2-1-1-4 Be aware of scams and frauds such as: Phishing, Pharming, and Hacking.**

Phishing is a type of scam that targets information. For example, you, along with thousands of others, get an email that appears to be from your bank or an online payment company. It does not matter that you do not have an account with that organisation, the chances are that someone on the large mailing list will. The email explains that there has been a security problem and asks you to confirm your login details. There is a link embedded in the email to take you to the website. But it's not the real website! You end up on a very clever, authentic looking, replica website where everything you type in, including your username and password, is recorded. The thief now can access your account and you will have to prove that somebody else was using your username and password without permission.

Genuine emails will address you by name, not as "Dear Customer" or some general format. Phishing emails often have spelling and grammar errors and the link provided will usually send you to a different URL than the one spelled in the email.

In Europe, Middle East and Africa phishers (those who send phishing emails) are turning to more sophisticated scams like spear phishing, which is when you receive an email that appears to be from someone you know - it is actually from a criminal who wants your credit card and bank details, passwords and the financial information stored on your PC, laptop or smartphone.

Be cautious - do not post too much personal information on social media sites. If a friend emails you asking for a password or other information, call that friend or send a separate email to verify it is authentic.

Pharming is when a criminal hacks into a genuine website and re-directs all traffic to the bogus replica website - the user might be convinced that the website is genuine and can be tricked into providing personal information. Even if you type a genuine web address in your Internet browser, a pharming attack could redirect you to a fraudulent website.

Hacking is accessing other people's computer systems by breaking into a security system. The first hackers did it to prove it could be done and to show how clever they were but now hackers are focusing on stealing personal and financial information. Unauthorised hacking is a crime in most countries.

Here is an example of a major hacking incident:

Hackers broke into the massive hospital network of the University of California, Los Angeles, accessing computers with sensitive records of 4.5 million people. See Fig. 4 below and read the full story on the CNN Money website, (<http://money.cnn.com/2015/07/17/technology/ucla-health-hack/>)



Fig. 4 UCLA Health hacking attack



## 2-1 Identity

### 2-1-2 Authenticate

#### 2-1-2-1 Understand the concept of user authentication.

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service. The authentication typically uses confidential information and when you want to access the restricted service you must enter a username, which is a unique identification of a person and a password, which verifies that a user is who they say they are. See Fig. 5 showing Twitter's user login screen, asking for a username and password.

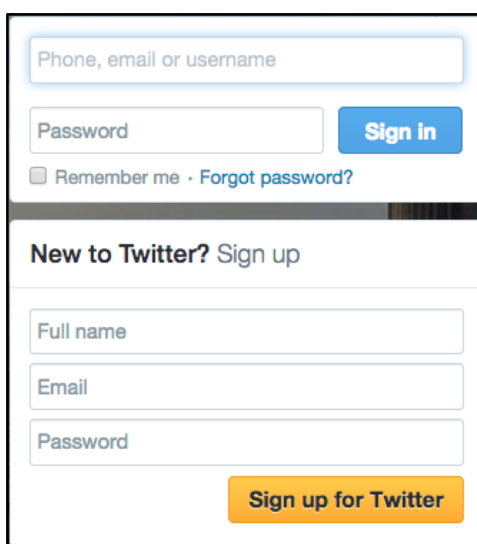
The image shows a screenshot of the Twitter login and sign-up interface. The top section is for logging in, featuring a text input field labeled 'Phone, email or username', a 'Password' input field, and a blue 'Sign in' button. Below these is a checkbox for 'Remember me' and a link for 'Forgot password?'. The bottom section is for new users, titled 'New to Twitter? Sign up', and contains three input fields for 'Full name', 'Email', and 'Password', followed by an orange 'Sign up for Twitter' button.

Fig. 5 Twitter's - user login

#### 2-1-2-2 Know how to develop good password practices; password length, mix of alphanumeric characters, change frequency.

Passwords should be at least seven characters long and contain a mix of: uppercase (A - Z), lowercase (a - z), numeric (0 - 9) and special characters (&, ?, \_ , ! , \$ , # , or %). A good password is a non-word made up by combining things you can remember. Bad passwords include names of family members, pets and sports teams – anything that can be guessed by somebody who knows you.

Note: Special characters (&?, \_ , !, \$, #, or %) are not always permitted in passwords on all websites due to system limitations.

Do not use the same password for different accounts. It is also good practice to change a password regularly; work-related passwords often have to be changed frequently.

### **2-1-2-3 Understand two-factor authentication: tokens, smart cards, biometric.**

The ways of verifying a person's identity fall into three categories. These are: something you know (*knowledge factor*), something you have (*possession factor*), or something you are (*inherence factor*). These categories are called authentication factor groups.

- Something you know could be a password, PIN, date of birth, or your mother's name.
- Something you physically have includes an ATM card, a smart card, or a security token.
- Something you are (also called biometrics) can be a fingerprint, face recognition, or voice print.

The two factors must be from two different groups. Three-factor authentication is considered the strongest and means providing one factor from each group. Two-factor authentication is more common but the two factors must be from different factor groups. To enhance security, combining at least two factors (e.g. what you know [i.e. your PIN] with what you have [your ATM card], further protects against fraud).

Example: Banks are more commonly using a security token like the one shown below as a second authentication factor. This token is a small piece of hardware with a digit display that is used to authorise a user.



## 2-1 Identity

### 2-1-3 Anti-Virus

#### 2-1-3-1 Understand the term 'virus' and distinguish between different kinds of viruses such as worms, Trojan Horses, etc.

**A computer virus** is a computer programme that can reproduce itself and spread from one computer to another via networks. It is capable of damaging the host system by destroying data or sending information to other systems; it could send itself to everyone in your email address book, and then repeat the damage. To combat viruses, anti-virus and anti-spyware software are helpful, but they must be updated regularly to ensure protection.

**Malware** is malicious software used by hackers to attack computer systems - worms and Trojan horses are two examples of malware.

**A computer worm** is a malware computer programme that duplicates itself and spreads via computer networks; it may generate email messages containing copies of itself. It consumes system resources, slowing or halting other tasks and can also open a back door for a hacker to gain control of the computer. The term 'worm' comes from a science fiction story called *The Shockwave Rider* written by John Brunner in 1975. The story is about a government that controls its citizens through a powerful computer network, a freedom fighter infests the network with a programme called a tapeworm forcing the government to shut down the network, thus destroying its base of power.

**A Trojan Horse** is another type of malware that does not duplicate but loads itself onto a computer by pretending to be a legitimate programme, such as a game or free software. Once loaded, it sits in the background and may be used to distribute junk email (spam) or to open a back door. The term 'Trojan' or 'Trojan Horse' is derived from the wooden horse story in Greek mythology that tricked defenders of Troy into taking hidden warriors into their city; Trojan horses present themselves as harmless, useful gifts in order to persuade victims to install them on their computers. Some operations that could be performed by a hacker using a Trojan horse include giving the hacker remote access, data theft, causing the computer to crash, modifying or deleting files, or keylogging. Examples are Netbus, Sub7, Beast, Zeus, ProRat, ZeroAccess. A keylogger is a hardware device or software programme that records the real activity of a user, including the keys they press on a keyboard.

Some other types of virus programmes:

- **Logic bombs/time bombs** - viruses programmed to initiate at a specific date
- **Macro viruses** - viruses that use another application's macro programming language to distribute themselves. They infect documents such as MS Word or MS Excel and are typically spread to other similar documents.
- **Polymorphic viruses** - viruses that not only replicate themselves by creating multiple files but also change their digital signature every time they replicate.

### 2-1-3-2 Understand the purpose of anti-virus software.

**Anti-virus software** is used to prevent, detect and remove malware including computer viruses, worms and Trojan horses from PCs, laptops, tablets and smartphones. Every computer or smartphone should have anti-virus software installed. Anti-virus software scans hard drives to detect malicious software programmes and can remove or quarantine viruses and worms; this process is sometimes referred to as disinfecting. The anti-virus programme works by identifying file patterns and file activity that indicates any kind of attack on the machine of any of the files stored on the machine.

There are many different anti-virus software programmes available. Some are free, but most of them must be purchased. If you buy anti-virus software, you will have to pay to keep it updated. Some suppliers provide a version of their software which is free for personal use, but it has less functions than the paid version. The software must be kept up to date with updates every few days at least to ensure that your PC, laptop, tablet or smartphone is protected against the latest malware.

Anti-virus blog websites keep users up-to-date with the latest information on viruses. For example, visit Antivirus-Blog.com (<http://www.antivirus-blog.com>) for more information and the latest security news posts, see Fig. 6:

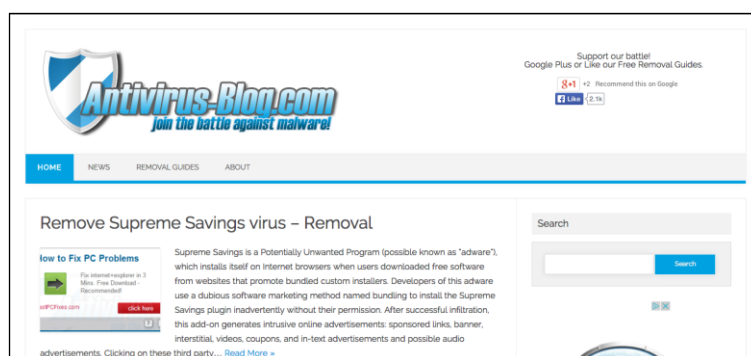


Fig. 6 Anti-virus blog - antivirus-blog.com

### **2-1-3-3 Understand the need to keep anti-virus software up-to-date.**

Most anti-virus software recognises viruses by searching for known patterns of programming code within files; these patterns are known as the virus signature. New viruses are constantly appearing so the creators of anti-virus software have to continually update their software to combat emerging threats. Usually the anti-virus programmes run updates automatically, with the anti-virus software provider updating the anti-virus programme that is stored on the user's PC, laptop, tablet or smartphone, to make sure that all the latest virus information is included and the user's data is protected.

### **2-1-3-4 Understand what a Firewall does and why it is necessary.**

Connecting a computer to the Internet makes it visible to every other computer on the network, when you connect to the Internet your computer is identified by a unique number - the IP (Internet Protocol) address and is potentially viewable by anyone else on the Internet.

This presents an opportunity for remote misuse by someone who wants to access your personal information and data. A firewall is a software or hardware-based system that controls the flow of communications across networks of computers by examining their source, destination and type - and comparing these with predetermined lists of allowed and disallowed transactions. It blocks or permits access to your computer, giving you increased security as it can hide your computer from the Internet and detect illegal attempts to access your computer and data.

## 2-1 Identity

### 2-1-4 Anti-Spyware

#### 2-1-4-1 Understand the term 'Spyware', and the risks associated with Spyware.

Spyware is a name for malicious software that collects information about the use of the computer without your knowledge. It can come bundled as a hidden component of free programmes downloaded from the Internet and can track your movements on the web for advertising purposes. Some spyware may include a keylogger to capture everything entered through the keyboard, (including the recording of passwords and credit card numbers) and sends the information to criminals. A keylogger is a hardware device or software programme that records the real activity of a user including the keys they press. Most anti-virus software will also remove spyware.

#### 2-1-4-2 Know how to run anti-Spyware software, and how to remove Spyware from your computer.

Running anti-spyware is similar to any other anti-virus software. These programmes normally run in the background and monitor any suspicious activity.

#### Exercise - Run an anti-spyware software scan

To run a scan you will first need to check that you have anti-spyware installed on your computer.

1. Look for the anti-spyware icon on the taskbar; it may be part of your anti-virus programme.
2. Double-click on the programme icon in the taskbar
3. Select Scan or Scan Now from the menu
4. Click on Full Scan, then OK.

If any spyware is found, you will be given the option to delete the offending programme or move it to quarantine.

### **2-1-4-3 Recognise the warning signs that Spyware may be on your computer.**

Any or all of the following can be signs that your computer is infected with spyware:

- Your browser homepage has changed to an unknown site without your knowledge
- Your computer starts crashing, freezing or locking up, but you have not changed anything recently
- Strange emails appear in your 'Sent' folder that you didn't send
- You notice a lot more pop-up ads when you are browsing
- The hard drive is running, even when you are not on the computer. Or it could be running very slow while using it
- There are additional toolbars in your browser that you cannot remove
- You conduct a web search, but another browser or search engine completes the search
- Mysterious files appear on your computer system

If you suspect your computer is infected with spyware, access your anti-spyware programme and run a scan, this should identify spyware and give you the option of deleting it or moving it to quarantine.



# Quiz

**Q1.** Following the theft of your laptop an unexpected charge has been made on your mother's credit card. What may have happened?

- a. Phishing
- b. Pharming
- c. Identity theft
- d. Spyware

**Q2.** An email message has just come into your older brother's inbox. It seems to be from the bank, looking for him to re-enter password details, but there are spelling and grammar mistakes, and you are suspicious. What might this be?

- a. Phishing attempt
- b. Virus
- c. Hacking attempt
- d. Hoax

**Q3.** Which password is considered the safest?

- a. latitude
- b. Lat1tude3#
- c. LATITUDE
- d. latitude5

**Q4.** Which authentication method is based on biometrics?

- a. PIN
- b. ATM card
- c. Fingerprint
- d. Mother's name

**Answers Overleaf**

# Answers

---

**Q1. c. Identity theft**

**Q2. b. Phishing attempt**

**Q3. b. Lat1tude3#**

**Q4. c. Fingerprint**

## Chapter 2-2

### Secure

**2-2-1 Backup**

**2-2-2 Email**

**2-2-3 Wireless**

**2-2-4 Physical**

**2-2-5 Smart Devices**

## 2-2 Secure

### 2-2-1 Backup

#### **2-2-1-1 Understand what the term 'backup' means, and why a regular backup routine is important.**

Backup refers to making copies of your data for recovery in case of loss. There are many ways in which data could be lost. Accidental deleting, corrupt hardware, natural hazards such as fire and water damage, virus attacks, theft, loss, and many more. Accidentally deleting files typically places the files in the recycle bin, which can be recovered easily enough, but if not, recovery can be a time-consuming task with no guarantee of success. If files have been deleted in a virus attack, there is very little chance of getting them back. Hard disks do fail from time to time and in the case of equipment failure, recovering data will require professional assistance and will be costly.

Your school should have a backup procedure that outlines a regular plan of copying and backing up important data and program files. Many schools' backup procedures cover the basic requirements: essential school programs, information and data (including students' grades, attendance and other personal information). If your school does not provide backups for the files you create in your classroom, it is recommended to make backup copies of your lesson plans, curriculum resource pages, handouts, tests, and other types of files that represent years of work.

Data loss is unpredictable, so you should always have an up-to-date backup. The best way to be sure is to have a regular backup schedule. The more often you back up, the less data you will lose. A few minutes spent once a week is much better than having to rewrite a month's worth of work reports, or losing your exam questions, or rewriting progress reports for every student in your class.

Most computers have their own backup programs; Fig. 7 on the next page shows an example of a Backup Process in Windows 7 that gives you information about backup options.

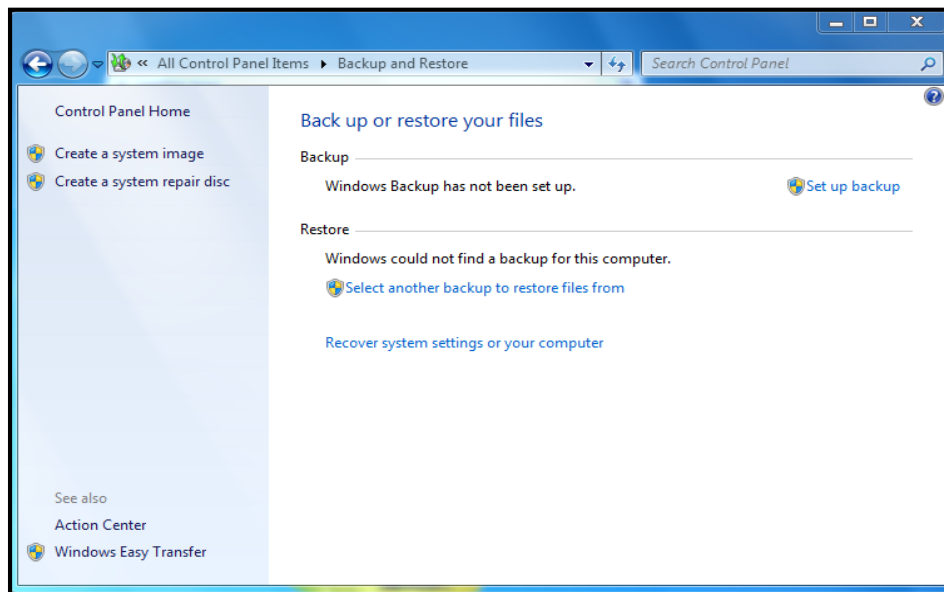


Fig. 7 BackUp Manager Example

### 2-2-1-2 Recognise common backup devices: Cloud Storage, USB Drives, External Hard Drives, and be aware of different capacities.

The easiest and most feasible way to back up your files is to copy your files (documents, pictures, photos etc.) through a USB flash drive, an external hard drive or a cloud storage application. USB flash drives are usually small in size and can hold gigabytes of information. External hard drives are a more expensive option but can be used to back up everything on your computer, including your computer's entire hard drive, programs and operating system. Cloud storage enables you to upload, store and access data online; for example, you can save something using cloud computing on one device, and you can easily access it on your phone.

Table 1 below illustrates the typical maximum storage capacity of common storage devices:

Device	Maximum Storage Capacity
External hard drive	Up to 2TB or more
USB flash drives	Commonly up to 128GB
Cloud storage app	Up to 15 GB for free; varies if more space needed

Table 1 Storage Capacities of Common Storage Devices

Regardless of where you back up your data, it should be kept at a separate location from the originals, in case of a fire or flood for example. If such a disaster occurs, all of your data could be lost if it is stored in one place.

### 2-2-1-3 Understand what cloud-based backup entails.

Cloud computing is the use of computer resources that are delivered as a service over a network - typically the Internet. The name comes from the common use of a cloud shaped symbol that is used to simplify complex situations. Users access cloud-based applications through a web browser or mobile app and the user's data is stored on servers at a remote location. Users normally have a limited amount of free storage space, when that is used up the providers charge a fee. Paid services offer more storage and often special backup software to automate the process. The benefits of cloud storage are that it is inexpensive - often free, is readily accessible from a range of devices, has automated backup and recovery systems, is ideal for collaboration purposes, is more secure as backups are physically removed from original files, is invisible – has no physical presence and allows for automatic updates of your files across all of your devices.

Some examples of free/paid services are: Just Cloud ([www.justcloud.com](http://www.justcloud.com)), Dropbox ([www.dropbox.com](http://www.dropbox.com)), and Google Drive (accessible via your Gmail account).

Fig. 8 below illustrates Just Cloud's sign-up service that enables access to your files from anywhere:



Fig. 8 Cloud-based storage - Just Cloud (<http://www.justcloud.com/>)

### **2-2-1-4 Use backup features on your computer, and understand what it means to restore a backup.**

Operating systems have different options for backups; the following exercise takes you through the steps to complete a backup on a Windows 7 computer:

#### **Exercise - Complete a Backup on a Windows 7 Computer**

1. Click the Start button and open the Control Panel.
2. Select 'Backup and Restore'.
3. Specify the device to store the backup and what folders and files you want to backup.
4. Click on 'Backup Now'.

#### **Restore files from a backup**

You can restore backed-up versions of files that are lost, damaged, or changed accidentally. You can also restore individual files, groups of files, or all of the files that you've backed up. In order to have the option of restoring your files you should ensure that you backup regularly.



## 2-2 Secure

### 2-2-2 Email

#### 2-2-2-1 Understand the concept of junk/spam email and the need to filter email.

Spam is usually considered to be unsolicited electronic junk mail or junk newsgroup postings - generally it is unwanted email that is advertising a product or service from a company or website.

Internet Service Providers (ISPs) block most spam messages before they reach your inbox by using 'spam filters': software programmes which sort incoming email to identify and prevent junk/spam getting to your inbox. Even so, lots of junk email passes through the ISP filters cluttering your inbox that you could easily miss messages from friends or colleagues. Fortunately, most email software can filter unwanted messages as they arrive and you can set rules to send unwanted messages to a junk/spam folder and thereby blocking future emails from the same sender.

#### 2-2-2-2 Turn on the spam filter in your email.

The method for turning on spam filters varies depending on your email program. In Windows Mail, right-click on the message and select Junk Mail. You can then mark the message as junk and block further emails from the sender or from anybody with the same email address. Most online email systems also have options to filter spam and for reducing spam. Gmail promises less spam through their email filters, seen in Fig. 9 below:

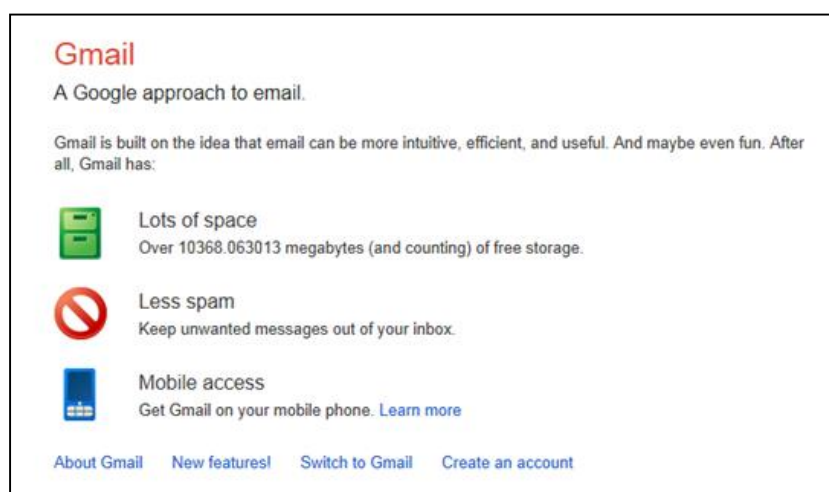


Fig. 9 Gmail - Less Spam

### **2-2-2-3 Set Spam filter rules.**

By setting up filters on your email account, you can automatically mark all messages from a certain sender or with a certain word in the subject line. Marked messages can then automatically be deleted, or marked as read, or copied to a certain folder.

## 2-2 Secure

### 2-2-3 Wireless

#### 2-2-3-1 Understand what a wireless or Wi-Fi network is.

Wi-Fi is a type of wireless local area network (WLAN). Wi-Fi is usually used to provide a connection to the Internet. Any Wi-Fi device can connect to the Internet via a wireless network access point. Each wireless network access point has a wireless range of about 20 meters and is known as a hotspot. The connecting device can be a personal computer, laptop, tablet, smartphone or video game console. Wi-Fi is widely installed in cafés, airports and many other public buildings and is often provided free of charge. Fig. 10 below shows an example of Wi-Fi Cafe spots in London, UK where the spots are listed and shown on a map.



Fig. 10 Wi-Fi Hotspots in London,  
(<http://www.wificafespots.com/wifi/city/GB--London>)

You can also download an app for your smartphone from this site, which stores the locations of the hotspots.

#### 2-2-3-2 Recognise the advantages and risks associated with using public Wi-Fi hotspots.

Public Wi-Fi hotspots are widely available in urban areas some of which are provided free of charge. If the hotspot is provided by a business such as a café, or airport for its patrons, there may be a charge for the service.

### **Advantages**

- You can use your laptop and smartphone to access the Internet. Using your own device in a hotspot gives you easy access to the World Wide Web and all your online accounts.
- A hotspot is a convenient place to check your email for important updates while you're on the go. Many coffeehouses, bars and restaurants offer hotspots, so you can get something to eat or drink while you go online.
- Hotspots at airports are convenient because people can access the Internet before boarding a flight when they usually have to turn their device off for the duration of the trip.
- If you're staying at a hotel that has a hotspot, typically you can use the Internet in your room without having to go to the lobby or an Internet cafe.

### **Risks**

- Data sent over public Wi-Fi hotspots can be intercepted by anyone else logged onto the network. Criminals can set up fake free Wi-Fi hotspots in public places and use them to steal personal information, such as usernames and passwords.
- Public Wi-Fi networks often have no security and can easily be intercepted.
- If too many people are using a particular hotspot, it could become overloaded which would affect performance and you may lose the connection.

### **2-2-3-3 Recognise the security advantages of using the latest WEP or WPA wireless protocols.**

Domestic/private Wi-Fi hotspots are generally secured by a password, also called a wireless security encryption key to ensure that access is only available to authorised users. Encryption is the process of converting data into a form that cannot be easily understood by unauthorized people, such as hackers. Most Wi-Fi hotspots do not encrypt the information you send over the Internet and are not secure. If you regularly use the Wi-Fi hotspot to access online accounts, consider using a Virtual Private Network (VPN) to encrypt traffic between your device and the Internet.

There are two encryption standards for Wi-Fi networks. The original wireless encryption-the standard, Wired Equivalent Privacy (WEP)-was easy to get around and has been replaced by Wi-Fi Protected Access (WPA and WPA2) encryption.

These security measures help to ensure that you can access the Internet safely, keeping your personal information and data safe.

## 2-2 Secure

### 2-2-4 Physical

#### **2-2-4-1 Recognise physical security considerations around laptop, tablet usage.**

Security when using a portable computer such as a laptop or tablet is not just concerned with passwords, back-ups and encryption. Because of their size, laptops and tablets are vulnerable to loss and theft. If they are left on car seats or unattended in public Wi-Fi hotspots, they make an inviting target for a thief who can quickly carry them away.

#### **2-2-4-2 Know how to minimise risk associated with theft or loss: keep device in view, use a security cable (if appropriate), password protect, note serial number, use security pen marker.**

There are some basic precautions that you can take to reduce the risk of losing a portable computer through theft or carelessness.

- Always keep the device in sight and leave it in a visible area to deter possible thieves. If possible, remain in physical contact with it at all times.
- Attach a security cable, privacy screen or security alarm to your laptop – most thieves will look for an easier target. Fig. 11 shows a typical example of a cable lock:



Fig. 11 a typical security lock fitted to a laptop

- Add conspicuous labels with your name, this will deter a potential thief and aid recovery if the worst happens.
- Make sure that all user accounts need a password so the thief cannot login to the computer.
- Make a note of the product code and serial number and keep them in a safe place, not in your laptop bag.
- Write your contact information on the computer using an anti-theft pen that will show up only under ultra-violet light.

### 2-2-4-3 Recognise security issues around disposal of computers and the importance of data removal before disposal.

We all enter personal information on our computers, but even if you were careful and deleted it immediately sometimes data can still be recovered from your computer by someone using a data recovery program – even if you have emptied the recycle bin. Even reformatting the hard drive may not remove all data from the disk. Information that could be on your electronic device includes old emails and the contents of your browser cache. Since you do not know who will next own your computer, you do not know how they may use that information.

The surest way to make sure that no personal data remains is to remove the hard drive and destroy it physically but this will leave the computer unusable. The next best option is to use a file shredding programme, one free version is called File Shredder, which will overwrite all the free space on the disk to military standards, see Fig. 12 below which shows the File Shredder Download screen - <http://www.fileshredder.org>

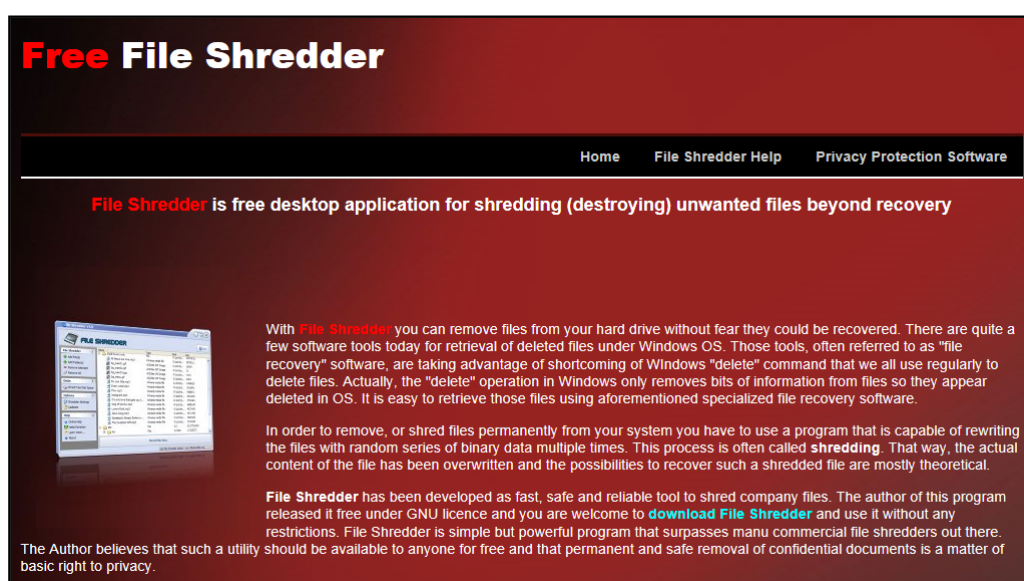


Fig. 12 File Shredder Download Screen



## 2-2 Secure

### 2-2-5 Smart Devices

#### **2-2-5-1 Recognise what information your device contains and shares online and how it could be misused.**

Today your smart device barely leaves your hands and definitely does not leave your sight for most of the day. That means your interactions throughout the day have something to do with your smart device, typically a phone. That also means that a lot of information is saved on that device. Information could include messages, emails, pictures, videos, contacts, passwords, and applications.

This information can easily be shared online through messaging apps, chats, emails, and sometimes in the background through applications installed on the device. More on downloaded apps can be found in Section 2-2-5-4. Information in the wrong hands can be misused to bully, embarrass, and commit crimes such as identity theft.

An example of such a hazard could be the theft of your device allowing the thief to obtain your personal details through saved information that is not protected. It could be your physical address, access to your email that provides an easy and quick way to reset passwords on any online account, or use of other confidential or financial information.

#### **2-2-5-2 Be aware of basic security features: password protect device, set automatic locking facility, install security software, install operating system updates, mobile tracking.**

From the previous example, it is quite evident that the uses of the built-in basic security features are a means for protecting your information. There are a few mentioned in this section and there are applications available online providing additional securities as well.

First and foremost, you must password protect the device as soon as possible. This process is typically done through the 'Settings'/'Options' menus of your smart device. Make sure the password you create is strong enough to avoid someone cracking into the device.



Setting an automatic locking facility through your smart devices settings/options menu will create a rule locking your device after a certain period of time. There are security software applications available for installation that will also lock your device upon leaving a designated safe location such as your home or office, which make for great tools in case the smart device is stolen.

Updating your smart device's operating system is also vital for security purposes. These update patches are provided when flaws are discovered in the software. The updates repair the possible security holes.

Mobile tracking is another important tool that assists in locating your smart device. Typically this service is provided by your phone manufacturer, but your mobile provider and third party app developers can also do the same. This service obtains the current location of your smart device by using the radio towers on your smart device network or through the device's GPS signal. Once this position is obtained you can then proceed to the location (if you forgot it in your office) or sometimes there are available options to lock or completely wipe (full delete) the device in the event that it is suspected to be have been stolen.

### **2-2-5-3 Know how using encryption on your smartphone can help prevent data theft.**

Most smart devices have the option to encrypt data. Encryption stores your data in an unreadable and scrambled form. In Android phones the PIN must be entered upon powering up the phone and unless someone has the correct password or pin the data is unusable and this will help protect the sensitive information stored on the device. Every time the phone is locked the data remains encrypted until the correct password is entered.

Note that using encryption will slow your device's performance due to the added load on the processor to encrypt and decrypt the information stored. This is highly recommended for corporate devices to protect data from corporate espionage.

### **2-2-5-4 Be aware of security issues with apps. Only download apps from approved sources, check apps permissions.**

Applications for smart devices are one of the greatest inventions of this century. We have applications like WhatsApp for messaging, Facebook & Twitter, and others to make our lives more convenient. Unfortunately, when applications are installed on your device, they also potentially open an access door to your device and the information store within it.

Downloading applications from trusted sources such as the iTunes store for Apple products, or the Google Play store for Android devices reduces the risk of someone abusing this access.

To provide additional security against misuse, every user should take the time to read and understand the application permissions that are accepted prior to installation. See Fig. 13 as an example showing an application that is requesting permission to locate your device using the built in GPS (Global Positioning System) at any time.

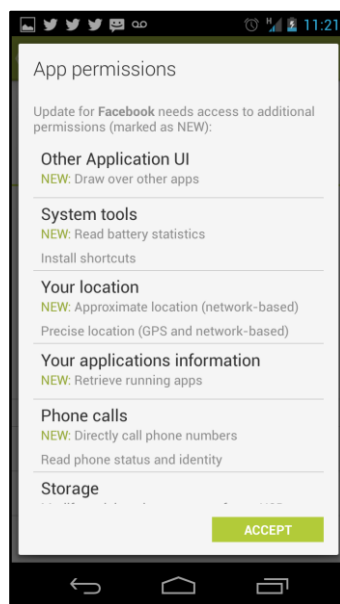


Fig. 13 App requesting access to your GPS

### **2-2-5-5 Be aware of viruses on mobile operating systems and mobile malware.**

A mobile malware is software that targets mobile devices with the intent to damage or leak confidential information. Just like all devices connected to the Internet, your mobile smart devices are susceptible to virus attacks and malware similar to those that attack your computer.

Mobile malware continues to be on the rise and does not seem to be slowing down. An article by Forbes stated that 200 new threats are created every minute. (<http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/> )

Therefore it is recommended to install antivirus applications that will protect your device from such attacks.

### **2-2-5-6 Be aware of security threats arising from unsolicited email or text messages. Recognise symptoms of malicious software infection: unusual data charges on bill, unexplained changes in user interface.**

Unsolicited email and text messages are also called spam. They normally come with advertising content that might be malicious. They might have a link to a website that could have criminal intent or an included attachment, which could be a virus.

The majority of mobile malware can be divided into three main groups: 'SMS Trojans' (which drain mobile accounts by sending SMS messages to premium-rate numbers); 'Backdoors' (which provide unauthorised access to a smart device making it possible to steal data, change settings or install malicious programs); and 'Spyware' (which collects data from the mobile device, including contacts, passwords, or even photos or video).

### **2-2-5-7 Know how to turn off automatic Wi-Fi and Bluetooth functions to prevent unauthorised access to your device data.**

Bluetooth is a low-power, low-cost wireless technology for connecting devices over short distances. It is commonly used to connect hands-free headsets to mobile phones. When you turn on Bluetooth on a mobile phone under 'Settings – Wireless & Networks', you must then scan for devices that will check for other Bluetooth devices within range. Select the device you are interested in and pair with the device. When you are finished, turn off Bluetooth by selecting 'Settings' – 'Wireless & Network' – 'Turn off Bluetooth'.

There is an option available on smart devices that permit other devices to find your device. Keeping this option toggled on can expose you to risks of hacking using the Bluetooth technology. It is recommended that you turn that feature off after pairing a device.

Wi-Fi connections are also similar to Bluetooth but more powerful and therefore extend the range as well as the possible risk. Almost all smart devices now use Wi-Fi technology to connect to the Internet. Connecting to Wi-Fi technology that is 'open' meaning it does not have a password is the most risky since there might be many devices logged on that are unknown to you. Using certain software, someone might be able to access your smart device and the information stored within. This is why it is very important to regularly back up your smart device data to avoid loss through theft or attacks.

### 2-2-5-8 Know how to delete all personal information when disposing of device.

If you are thinking of upgrading or replacing your mobile device, there are three important steps to take before you resell or recycle your old device. The first step is to back up or transfer your personal information to your computer or new mobile device. The second is to wipe or factory reset your device. This is sometimes called a hard reset and it essentially deletes all the memory and information to bring the device back to its original factory state. In some cases this also removes third party applications. If not, ensure you uninstall applications following instructions from your mobile device manufacturer. The third and final step is to remove or delete the external storage card, typically named 'SD' card.

To perform a hard reset, use the Internet to locate instructions specific to your mobile device that will detail the process and explain the extent of information deleted.

Fig. 14 below provides an example using an iPhone mobile smartphone.

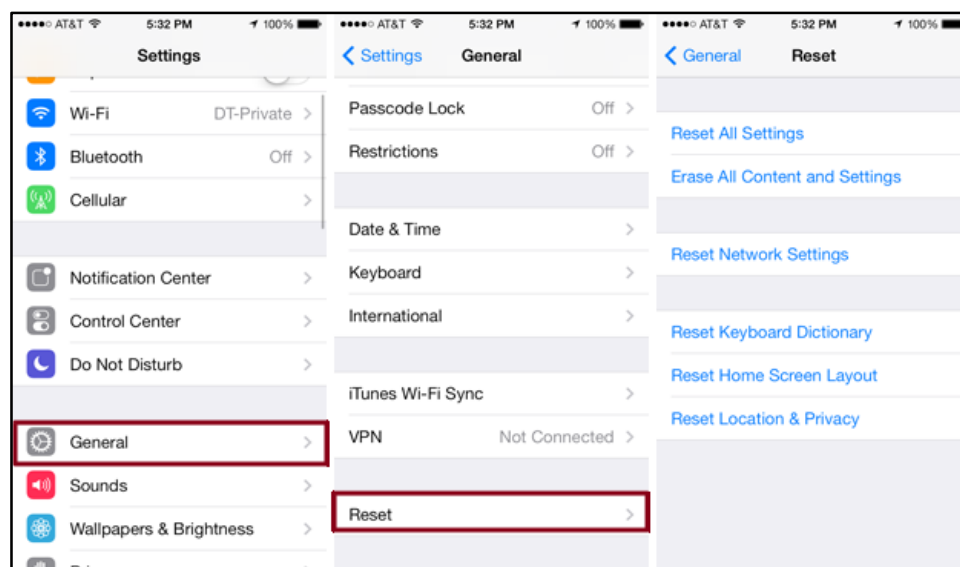


Fig. 14 Hard Reset in an iPhone smartphone

### 2-2-5-9 Know how to enable and disable location settings. Understand the advantages and risks of enabling location settings.

Most of the recent mobile smart devices have built-in GPS that provides an accurate location of your device using both cellular and satellite services. This feature allows manufacturer and third-party applications to use this location technology to provide location-based services.

Use the 'Settings' menu on these smart devices to enable or disable this service.

Advantages of enabling location services:

- Emergency services allow responders such as an ambulance or the police to more easily locate you.
- Theft recovery in the event your device is stolen; you could locate the phone using built-in or third-party applications.
- Location based social networking, which allows friends to connect if they are in close proximity such as visiting the same café or mall.
- Receive directed adverts and promotions relevant to your specific location.

Disadvantages of enabling location services:

- Battery drains much quicker when your smart device GPS is running.
- Third party applications might inundate your mobile phone with messages and push notifications. This could just be a nuisance to you but it will also eat up your data allowance for the month.
- Privacy is potentially given up because spying can occur by anyone that has or can gain access to your location using the Internet. This could occur from a virus that is installed on your device or from the multitude of applications installed as well.

**2-2-5-10 Only share your mobile number with people you know and trust. Keep a record of your IMEI number in case your phone is lost or stolen.**

Your mobile number is the door to your private and professional life. In some cases there are two separate numbers, but for a lot of people it is a single number. If your number gets in a telemarketer's hands, a flood of marketing and promotional calls will start to come in. Great examples of this are the contests that occur at the malls and petrol stations around the region. You are typically asked to provide your name, email and phone number in the event you win a prize such as a new car. This is strictly used to market products for the vendor and for other partnering companies. Next time you provide your information in such a contest consider what might be the consequences.

Every smart device that has a built-in phone or GSM modem must have an IMEI number. This is the International Mobile station Equipment Identification number that is 15 digits and is unique for each and every device. It is important to keep this number in your records at home or at the office should you lose the device or it is stolen. Using this number the local cell provider can put a block on that IMEI so that if someone else were to use the phone it would automatically disable the calls, or the local authorities could use it to positively identify your phone in the event it is found.

IMEI numbers are found on the original box the smart device came in and can also be found using the menu system on the smart device. As you might know by now, the 'Settings' menu is the most likely place to find this identification.

### **2-2-5-11 Know how to switch on the Internet filter to block inappropriate Internet content.**

Parents can set filters for what multimedia content their children can download on their phones. While content filters are more important for smartphones with full web access and video download capability, most mobile phones now have some kind of Internet browser. Content filters are not foolproof and inappropriate content can also be received via text/SMS, IM or email.

An example is on Apple's iTunes website (<https://itunes.apple.com/gb/app/k9-web-protection-browser/id407657840?mt=8>) you can download the K9 Web Protection Browser software for parental controls and Internet filtering, it is available for iPhones and iPads as a safe browser for the family. See Fig. 15.

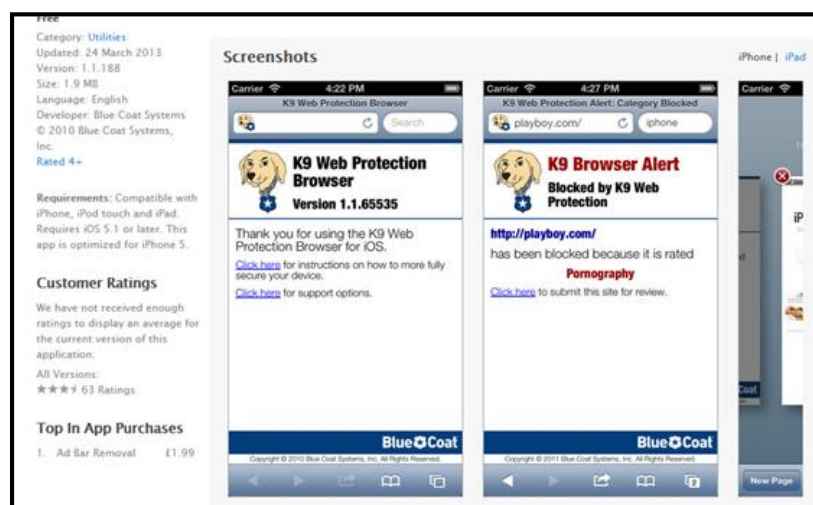


Fig. 15 iTunes K9 Web Protection Browser

# Quiz

---

**Q1.** What is the computing term for making copies of your files and information in case of loss or theft?

- a. Mirroring
- b. Locking
- c. Backup
- d. Duplicating

**Q2.** Which type of storage gives you the ability to access data online?

- a. Cloud-based storage
- b. Hard disk
- c. USB drive
- d. CD-ROM

**Q3.** What does spam email refer to?

- a. Sorted email
- b. Unwanted email
- c. Expired email
- d. Overdue email

**Q4.** True or False: Public Wi-Fi hotspots are a good place to conduct online banking.

- a. True
- b. False

---

**Answers Overleaf**

# Answers

---

**Q1. c. Backup**

**Q2. a. Cloud-based storage**

**Q3. b. Unwanted email**

**Q4. b. False**



## Chapter 2-3

### Beware

**2-3-1 Online Risks**

**2-3-2 Shopping Online**

**2-3-3 Paying Online**

## 2-3 Beware

### 2-3-1 Online Risks

#### **2-3-1-1 Recognise the risks in everyday use of the Internet: email, web browsing, online banking, online shopping, social networking etc.**

We use the Internet as part of our everyday lives and we need to be aware of the risks involved in using email, web browsing, banking and shopping online and using social networks.

Here are some examples of the risks faced when online:

- Receiving and responding to spam;
- Responding to emails which are scams or can lead to a hacker gaining control of the computer;
- Exposing personal information;
- Becoming the victim of cyberbullying;
- Infecting the computer with viruses;
- Exposing personal and financial information that could result in identity theft;
- Being the victim of scams or hacking;
- Buying goods that do not actually exist;
- Identity theft;
- Exposure to inappropriate content, such as pornography, racism or online radicalisation;
- Posting personal information that can identify and locate a child offline;
- Inadvertent involvement in making or distributing illegal or inappropriate content

#### **2-3-1-2 Recognise how pervasive inappropriate material is on the Internet.**

According to *Digital Journal*, “Investigators say 30 percent of all web traffic is [inappropriate content]” (<http://digitaljournal.com/article/322668#ixzz2RT1tY9cS>) and according to the statistics, the only sites that surpass the biggest explicit material sites in traffic are sites like Google and Facebook. Aside from inappropriate material, there are many websites that contain material that is offensive and not suitable for both adults and youth. These include websites that incite racial hatred and other discriminatory behaviour as well as those that promote adult material. Many people receive spam that includes hidden links to websites that contain offensive material - blocking spam and junk mail was covered in Section 2-2-2 Email.

The Information Technology and E-commerce Council is in 2004 preparing a new Cybercrime Bill. The existing Sec 33. Penalties are no longer sufficient. Philippines Republic Act No.8792 is an act provided for the recognition and use of Electronic Commercial And Non-Commercial Transactions, penalties for unlawful use thereof, and other purposes. Fig. 14 below is a graphic from the article. The full article can be found at (<http://www.cybercrimelaw.net/Phillipines.html>)

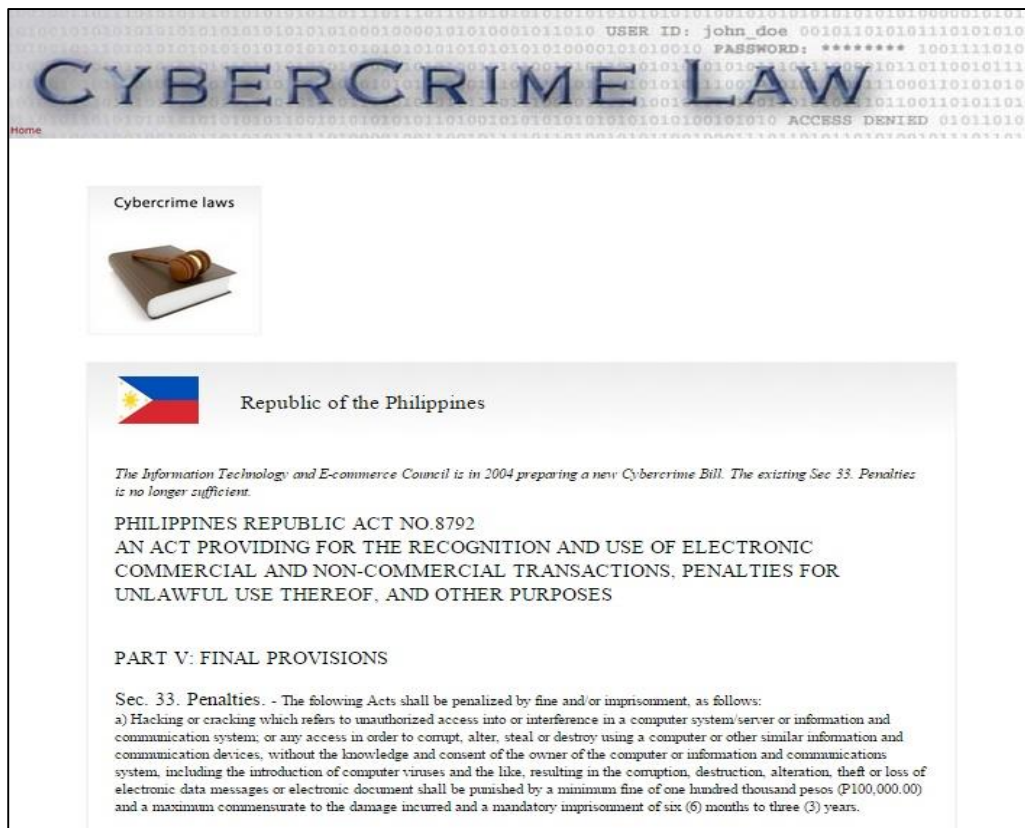


Fig.16 Graphic from the cybercrime law article about a new Philippines Republic law on cybercrimes

### 2-3-1-3 Be aware of common threats: recognise suspicious email requests, potentially malicious websites.

The most common source of threats is from email. We do not have to search out trouble, spammers can get a hold of our emails addresses and target us.

There are a number of things we can look out for such as:

- Emails asking for your bank details because you have won a prize in a competition you didn't enter, or
- A philanthropist has picked you at random to run his charity emails with links to websites where the web address differs from link text.
- An email message from a bank or other online vendor asking you to re-enter and validate your username and password details may often be fraudulent; always be cautious if you are asked to enter this information.

Anti-virus and anti-spyware, covered in Sections 2-1-3 and 2-1-4, should be installed on your computer to give you some protection against spyware and malware that could lead you inadvertently onto potentially malicious websites.

## 2-3 Beware

### 2-3-2 Shopping online

**2-3-2-1 Know how to protect yourself before shopping online: use the most recent version of your browser, ensure your anti-virus software is up-to-date, etc.**

It makes sense to take basic precautions to protect yourself before shopping online. Hackers are continually looking for weaknesses in browsers to exploit and developers are equally busy trying to close off these weaknesses. Make sure that you have the most recent version of your browser and turn on automatic updates to make sure that it stays up-to-date.

Microsoft (MS) Internet Explorer is a web browser that ships with MS Windows, and the updates are included when you install Windows updates. The following exercise demonstrates how you can install updates or set up automatic updates using MS Windows:

#### Exercise - Install Windows Updates

1. Left-click 'Start'.
2. Left-click 'All Programs'.
3. Left-click 'Windows Update'.
4. Left-click 'Install updates'.

The screen shown in Fig. 17 is displayed:



Fig. 17 Windows Update screen

You can change the settings so that the updates are done automatically, follow these steps:

1. Left-click 'Start'.
2. Left-click 'All Programs'.
3. Left-click 'Windows Update'.
4. Left-click on 'Change Settings' on the left side and you will see the screen shown in Fig. 18 below:

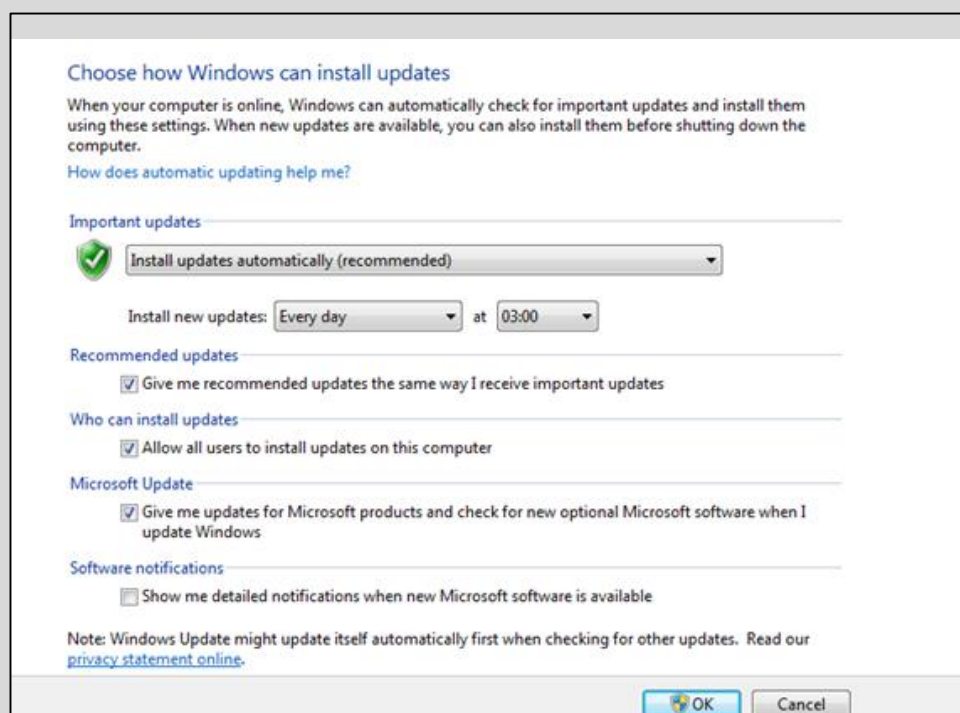


Fig. 18 Windows install updates automatically screen

5. Select a time for the updates to be installed, and then click 'OK'.

It is also vital to keep your anti-virus software up to date in order to provide the most complete protection. Thousands of new viruses are detected every year, not including the variants of new and existing ones. Each has a set of characteristics or signatures that enable antivirus software manufacturers to detect them and produce suitable resolutions through the updates.

### 2-3-2-2 Know how to identify a secure website: padlock icon on browser status bar, an 's' added after the http protocol in the URL.

If you are shopping online, you will need to enter your bank or credit card details to complete the purchase. You should ONLY enter bank or credit card details on secure websites. You can identify a secure website through two distinct methods. The first method is for the URL in the address bar of the browser to begin with 'https://', the key is the 's' at the end of 'http'. Unsecure website URLs typically begin with 'http://'. The second method, depending on the browser you are using, should show a lock symbol on the status or address line, click on the lock symbol to see the SSL digital certificate. SSL stands for Secure Sockets Layer, which is a type of encryption protocol over the Internet. Fig. 19 below shows an example of a shopping site (<https://en-ae.wadi.com/>), you can see https:// in the address bar which means that the website has secure checkout.

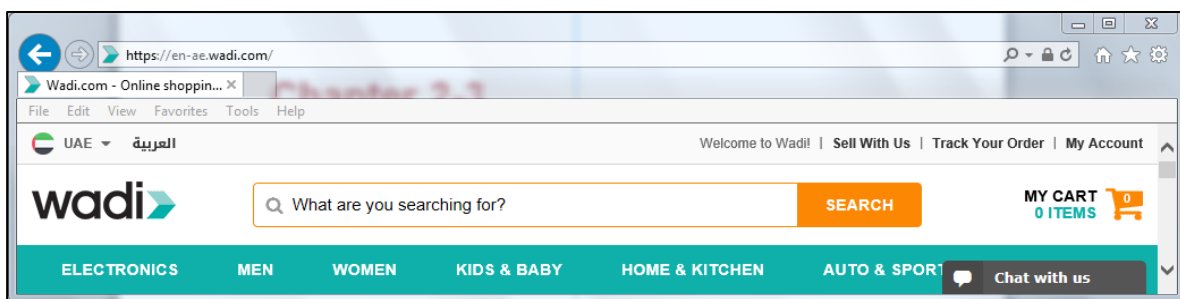


Fig. 19 Example of https:// in URL protocol (<https://en-ae.wadi.com/>)

### 2-3-2-3 Know about privacy policies.

Every reputable website will display its privacy policy; it is often a link at the bottom of the screen. The policy should tell you what information is collected, what it is used for and where to complain if you feel that your information is being misused. Fig. 20 is an example of a privacy policy from <https://en-ae.wadi.com/>, the same website as shown above in Fig. 19.

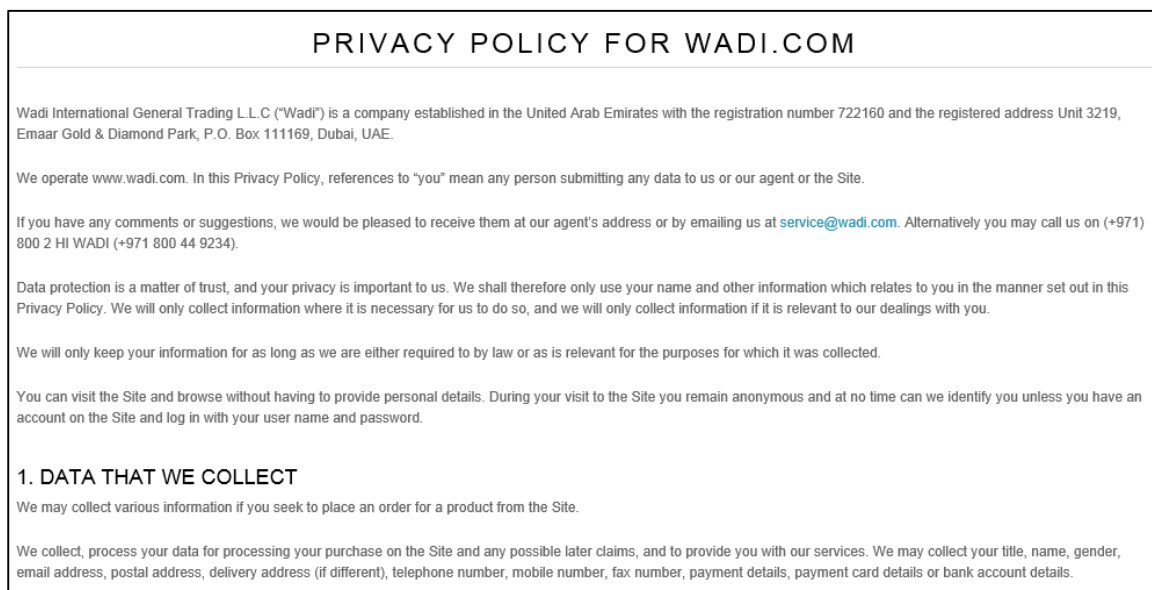


Fig. 20 Privacy Policy Sample (<https://en-ae.wadi.com/>)

### **2-3-2-4 Be aware of the information being collected to complete the transaction and determine if it is appropriate.**

A website should only ask for the minimum information necessary. Use common sense when entering your personal information online. For example, your postal address is required only if items are being shipped to you. A shopping website should never ask for information such as your date of birth, or mother's name which might be used in identity theft.



## 2-3 Beware

### 2-3-3 Paying online

#### 2-3-3-1 Be aware of safe payment options: credit card, debit card, etc.

Shopping websites usually offer a number of payment methods, use an online payment service if it is available, such as Prosum (<http://www.prosumfzc.com/>), see Fig. 19 below, or WorldPay ([www.worldpay.com](http://www.worldpay.com)). To use an online payment service, the buyer and seller generally set up accounts that allow them to make or accept payments. Buyers provide payment information, like bank account or credit card numbers, and sellers give information about where payments should be deposited. Another method of payment is wire transfer or credit transfer, which is a method of electronic funds transfer from one person or institution to another, an example is Western Union ([www.westernunion.com](http://www.westernunion.com)).

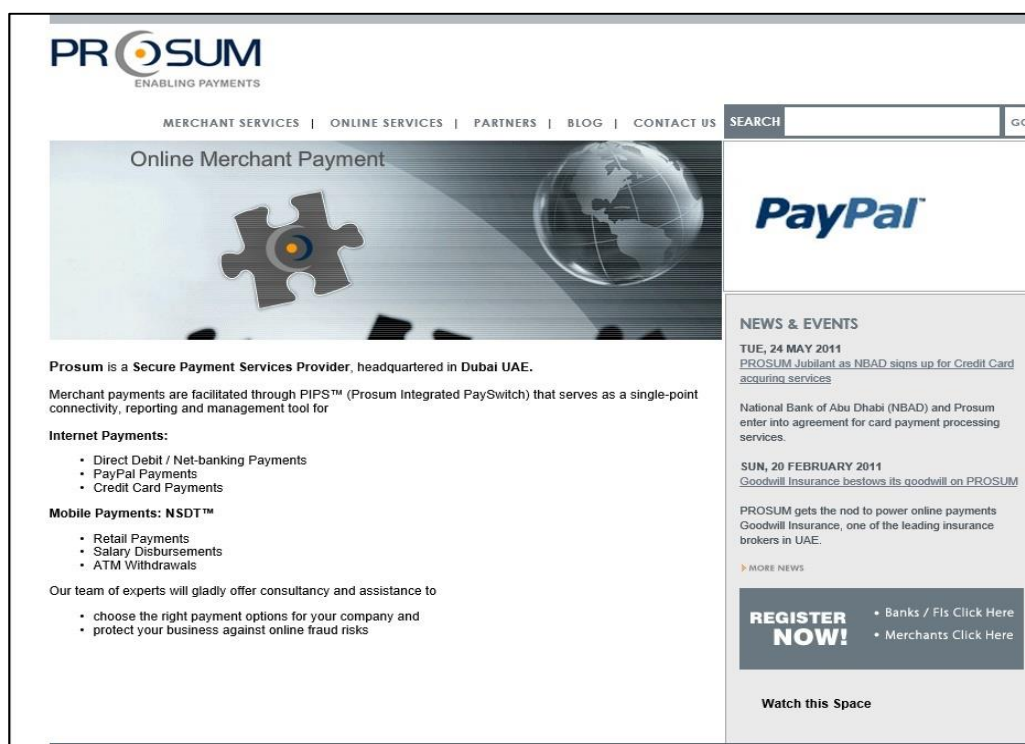


Fig. 21 Prosum - an example of a secure payment services provider

You should only make payments for purchases or transactions that are genuine. Only give credit or debit card details on secure (<https://>) sites; never send money to a stranger using a money transfer service and never send money to pay for taxes or fees on foreign lottery winnings - if you did not enter the lottery, you cannot win a prize!

### **2-3-3-2 Recognise when to use and when to turn off Auto-Complete tools.**

Some browsers have an auto-complete tool that stores information such as name and address when you are filling in forms on websites. The next time you fill in a form it will recognise the same fields and use the same information. This can be a useful timesaver when completing questionnaires or entering a list of email addresses.

On the other hand, auto-complete can be risky because it is not always just you who is using your computer. If your computer is stolen it adds a further risk of identity theft. In general you should turn off auto-complete, especially if you are making an online purchase from a computer that is used by other people or if you are entering bank account or credit card details from another computer.

### **2-3-3-3 Recognise different security measures around payment: using pop-up blockers, turning off Auto-Complete tools, browser security and filtering settings.**

There are a number of different security settings in most browsers. You should use as many as possible when entering bank or credit card details on any computer, even one that only you use.

- Turn on the pop-up blocker – although with two-factor authentication that might cause a problem
- Turn off cookies and auto-complete – this will provide a second layer of privacy and security
- Ensure that you are using a secure website as described in 2.3.2.2

# Quiz

---

**Q1.** You want to shop online for a music video you like. Which letter within the website address you are about to purchase from indicates that the website has some extra security?

- a. 's'
- b. 'd'
- c. 't'
- d. 'h'

**Q2.** Which web browser feature may leave some of your secure access details in the browser for someone else to use?

- a. Toolbar search
- b. Auto-Complete
- c. Favorites
- d. Pop-up blocker

**Q3.** What symbol is usually present on secure payment screens?

- a. lock
- b. circle
- c. star
- d. cross

**Q4.** Which one of the following actions helps you operate and use your computer more securely?

- a. Turn on pop-up blocker
- b. Turn off SPAM filter
- c. Turn off pop-up blocker
- d. Minimize pop-up screens

---

**Answers Overleaf**

# Answers

---

**Q1. a. 's'**

**Q2. b. Auto-Complete**

**Q3. a. lock**

**Q4. a. Turn on pop-up blocker**

## Chapter 2-4

### Think First

**2-4-1 Personal Identity**

**2-4-2 Sharing Devices**

**2-4-3 Social Networking**

**2-4-4 Spamming and  
Phishing on Social  
Networking  
Platforms**

**2-4-5 False Identities on  
Social Media and  
Grooming**

## 2-4 Think First

### 2-4-1 Personal Identity

#### **2-4-1-1 Understand the concept of online identity and what social networking means.**

An online personal identity is a social identity that an Internet user establishes in online communities, it is also referred to as screen name or Internet persona. Although some people prefer to use their real names online, some Internet users prefer to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally identifiable information.

A social network is a website that allows you to connect with friends and family, share photos, videos, music and other personal information with either a select group of friends or a wider group of people, examples such as Facebook ([www.facebook.com](http://www.facebook.com)), Twitter ([www.twitter.com](http://www.twitter.com)), LinkedIn ([www.linkedin.com](http://www.linkedin.com)) and YouTube ([www.youtube.com](http://www.youtube.com)) are great ways of keeping in touch with friends and family as well as making new connections with people based on similar interests or professions.

#### **2-4-1-2 Be aware of the implications of putting personal information online.**

Once information is posted online it cannot be retracted. Even if you delete your post, there is probably a copy of it somewhere.

Once information is posted online, it can be accessed by anybody who has Internet access. This includes your friends, your parents, your school or college, your employer, your students - and also potential hackers, scammers and stalkers. Posting your personal information makes you easily identifiable, the post will always be there and you will always be associated with the post.

#### **2-4-1-3 Consider who can access your personal information: friends, work colleagues, employers, criminals, predators.**

It is important to realise that your public profile is just that: public. Public information is available to everyone. How much information about yourself would you consider telling to a random stranger? That is what you are doing with your public profile. Even if you restrict it to friends of friends, that can be a lot of people. If you have 160 friends and each has 160 friends, that is a total of 25,600 people. Can you trust them all?

### 2-4-1-4 Know about social networking privacy options, and why they are important.

It is essential to review privacy options on your social networking websites. What you can do varies depending on the site. Generally, you cannot stop people posting comments about you and you cannot stop people posting photographs of you. What you can do is stop people from tagging you in photographs. You can stop people from seeing your birthday or where you go to school or work, or your current status. Restrict certain information so that only actual friends see it, if anyone else wants to know more about you, they can send a friend request and you can decide what you want to let them know. Fig. 22 shows an example of Facebook's privacy options that provide you with a clear picture of what is public and who can look you up. These options are customizable through the 'Edit' links shown.

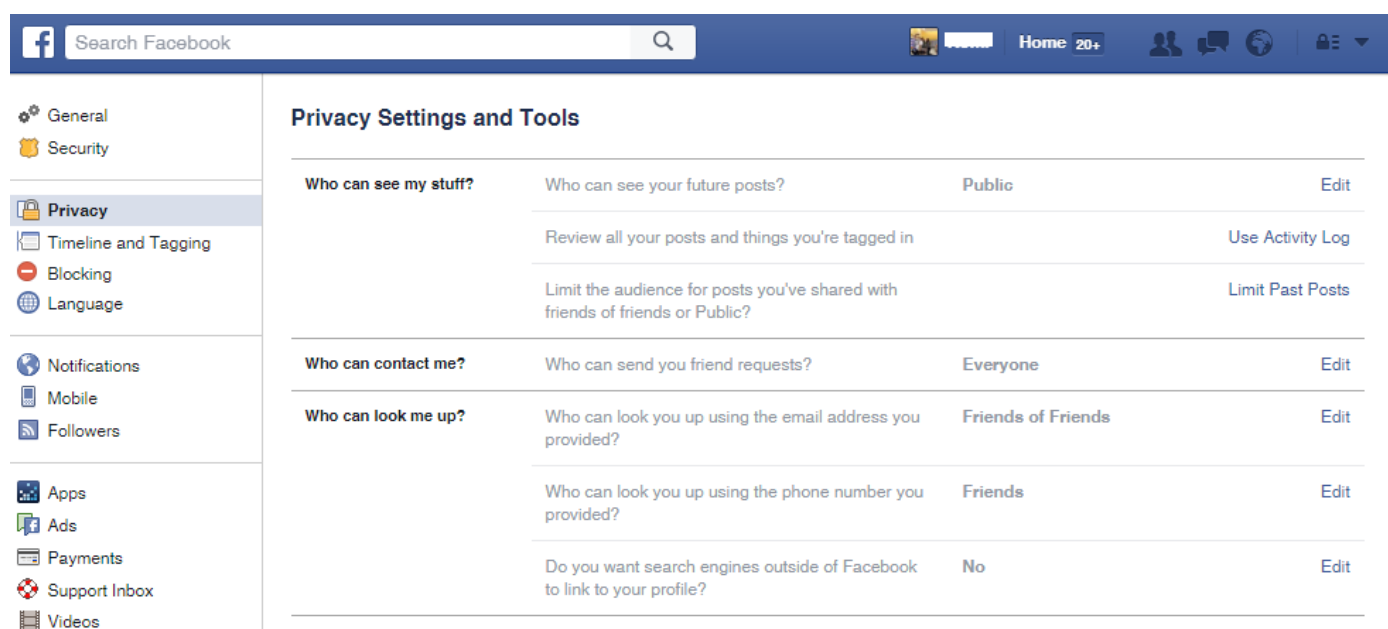


Fig.22 Facebook Privacy Settings and Tools (<https://www.facebook.com/privacy>)

To access the privacy options on most social networking sites, click on the 'Tools' icon on the site, an example is shown in Fig. 23 below.

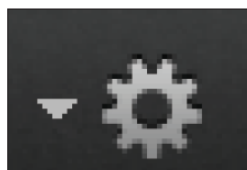



Fig. 23 Example of a Tools icon

To access the Twitter privacy options:

1. Click on the 'Tools' icon.
2. Click on 'Settings'.
3. Click on 'Security and Privacy' on the right hand side of your screen

The privacy options include those shown in Fig. 24 below:

---



---

## Privacy

**Photo tagging**

☐ Allow anyone to tag me in photos

☒ Only allow people I follow to tag me in photos

☐ Do not allow anyone to tag me in photos

**Tweet privacy**

☒ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more](#).

**Tweet location**

☐ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)

Delete all location information

This will delete all location information from past Tweets. This may take up to 30 minutes.

**Discoverability**

☒ Let others find me by my email address

☒ Let others find me by my phone number

[Learn more](#) about how this data is used to connect you with people.

**Address book**

Manage your contacts

Contacts you've uploaded to Twitter from your address book.

Fig. 24 Twitter Privacy options



## 2-4 Think First

### 2-4-2 Sharing Devices

**2-4-2-1 Be aware of the range of devices that can be used to share information: mobile phones, smart phones, mP3 players, iPods, tablets, etc.**

Devices can share information in ways that were unimaginable just a few years ago. Smart phones and tablets can share information over a network such as the Internet, bluetooth, and wireless. Almost any device, including MP3 players and iPods, can connect to a network and share information with any other device that can connect to the same network.

Social media networking sites have also made it easy to share information, especially pictures and videos from these devices.

**2-4-2-2 Beware how photo and video features may be used to record and post inappropriate content online.**

Examples of posting inappropriate content include sending explicit inappropriate messages and/or photographs; and taking unauthorized photographs of someone - the victims of this practice are usually females who feel harassed or humiliated when they realise that they have been victimised. This is especially the case when such images have already been disseminated on the Internet and they are identifiable.

Any device with a camera can send any photograph taken as a message, and once it is sent, the originator has no control over where it goes next. Social media websites generally have 'Terms of Use' agreements that provide rules and guidelines to ensure appropriate use by all its users.

YouTube's Community Guidelines, shown in Fig. 25 on the next page, try to ensure that users do not post anything inappropriate. The guidelines set out the rules of use for the site, and can be read in full at [http://www.youtube.com/t/community\\_guidelines](http://www.youtube.com/t/community_guidelines).

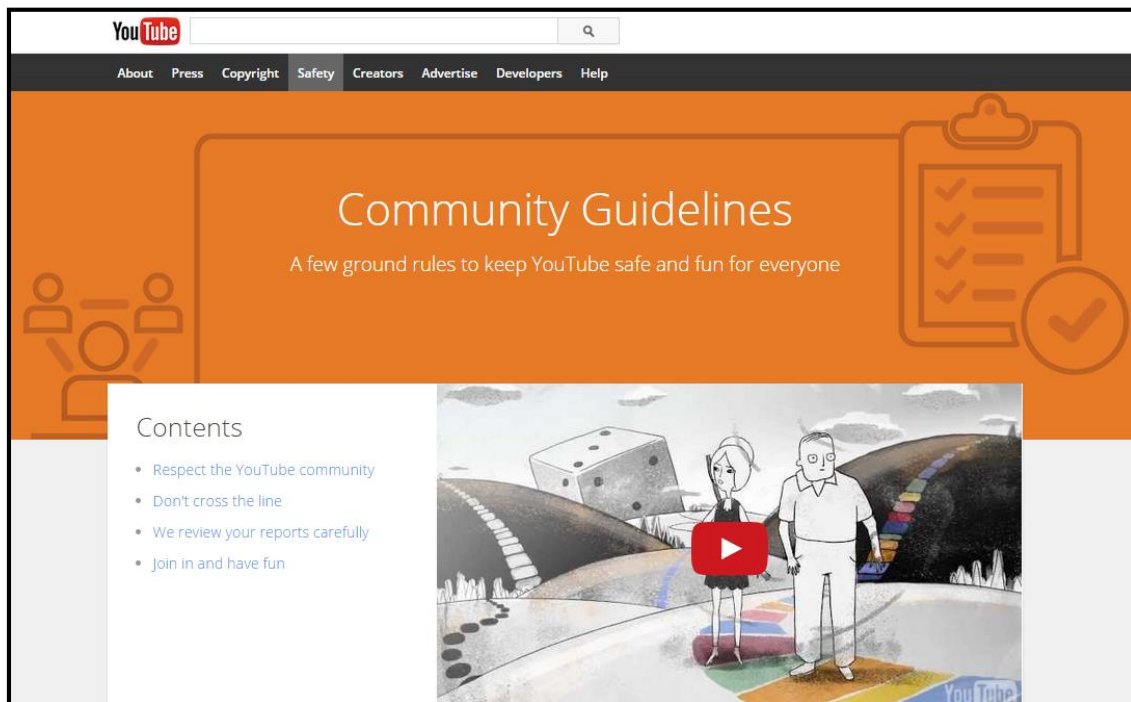


Fig. 25 YouTube's Community Guidelines

Online social networking has become one of the most popular activities for children and young people. Platforms like Facebook, Instagram, Snapchat and Twitter usually require users to be at least 13 years old prior to setting up an account. To help safeguard children and young people, parents must set controls and filter what their children see.

Parental controls and guidance are covered in Section 2-6-2.

**2-4-2-3 Be careful when posting pictures or movie clips online with your mobile phone. Ask permission of others before you post photos or video clips of them with your mobile phone.**

As discussed in previous sections of this book, individual privacy has become more and more important and personal liability seems to be growing with the number of videos and photographs taken and posted online using mobile phones. This is not a warning but a reminder to be considerate and cautious when posting photos online. Asking permission is always the best and safest way to reduce or eliminate this liability.

Here is a quick example to emphasize the importance. Certain countries are now imposing a law that only allows parents to post photos online of their children. Anyone else taking photos of minors and posting them without permission could face criminal charges. Of course this is not always enforced but it is creating a precedence for the future.

## 2-4 Think First

### 2-4-3 Social Networking

#### **2-4-3-1 Recognise different social networking sites used by young people, such as: Facebook, WhatsApp, Instagram, Snapchat, Twitter, Periscope.**

Different social networking sites tend to be used by different groups of young people. It is important to use a platform that is appropriate for the age group. If you lie about your age and log onto a site aimed at older people, other users can make assumptions and send comments or material that you may find inappropriate. The point of a social networking website is to use one that is popular with your friends and/or like-minded individuals.

Facebook is the market leader with over 1.5 billion users (source: <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>) and was initially aimed at college students. Its appeal has extended to all age groups, but make no mistake, teens and young adults still use their accounts. However, Facebook is not the primary platform on which they interact and engage with friends anymore.

Contrary to adults, teenagers access and utilise alternative social media platforms and virtual communities in various ways. One example of how they do this is by interacting on mobile applications. The Facebook app and Facebook Messenger are two different ways Facebook users can stay in touch with friends anywhere they go.

Another popular app people use is WhatsApp. In February 2016, it reached 1 billion users (<https://blog.whatsapp.com/616/One-billion>). It is recognised as an alternative text messaging application, where anyone can stay in touch with family and friends for free.

Instagram is a very popular platform adolescents use. Although most people have Facebook accounts, Instagram is a social media outlet used much more frequently by teens. It's a lot more interactive, as teens scroll through applications without the fear that something they like or comment on will show up on someone else's newsfeed. They can scroll through high-quality images while also giving the impression that it's for the "younger crowd".

Younger crowds are also attracted to video-related content. Although many social

media platforms do this now, one platform that built their foundation on video is Snapchat. As a result, it is quickly becoming very popular to the younger generation, to the point where 7 billion videos are being watched per day, which is quickly catching up to Facebook. (<http://www.bloomberg.com/news/articles/2016-01-11/snapchat-s-daily-mobile-video-views-said-to-rival-facebook-s>)

There is also a lot less social pressure of being followed by people you do not know. Once you post a 'story', your followers only get to watch it once.

Twitter, another well-established networking site, has a large base: nearly 320 million monthly active users with a total average of 500 million tweets per day.  
(source: <https://about.twitter.com/company>)

Contrary to previously mentioned platforms, teens consider Twitter a place to follow/be followed by people they've never met. Now, they are able to do it in video format using Periscope. In essence, teens are now able to watch live videos from all over the world.

Other social networking sites include Vine & Keek (short-video sharing networks), Soundcloud & MySpace (which emphasise on sharing music), and Pinterest & Flickr (online photo sharing platforms).

### 2-4-3-2 Know how to create a social network profile and how to set your profile to private or public view.

There is no such thing as complete privacy online. When it comes to profiles, remember it may not only be your friends who are viewing your profile so you should not reveal too much. In creating a profile, ask yourself how much would I want a stranger to know about me?

Your profile usually consists of your name, location, date of birth, interests, status and a photograph. Settings allow you to decide who can view your profile. Public can be seen by everyone, that is anyone with access to the Internet. Individual items can be made private, which means that you can restrict viewing to friends or close friends. The example in Fig. 26 below is Facebook's 'Privacy Settings and Tools' screen, and you can make the changes mentioned in 'Who Can Look Me Up?' by selecting the 'Edit' link to the right. The setting 'Everyone' means the information is public, so to change the setting to private, click on 'Edit'.

Privacy Settings and Tools			
Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of Friends	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address or phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	On	Edit

Fig. 26 Facebook - Privacy Settings and Tools (<https://www.facebook.com/settings/?tab=privacy>)

### 2-4-3-3 Know that anyone may be able to view your online profile, search by criteria and access information about you.

Your public profile can be seen by friends and colleagues, prospective employers, police, stalkers and registered offenders. Public means everyone. To check on how much information you are making public, type your name into a search engine and find out what is displayed in the results.

Keep your public profile appropriate for everyone to see.

#### **2-4-3-4 Recognise some of the dangers of social networking: inappropriate content, age verification issues, access to profiles, potential for predators.**

Most social network sites do not verify your identity when you sign up. Twitter only verifies celebrity accounts and Facebook simply verifies that you have access to the phone number you supplied. This means that anyone can set up a social network account using false information and an assumed identity.

This can lead to children and adolescents accidentally accessing inappropriate images and becoming victims of scammers and predators. Exploitation can include exposure to explicit or harmful content, and encouraging young people to post unsuitable content or images of themselves. Some issues to be aware of when using social media networking sites include:

- Gathering personal details - age, name, address, mobile telephone number, photographs;
- Promising meetings with celebrities or sports stars, or offers of free gifts;
- Paying young people to pose for explicit photographs;
- Bullying or intimidating behaviour;
- Asking to meet children or young people;
- Pretending to be a child or young person in order to meet.

## 2-4-4 Spamming and Phishing on Social Networking Platforms

### 2-4-4-1 Recognise that spamming and phishing are also prevalent on social networking sites.

The rapid growth in social networking sites has meant that they have become a prime target for spamming and phishing. In previous years, email was the main medium that spammers and phishers used to reach their victims. With the growing sophistication of filters deployed by email service providers, that window has closed down considerably. Instead they have migrated to social networking sites that carry a lot of public but personal information, which also have more active user bases.

### 2-4-4-2 Be aware of suspicious links to online ads, status updates, tweets and other posts.

While using your preferred social networking site, you will notice a multitude of online ads, tweets, posts with links, and status updates that don't seem quite right. The link in the status update, tweet, or post might have a strange combination of letters and numbers or might have generic wording that would not come from your friends. It is recommended that you avoid clicking on these links unless you can identify or verify that this link is legitimate. See Fig. 27 below.



Fig. 27 Spam links in status updates

Online ads are harder to uncover and most are just spamming people to obtain revenue through 'pay per click (PPC) advertising' or product sales. If you decide to open an ad online from a social networking site, please make sure you avoid downloading attachments unless you are confident of the website and company.

### **2-4-4-3 Understand the term ‘Social Engineering’ and be aware of the threats posed by social engineering attacks.**

Social engineering, in the context of social networking sites, refers to the psychological manipulation of people (most commonly young people) to divulge confidential information which might be used later to steal or commit other crimes against the victim. Social networking sites are the perfect platform for such attacks because users add other users on a regular basis and they become ‘friends’. Someone trying to commit this attack can patiently build relationships and eventually use that trust to commit a crime.



### **2-4-4-4 Recognise how easy it is to create a profile on social networking sites and how criminals can use this as an opportunity to pass themselves off as someone else.**

Creating a profile on social networking sites will take a beginner less than five minutes, and for those that have done it before it could take less than 60 seconds! Social networking sites cannot request and/or verify a lot of personal information based on the sheer volume of new users registering on a daily basis. So most sites require very little information such as a name, email address, and age or date of birth. This information is rarely verified and consequently people easily create fictional profiles or they could pass themselves off as someone else. This occurrence can lead to crime through the social engineering attacks mentioned in the previous section.



## 2-4 Think First

### 2-4-5 False Identities on Social Media and Grooming of Young People

**2-4-5-1 Be aware of the cyber threats posed to children by the use of false identities: access to personal information, grooming, child exploitation.**

As mentioned in Section 2-4-4-4 its easy to create a false identity on social networking sites. That said, imagine an adult that creates a profile of a young child to communicate with minors online. The act of 'child grooming' is done to befriend minors and establish an emotional bond with the intent to sexually abuse that child. There are many forms of child exploitation and this is not a pleasant subject to discuss but it is vital that teachers (and parents) understand the threats and address them to ensure young people stay safe online.

**2-4-5-2 Understand the different types of grooming, including radicalisation**

Grooming is a word used to describe the action adults take in an effort to take advantage of children through the use of false online identities. Adding a user on a social networking site allows immoral individuals to potentially view pictures of your friends and better understand a child's lifestyle through their posts without exposing their true selves. This could be used to further access more personal information at some point and might endanger a child's safety, both online and in real life.

There are a number of specific techniques that offenders use to mask their behaviour. Many deliberately establish themselves as a kind person you wouldn't suspect as an online offender because they brand themselves as 'nice' and/or 'innocent'. These disguises include, but are not limited to:

- An upstanding person in the community who is willing to help someone during depressing times
- Pretending to be someone of a much younger age who is looking to establish an online friendship
- Someone who uses radical ideologies and/or religious principles to convince young people to normalise their beliefs, but to embrace them as their own.

All these methods are ultimately used to gain trust in order to manipulate a child.

### **2-4-5-3 Understand the role that social media plays in radicalisation and how the internet is used for radical propaganda**

As society increasingly embraces the Internet, so do online extremists. In particular, social media offers online radicals the capability to communicate, collaborate and convince teens to do extremist acts. Many people have read articles and/or watched videos online and/or have directly talked to representatives of extremists groups and have, in turn, left their families to commit acts of terror and fight for a 'greater cause'.

This propaganda includes images and videos that promote an image of success online in order to attract young people to join the winning side and eventually live a fulfilling and exciting life. Social media posts are also created across all platforms to hold the idea that they can find a sense of belonging to a vibrant virtual community where they won't feel judged.

Online radical supporters continue to use several social media platforms, including:

- Facebook is used to share content, such as news stories, among their peer groups.
- Twitter is used because it is a popular social media platform that is easy to establish an account, share material with large numbers of people (using hashtags) and staying relatively anonymous at the same time.
- YouTube is used to host videos, created by official representatives of radical groups and by users themselves. Multiple 'dummy' accounts will be set up so that when videos are taken down they can be reposted quickly. (Many YouTube links are shared on other platforms, particularly Facebook and Twitter.)
- Instagram is used to share photosets frequently produced by various radical organisations. It is also used to share their lifestyle, often showing landscapes and images suggesting they are living a full and happy life.
- WhatsApp is used as a peer-to-peer network, so that sensitive information can be shared privately. This includes chats to befriend a victim and can end with procedures for travel, what to pack and who to contact on arrival. (Other messaging apps are used as well, including Kik and Telegram).

Because social media provides several mediums for online radicals to post content, it presents an illusion of normality for young teens who are exposed to it. It must be known that, just because something *looks* normal online (like posting a selfie or a picture of food) doesn't make it normal.

#### **2-4-5-4 Understand what is meant by the term radicalisation**

To be clear, online radicalisation is defined as the process whereby people become extremist. The term – along with the definition – alone is ambiguous, as radicalisation can refer to so many different concepts and effects.

In this context, however, online radicalisation is referred to as the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media, and as a result moves towards those views.

#### **2-4-5-5 Understand the role and responsibilities of teachers in safeguarding children and young people**

The reason why teachers need to understand and teach radicalisation is because schools play a role in education. Therefore, they should play a role in safeguarding children from any online abuse and should be vigilant about signs of possible physical or emotional abuse from online radicals who want to recruit young, innocent minds.

If you have a concern for the safety of a young student at risk of radicalisation, discuss the issue with your school's designated safeguarding lead, a school counsellor and/or the child's parents.

#### **2-4-5-6 Understand the push and pull factors associated with radicalisation**

Many people believe the increased influence of online radicalisation is simply based on the notion that people with similar beliefs and values now have better access to the Internet. They still have the impression that social inequality and poor education. Although these elements are factors to take into consideration, it is not the only reason why radicalisation issues are getting so much global news coverage.

Research has found no link to social inequalities or poor education. In fact, counterterrorism pundits argue that they are seeing more young people from caring middle-class families being recruited. With regards to religious extremists, a large number of young teens are exposed to this content – and eventually recruited – do not practise their faith regularly.

(<http://www.theguardian.com/commentisfree/2015/mar/01/what-draws-jihadis-to-isis-identity-alienation>)

Educators need to recognise that there is both a push factor and a pull factor to online radicalisation specific to the GCC:

- The “push” refers to the Western intervention in Muslim-majority countries (e.g. perceptions of foreign policy decisions that directly impact the region)
- The “pull” refers to the opportunity radical groups (e.g. religious fundamentalist groups) used to encourage young people to conform to their ideologies and contribute to their cause

Together, they shape a very narrow ethnic and cultural identity that individuals may feel pressured to striving towards. For instance, a teen who spends a lot of time online and often feels estranged from communities who follow mainstream forms of Islam might also feel unwelcomed by Western ideas. With a lack of inclusion to society and a lack of guidance from teachers and parents, it is through the Internet and online radicalisation where they may discover both their faith and a virtual community on which they can depend for advice.

### **2-4-5-7 Be able to recognise the signs consistent with individuals who are vulnerable to radicalisation**

The following issues can make individual children and young people susceptible to radicalisation:

- Identity crisis: Distance from cultural and/or religious heritage and feeling uncomfortable with their place in the society around them
- Personal crisis: Family tensions, feeling a sense of isolation, low self-esteem, disassociating from existing friendship group and becoming involved with a new group of friends with different interests
- Personal circumstances: Local community tensions, alienation from values within your community, events affecting a region of origin or an with which you identify, having a sense of grievance that is triggered by personal experience of bigotry or discrimination
- Unmet aspirations: Perceptions of injustice, feeling of failure, rejection of community values
- Criminality: Experiences of juvenile detention, previous involvement with criminal behaviour

Although the above issues are correlated with one's likelihood to be exploited to radicalisation online, there are certain changes in behaviour that you can find in *any* child that adults should keep in mind, as well. These include:

- General changes of mood, patterns of behaviour, secrecy
- Changes of friends and/or mode of dress
- Use of inappropriate language
- Possession of violent extremist literature
- The expression of extremist views
- Advocating violent actions and means
- Association with known extremists (online or offline)
- Seeking to recruit others to an extremist ideologies

#### **2-4-5-8 Be aware of the tools available to protect social media users and minimise the risk of radicalisation**

One of the first things people talk about when solving the issue of online radicalisation is to block the websites that contain violent and extremist content. This, however, provides limitations for what can be done at the school level. Plus, unless you want to restrict all access to the Internet, removing all inappropriate online content is impossible due to the fact that most social media content is generated by users and won't be removed until someone sees it and reports it.

That said, research also suggests that the methods and tools available to prevent various forms of risk behaviour are also effective in preventing radicalisation and recruitment to extremist groups. As a result, policymakers are working with schools (particularly counselors and teachers) to offer a range of methods that involve mentoring students and maintain a dialogue with groups of young people at risk.

In addition, there are best practices on social media to help reduce the risk of someone finding a young student and trying to connect with them. For example, make sure your students' privacy settings are set to private across all their platforms.

There are also options on social media platforms that prevent young students from seeing similar content. YouTube, for example, has a button you can click to prevent

students from seeing content related to that particular video. This is important to tell your students who may come across something inappropriate on their newsfeeds. See Fig. 28.



Fig. 28 YouTube's 'Not Interested' button.

There is still a need to continuously refine methods of radicalisation prevention and deradicalisation, but it is just as important to share counter-radicalisation content with other teachers, your students, and their parents (e.g. local authorities).

# Quiz

---

**Q1.** If you post something to a social networking site, will it be easy to delete later?

- a. Yes
- b. Sometimes
- c. Generally
- d. No

**Q2.** Which feature in social networking sites limits who can see your online profile?

- a. Access settings
- b. Online settings
- c. Privacy settings
- d. Usage settings

**Q3.** Which website is popular for sharing stories that can only be seen once?

- a. Facebook
- b. Instagram
- c. Twitter
- d. Snapchat

**Q4.** Which group of people is most vulnerable to online radicalisation?

- a. Young people
- b. Adults
- c. Senior citizens
- d. No one

---

**Answers Overleaf**

# Answers

---

**Q1. d.** No

**Q2. c.** Privacy settings

**Q3. d.** Snapchat

**Q4. a.** Young people



## 2-5 Virtual World

### Chapter 2-5

## Virtual World

**2-5-1 IM / Chatrooms**

**2-5-2 Video, Blogs**

**2-5-3 Online Games**

**2-5-4 Be Responsible**

## 2-5-1 IM / Chatrooms

### 2-5-1-1 Understand what Instant Messaging (IM) is, and what chatrooms are.

Instant messaging (IM) consists of sending real-time messages to another Internet user, much like text messaging on a mobile phone; it is very popular among younger generations, IM is also commonly used in the workplace as a quick way for employees to communicate with each other.

A chatroom is an online venue or virtual room where people with a shared interest can communicate with each other interactively in real time, as opposed to a forum where people communicate and carry on discussions more slowly by posting messages.

Some examples of instant messaging are Google Hangouts - <https://hangouts.google.com/>; Skype (see Fig. 29 below) ([www.skype.com](http://www.skype.com)); Facebook Chat to chat with your Facebook friends who are currently online. You can also use online apps, including the Facebook app and Facebook Messenger.





			
<b>Calling</b>	<b>Video</b>	<b>Messaging</b>	<b>Sharing</b>
Stay in touch. Make free Skype to Skype calls or call mobiles and landlines home and abroad at low rates.	Seeing is believing. Catch up face to face or get a whole group together on a video call.	At your fingertips. You're always in the loop with instant messaging, voice messaging and sending texts.	Share your world. Send photos, videos and files of any size. Get that secret recipe off grandma in seconds.
<a href="#">Discover calling</a>	<a href="#">Discover video</a>	<a href="#">Discover messaging</a>	<a href="#">Discover sharing</a>

Fig. 29 Skype features include Instant Messaging, and you can also make free video calls, video chat and share photos, videos etc.

## 2-5 Virtual World

### **Examples of Chatrooms:**

- irc2go (<http://en.irc2go.com/online.php>);
- Chathour (<http://www.chathour.com/>)
- Facebook's Live ChatRoom ([www.facebook.com/LiveChatRoom](http://www.facebook.com/LiveChatRoom))
- Paltalk (<http://www.paltalk.com/g2/webapp/groups/GroupsPage.wmt>)

### **Advantages of using Chatrooms:**

- You can meet people from all over the world that share common interests on topics such as music and entertainment, politics and religion in a safe and non-threatening environment.
- You can communicate directly with people and it can save you time.
- You can participate in an online community where there are no judgments based upon appearance.
- You can remain relatively anonymous and therefore remove the awkward first moments when chatting with a stranger.

### **Use chatrooms safely and be aware of the dangers, such as:**

- Chatroom discussions may become unethical or violent, or could promote hatred against others.
- Some people feel that they can act in any manner they want, which may result in harassment or bullying.
- Chatrooms are cruising grounds for paedophiles and other predators who want to make contact with young people.
- Online relationships with strangers in chatrooms can lead to you being cyber stalked, sent inappropriate material or pressured to arrange a real-world meeting.
- Flaming is common in chatrooms - where you make personal insults or disrespect a person.

Access to IM and chatrooms is available through PCs, laptops, tablets or smartphones, enabling you to keep in touch at any time.

### **2-5-1-2 Know how to create a generic IM profile.**

Before you can use Instant Messaging (IM) such as a chatroom, you must register and fill out a profile. The registration includes details about age, gender, address, but the profile is what you want other users to see. This IM profile enables you to log into chatrooms anonymously. You can assume an online personality that may or may not reflect real life. Choose a username that is unique but avoid anything that may be offensive. Most chatrooms and IM services insist that usernames must not contain any suggestive or inappropriate language.

If asked, choose an avatar (an image or picture that represents you) that suits the online personality, the avatar will be displayed when you are online. Again, try to choose one that is not offensive and will not be embarrassing.

### **2-5-1-3 Set options to allow contacts from a Buddy list only, and block unwanted contacts.**

In a chatroom, you can decide who can chat with you. If you feel uncomfortable with the way a conversation is going, you can block that person. People on a blocked blacklist cannot see when you are online. If you are younger, you can set rules that restrict users who can see you to names on a white list or Buddy list.

A white list is a list of e-mail addresses or domain names from which an e-mail blocking program will allow messages to be received. A buddy list is a list of people a user wants to communicate with.

### **2-5-1-4 Know how to disable a webcam.**

Some chatrooms automatically use a webcam if it is available. If you are not aware of this, potentially embarrassing videos could find their way onto the Internet. You can easily disable the webcam if you prefer not to use video, the following exercise shows you the steps:

#### **Exercise - Disable Windows Webcam**

To disable a webcam In Windows, take the following steps:

1. Go to 'Control Panel'.
2. Select 'Device Manager'.
3. Right-click 'Integrated Webcam'.
4. Select 'Disable'.

## 2-5 Virtual World

### 2-5-2 Video, Blogs

#### 2-5-2-1 Recognise the ability of the Internet to share videos: YouTube, MySpaceTV, etc.

Video hosting services allow users to upload and share pictures and videos; cameras, webcams and camera phones make it easy to capture images that can be uploaded and shared with friends and family. Some examples of social networking sites that enable you to share videos include:

- YouTube video sharing site ([www.youtube.com](http://www.youtube.com))
- Periscope livestream video app (<http://www.periscope.com/>)
- Flickr video and picture sharing site ([www.flickr.com](http://www.flickr.com))

See Fig. 30 below that illustrates that sharing is easy using televisions, PC's, laptops, tablets or smartphones.

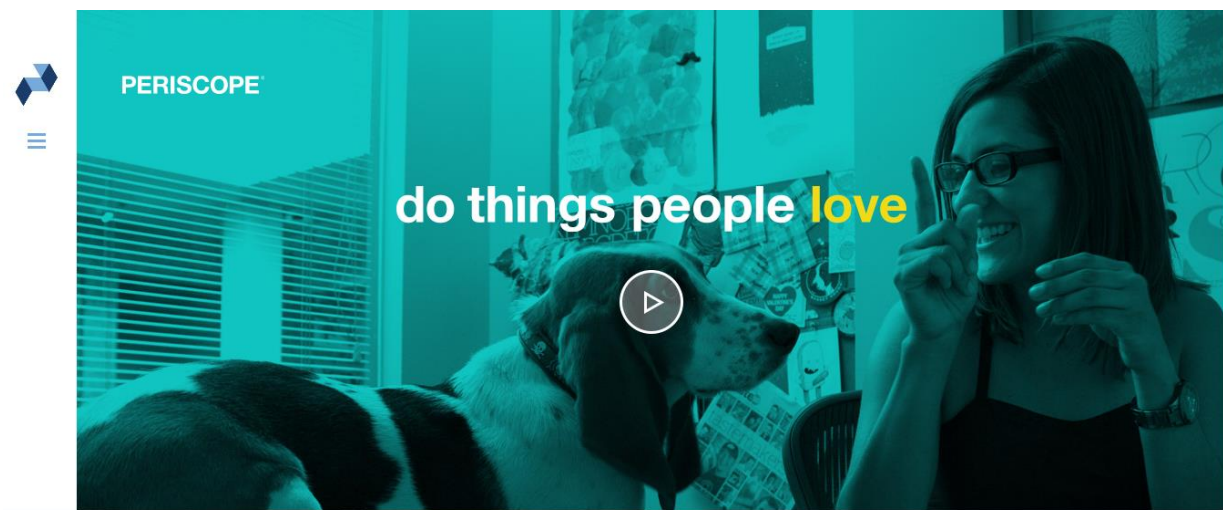


Fig. 30 Livestream video site Periscope. (<http://www.periscope.com/>).

When using video and picture sharing sites, you should always check the guidelines, safety policies and privacy guidelines.

Fig. 31 illustrates the help that YouTube provides to help users, teachers, students, etc.

Learn how to use the sharing site safely; note the section that pertains specifically to teen safety.

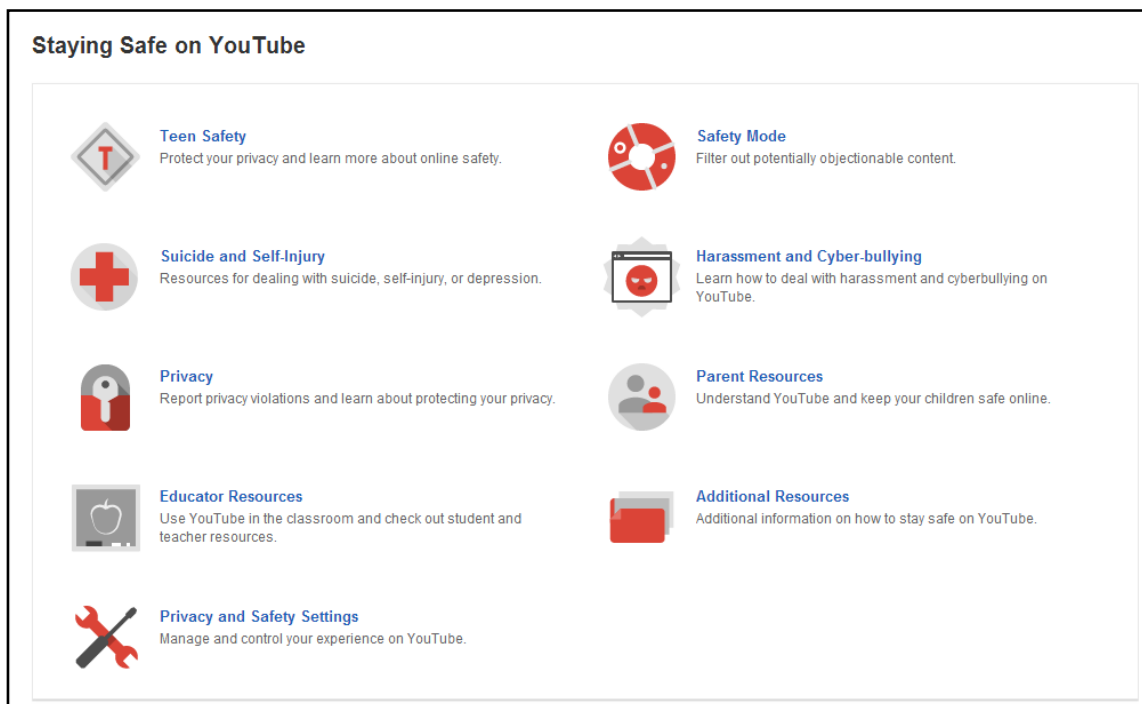


Fig. 31 Sharing safely with YouTube  
(<http://www.youtube.com/yt/policyandsafety/safety.html>)

### 2-5-2-2 Understand what blogs and micro-blogs are, and how they integrate with social networking.

Blog, short for web log, is a site containing a series of posts in chronological order, starting with the most recent post. A blog gives you your own voice on the web. It is a place to collect and share things that you find interesting – whether it is your political commentary, a personal diary or links to websites that you want to remember. Many people use a blog just to organise their own thoughts, while others command influential, worldwide audiences of millions. Professional and amateur journalists use blogs to publish breaking news, while personal journals reveal inner thoughts.

Blogs can be linked to your social networking website so that data entry posts can be set to automatically update social media pages.

Microblogging is a networking service that gives people short, frequent updates on smartphones or mobile devices. Entries are, for example, small sentences, single images or video links; they are sometimes referred to as microposts.

## 2-5 Virtual World

### 2-5-2-3 Recognise the risks associated with releasing personal information, or libel or gossip in a blog.

Even though a blog can be used to record what would previously have gone into a private diary, a blog is really a public record - they can be read by anyone with access to the Internet; any personal information in a blog is available to the public. Anything published in a blog is treated the same as if it was published in a newspaper. If your blog contains libel or gossip, you can be sued for defamation.

#### Good practice for posting:

##### Do not post:

- Comments that are abusive or may cause offence to others;
- Comments that might at any time cause embarrassment to yourself or others - what is posted online stays online;
- Personal information, it could easily get into the hands of criminals, online predators or online radical groups;
- Gossip about friends, colleagues, teachers, or anyone else

##### Do post:

- Comments that are true and not in any way libellous;
- Honest opinions that reflect your thoughts but do not offend others;
- Comments that are relevant to the subject

### 2-5-2-4 Understand how file sharing websites work, and the potential for viruses and malware from using file sharing sites.

File sharing websites allow users to share content, such as music or movies, and download to their computer. The process works by users connecting to an Internet based peer-to-peer network and making their files available to others connected to that same network.

Peer to peer simply means that the files are transferred from your device to the other people's device directly or vice versa. For example, a user logs on to the peer-to-peer network and searches for a particular song. In turn, the network searches through all logged on devices and displays who has it. The user initiates the download and a copy

of the song is transferred to their device. This is the file sharing process - the network makes everyone's files available in order to share.

The potential for viruses and other forms of malware from this activity is a major concern since users literally download files from unknown computers, some files are simply viruses disguised as songs or movies. Every time a file is copied, it is a chance for a virus to spread to each computer in the network. Some hackers use file sharing as a way to launch malware.

### Examples of file sharing sites include:

- **4shared** for free sharing of files, video, music, books, games, etc. (<http://www.4shared.com/>), see Fig. 32 below.
- **Hightail** free for sharing large files (<https://www.hightail.com>)
- **Fileconvoy** free large file exchange service ([www.fileconvoy.com](http://www.fileconvoy.com))
- **ShareFile** professional file sharing ([www.sharefile.com](http://www.sharefile.com))

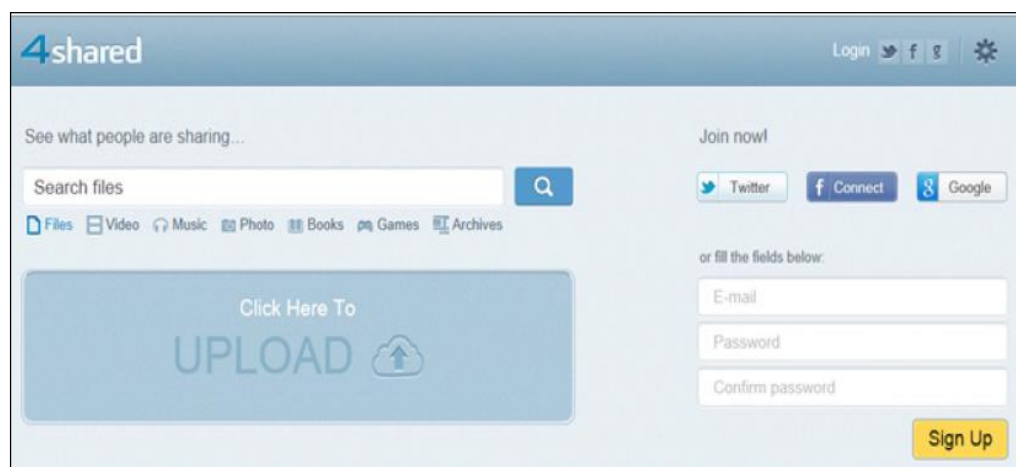


Fig.32 4shared - example file sharing site (<http://www.4shared.com/>)



## 2-5 Virtual World

### 2-5-3 Online Games

#### **2.5.3.1 Be aware of online Role Playing Games (RPG's) and related risks: unknown players, addictive quality.**

Interactive games allow you to compete against other players on the Internet. There are risks involved. The players see other players as avatars only and do not know the true personalities.

Some players can become obsessive or addicted to gaming such that almost all their spare time is spent in a virtual world. Online gaming is an indoor and sedentary activity, and spending large portions of time engaged in this activity can lead to health problems, trouble with work, psychological problems and breakdowns in personal relationships.

#### **2.5.3.2 Be aware to set privacy settings to block strangers from connecting with young people in games.**

One of the ways to protect young teens from online gaming is to change their privacy and online safety settings. If your students are signed into a gaming console, it is important that they are aware of its privacy and online safety settings (See Fig.33).

If you have a PlayStation, Xbox or any other gaming console, you can change your setting by following these three steps:

- Sign in to the live version of your account (e.g. Xbox Live), as you must be online to make these changes.
- Select the Privacy (or Online Safety) tab, depending on which setting you want to change for the child's account.
- Revise the settings as appropriate, and then select 'Save'.

## Privacy & online safety

The gamerpics below show the people in your Xbox family. To change someone's privacy and online safety settings, select their gamerpic, then make changes, then press Save. Any adult in the family can manage the settings for all the children in the family, but children can only see (and not set) their own settings. Parents if you update your child's settings, they will need to log out and log in for them to take effect.

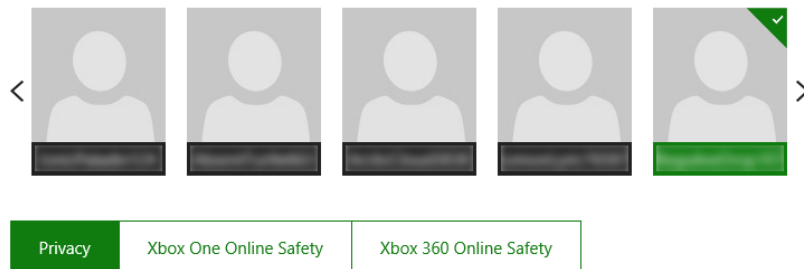


Fig. 33 Xbox Online Safety settings

**Disclaimer:** Children and teens may be restricted from changing privacy and online safety settings on their own account (like the Xbox One, for example).

Whether they can do it independently or not, it is important to discuss the issues of online gaming with parents to educate them about these safety options and how it can keep them from connecting with strangers to prevent the risk of being exploited.

## 2-5-4 Be Responsible

## 2-5 Virtual World

### **2.5.4.1 Learn how to be a responsible digital citizen by not circulating messages, pictures, or other material that can be hurtful. Share images only with people you know and trust.**

First and most importantly, only share images with people you know and trust. Sharing with strangers can create unwanted problems and subject you to unwanted attention and possible abuse. The instantaneous nature and vast reach of social networking sites means that personal attacks can occur and escalate very rapidly both between individuals and groups, such that, the damage created can be irreparable. This is relevant information to ensure that both teachers and students aren't harassed.

Second and just as important DO NOT circulate messages or pictures that could be hurtful to the people mentioned within, or to people receiving that material. Consider how you would feel if you were to find yourself the object of such hurtful material.

### **2.5.4.2 Know how to decline or block strangers and unwanted contacts. Be careful about planning to meet people you don't really know, even if they have become your 'online friends'.**

When strangers tirelessly try to add you to their network or continue to send you invites you have the option of blocking such requests using the social networking site's options. Every new contact goes through an approval process whereby you must choose to accept, ignore, or block a contact.

Contacts that are already part of your network might also begin to misbehave and you can manually block them by going through the settings on the site. Facebook, for example, requires you to locate their Facebook page and at the top near the profile picture there are a set of options in which one will say 'Block'. Once selected that friend will no longer be able to view or message you.

Remember, online friends that you have never met before are not necessarily real friends and you should carefully consider meeting those types of people in real life. Ensure there is a group of your real friends with you to provide a secure meeting environment and avoid sharing details about your life until a closer relationship is built with time.

#### **2.5.4.3 Use a webcam only with people you know – disconnect or disable it when not using it.**

A webcam, by online standards, is the same as inviting someone physically into your home. Would you normally invite a stranger into your home? Probably not, and therefore it is best to avoid using a webcam with strangers. If you choose to do so in certain instances, it makes more sense to move yourself and your device, if it is mobile, such as a tablet or laptop, to another location such as a café, which is typically where you might meet a new person.

When your webcam is not in use, ensure that it is disabled or disconnected. You can disable the webcam through the settings options in the applications that utilise the webcam. If you are using a webcam with a USB cable then simply disconnect the cable to disable it.

#### **2.5.4.4 Always treat others online as you would like to be treated yourself.**

The Golden Rule that is fundamental to human nature is that one should treat others as one would like others to treat yourself. This goes beyond real life, as the more time we spend online means it is becoming more important and standardised to respect others and abide by community guidelines on the web; many people refer to this as using proper 'netiquette' (short for network etiquette).

#### **2.5.4.5 Understand how to be an upstander and not a bystander when you see online behaviour that you know could be hurtful.**

As a teacher, how your students interact in the classroom goes far beyond what they say. It is important to be kind to people online, but if you see someone being bullied online, it is your duty to be a good digital citizen and make yourself available to those in need.

It's really important to adjust your views and attitudes online because you cannot take words back online after someone sees them; once you post, someone can immediately see it and remember it. However, it's also important to take a stance on issues like cyber bullying. Just like in real life, words can be hurtful, and there needs to be consequences for those who hurt others.

#### **2.5.4.6 Learn different strategies for dealing with cyber bullying and**

## 2-5 Virtual World

### **what to do if it arises.**

Naturally, talk about bullying online is going to be difficult if schools and teachers do not include it in a structural format. Teachers can play a direct role in dealing with cyber bullying by creating lesson plans that revolve around the issues and techniques people use to avoid cyber bullying, but more importantly teaching students about the repercussions of posting hurtful and regretful things online.

You can also create opportunities for students to research the subject themselves and think of creative ways to raise their own awareness about cyber bullying. They can customise their projects based on specific topics within the realm of cyber bullying and discuss how it has affected them and others within their local community. It also helps them engage in conversations in an attempt to find their own solutions on how to reduce cyber bullying.

Last but not least, it should also be recognised that there may be some students who may not feel comfortable talking to someone who they engage with on a daily basis, like a teacher or a parent, due to negative stigma. Therefore, one could also refer to a third party – such as a guidance counsellor – who has the technical skills and the professional experience to communicate with students more comfortably.

### **2.5.4.7 Be aware that downloading music, films, pictures, computer programs and games from the Internet may be against the law, unless it clearly says on the site you are using.**

Any material that has a copyright such as music, films, computer programs or games, and possibly pictures should not be downloaded without permission. This permission typically comes directly from the maker of the material or through a licensed dealer that sells the material for a fee. Downloading this material without permission is against the law. It is also commonly referred to as piracy.

Next time you think of illegally downloading files, consider the following statement. We all work for a living and could not afford to maintain a life without the money we earn. We have bills to pay, children to feed, and a rent or mortgage payment. The individuals that create this material also survive on the money they earn and when online users begin to take this material without paying it affects every person involved in developing the material that we enjoy.

#### **2.5.4.5 Always treat others online as you would like or expect to be treated yourself.**

Although the virtual world seems unreal at times, you must keep in mind that online users are real people with real feelings and they each have their happy and sad moments. You should try to treat others online just as you would expect people to treat you. This rule will help protect you and those you interact with in the virtual world.

## **Quiz**

**Q1.** Which technology allows you to instantly send a

**Q3.** What is the word people use when referring to

## 2-5 Virtual World

### Answers

---

**Q1. a.** Instant Messaging

**Q2. b.** Buddy list

**Q3. a.** Netiquette

**Q4. c.** Computer virus attacks

## Chapter 2-6

### Learn Together

**2-6-1 Discuss**

**2-6-2 Parental Controls**

**2-6-3 Online Addiction**



## 2-6 Learn Together

### 2-6-1 Discuss

#### **2-6-1-1 Learn together, discuss your computer use with friends and family.**

Children and young people use the Internet regularly and may be involved in more online activities than their parents. Most Internet use is positive, but they might sometimes behave in ways that leave them exposed to risks, such as, bullying or intimidation or exploitation. To help you stay Cyber Safety, regularly discuss your activities on the Internet with your family and friends, ask them questions particularly if you are unfamiliar with this activity.

#### **2-6-1-2 Accept that it is best to keep home computers in central and open locations.**

The best location to keep the computer is in a family area of the home, rather than a bedroom; this makes the computer accessible and parents can monitor computer use. User profiles can be set up for each family member and rules can be set for Internet use to ensure that the entire family enjoys safe Internet use.

When talking to parents, you should make it an effort to let them know that they should also make a habit of regularly checking their children's online activities to reduce risks such as exposure to inappropriate content or theft of personal information.

#### **2-6-1-3 Know about filtering and monitoring software to: filter explicit images, log online activities, set online timers, block personal information from being posted or emailed.**

By using Internet filtering software, access to content, which may be harmful, explicit or illegal, is blocked for anyone using the computer. There are two types of filtering software: ones that are in-built with your operating system software and you can manage from the desktop, and ones that are offered by the Internet Service Provider (ISP). Internet filtering software is only as good as the blocking lists of offensive or inappropriate content that is maintained for it. By checking with your Internet Service Provider (ISP) you can find out if filtering or other parental control options are offered as part of the service options.

Monitoring software records all computer activity and can provide information about different websites visited, Facebook or other social network activity, chat and instant messaging activity as well as search activity. Some monitoring software will provide alerts about any emails sent, so that an added level of control can also be in place. The parental control software that often comes installed on a computer also has a range of additional features.

### Some examples of freely downloadable software to help monitor Internet usage and block websites:

- K9 Web Protection (see Fig. 34 below) - <http://www1.k9webprotection.com/>
- Hidetools HT Parental Controls - <http://www.hidetools.com/parentalcontrol.html>
- NCH Software - <http://www.nchsoftware.com/childmonitoring/index.html>

### Using Parental Controls you can control:

- Time limits to prevent a user from logging on during specified hours.
- Games to choose an age-rating level for games and block unrated games or specific games.



Fig. 34 K9 Web Protection

## Exercise - Using Windows 7 to set up a Game Rating Systems using Parental Controls

1. Click the 'Start' button.
2. Click 'Control Panel'.
3. Click 'User Accounts and Family Safety', and then under 'Parental Controls' click 'Set up Parental Controls'. (You may be prompted for an administrator password, type in the password as instructed on the screen.)
4. Click 'Game Rating System'; you will be prompted to select a game rating system. Game Rating Systems examine the content of games and assign age ratings to them, similar to the system of age rating applied to movies. Each option has a link to their corresponding website for additional information.

**The age rating will apply to all users.**

## 2-6 Learn Together

### 2-6-2 Parental controls

#### **2-6-2-1 Recognise that parental controls are available on a range of media devices: digital TV, computer/video games, mobile phones, iPods, tablets and computer software.**

Parents can control more than just Internet access on a computer. On digital televisions it is possible to lock certain channels so that the user needs to enter a PIN to view those channels. Mobile phone service providers offer free parental controls; content filters allow parents to set limits to what content their children can download to their phones. Usage controls put the parent in charge of a child's phone usage. They can block certain numbers or restrict outgoing calls to a pre-approved list, and disable the phone during school hours, for example. Dual access allows both the parent and child to have access to the records regarding the child's account, including all numbers called.

Parental Control Apps can be downloaded directly to a Smartphone, examples are:

Mobile Minder - <http://www.mobileminder.com/> and Parental Control for Mobiles, Myfone.mobi - <https://play.google.com/store/apps/developer?id=Myfone.mobi>

Parental controls can be set up on a range of smart devices, including tablets, iPods and computer software. Operating systems, such as Windows, include Parental Controls as standard and parents are encouraged to work with their children to set up a safe computing environment.

An iPad is a popular example of a tablet. You can enable Restrictions, also known as Parental Controls, to prevent access to specific content and features, e.g. the Safari browser, YouTube, music, games, etc.

To enable Restrictions on an iPad, click on 'Restrictions' under 'General Settings' and then 'Enable Restrictions' and enter a pass code. The pass code is needed to change settings or disable the restrictions. You can configure a pass code for an iPad by following these steps, 'Settings' > 'General' > 'Pass code Lock'.

There are many free downloadable apps for mobile phones and tablets to help keep children and young people safe on the Internet. An example of free downloadable software is Kids Place (see Fig. 35 below):



Fig. 35 Example of parental control software – KidsPlace (<http://www.kiddoware.com>)

### 2-6-2-2 Set parental controls on operating software.

To set parental controls on a computer with Windows 7 operating software, follow these steps:

- Click on 'Start' button and select 'Control Panel'.
- Click on 'User Accounts' and 'Family Safety'.
- Add a user account for each person using the computer; assign a password to each user account.
- Click on 'Parental Controls' and for each user in turn:
  - Set time limits on what hours and on what days this person can use the computer.
  - Games are rated according to age, set an appropriate age group for this user and allow or block specific games.
  - Allow the user to run any program on the computer or specify which programs the user can run.

### 2-6-2-3 Know how to install or download parental monitoring software: [www.parentalcontrolbar.org](http://www.parentalcontrolbar.org)

There are a number of web monitoring solutions which allow you to block inappropriate content from the computer and that record the websites visited to allow you to make a judgment on whether they are suitable or not. Some are commercial but many are free. Options include Net Nanny, K9 Web Protection, Parental Control Bar for Internet Explorer & Safari, and ProCon Latte & FoXFilter for Firefox.

#### To install a Parental Control Bar:

1. Go to [www.parentalcontrolbar.org](http://www.parentalcontrolbar.org) (see Fig. 36 below)



Fig. 36 <http://www.parentalcontrolbar.org/>

2. Click on the 'Download Now' link at the top right.
3. This link will take you to another website ([download.cnet.com](http://download.cnet.com)) where you have to click on the button saying 'Download Now' on the left side of the page. (See Fig. 37 below)

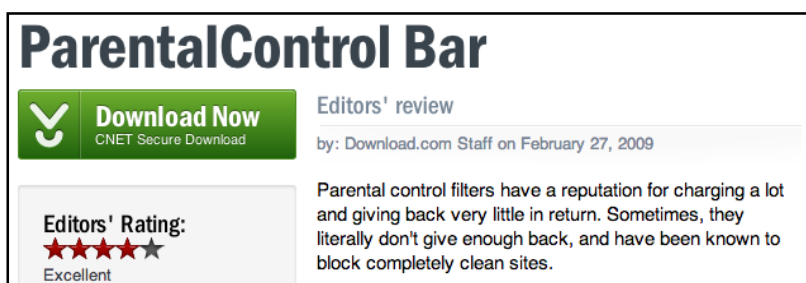


Fig. 37 Download Link

4. A 'File Download – Security Warning' window pops up on the screen. Select the 'Run' button shown in Fig. 38 on the next page.

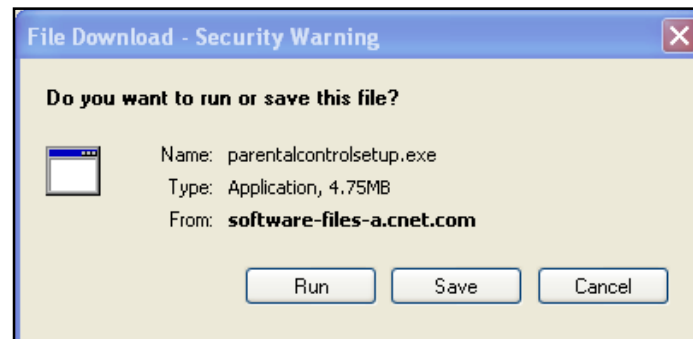


Fig. 38 Run or Save Window

5. Once the application is downloaded and launched, a 'Terms of Use' window should pop up and you need to select the 'I Agree' button. (As shown in Fig. 39 below).

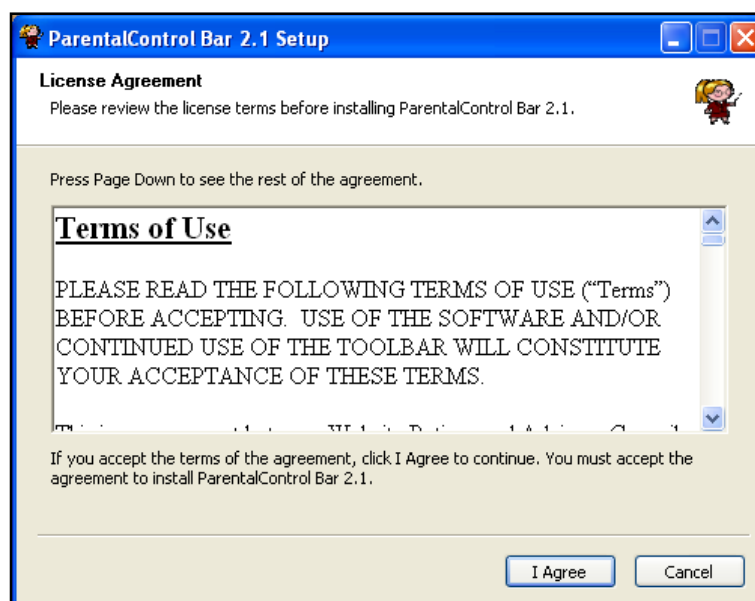
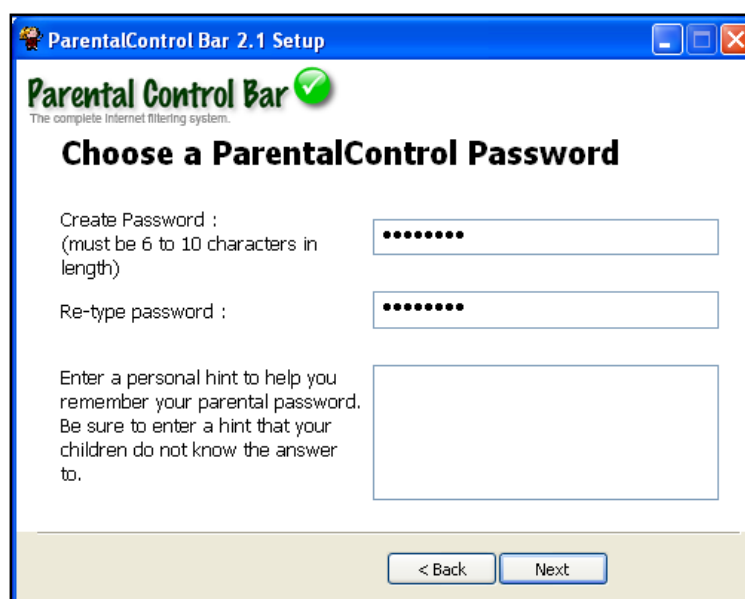


Fig. 39 License Agreement

6. On the Parental Control Bar window you need to create a password, confirm it and enter a hint to help you remember it in the event the password is forgotten. Once the necessary information is entered, select the 'Next' button. (As in Fig. 40 below)



The screenshot shows a window titled 'ParentalControl Bar 2.1 Setup'. The window has a blue title bar with standard Windows window controls. Below the title bar, there is a logo for 'Parental Control Bar' with a green checkmark and the text 'The complete Internet filtering system.' Below this, the main heading is 'Choose a ParentalControl Password'. The form contains three input fields: 'Create Password : (must be 6 to 10 characters in length)' with a text box containing seven dots, 'Re-type password :' with a text box containing seven dots, and 'Enter a personal hint to help you remember your parental password. Be sure to enter a hint that your children do not know the answer to.' with a larger text box. At the bottom of the window, there are two buttons: '< Back' and 'Next'.

Fig. 40 Choosing a password

7. Under 'Forgotten Password Assistance' from the window you see on your screen, you need to enter an email twice accordingly. Then press on the 'Next' button. (Look at Fig. 41 below). This will specify the email account that can reset the password if it is forgotten.



The screenshot shows a window titled 'ParentalControl Bar 2.1 Setup'. The window has a blue title bar with standard Windows window controls. Below the title bar, there is a logo for 'Parental Control Bar' with a green checkmark and the text 'The complete Internet filtering system.' Below this, the main heading is 'Forgotten Password Assistance'. The form contains two input fields: 'Enter parental email address: (e.g.:jane.doe@example.com)' and 'Re-enter parental email address:'. Below these fields, there is a paragraph of text: 'Should you lose your password you will be able to have your forgotten password sent to the email address specified above. Make sure you enter an email address that you are certain your children do not have access to.' At the bottom of the window, there are two buttons: '< Back' and 'Next'.

Fig. 41 Forgotten Password Assistance



8. Finally click the 'Finish' button to exit, see Fig. 42 below.

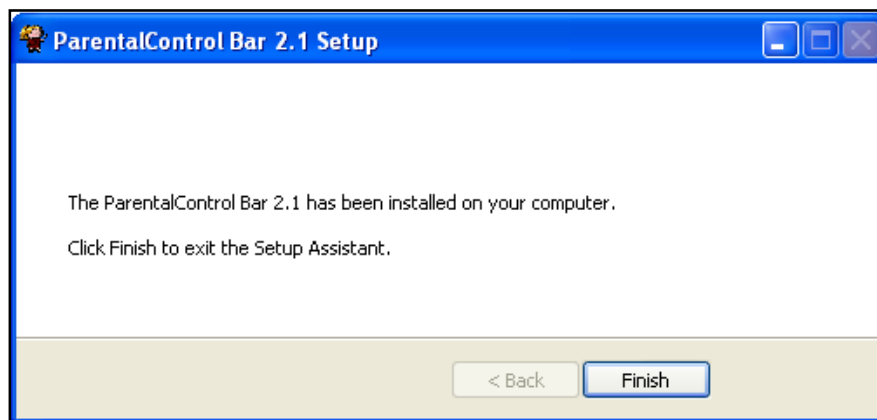


Fig. 42 Setup completion window

9. The installation process is complete and you should see a new 'Congratulations!' web page in your Internet browser as shown in Fig. 43 below.

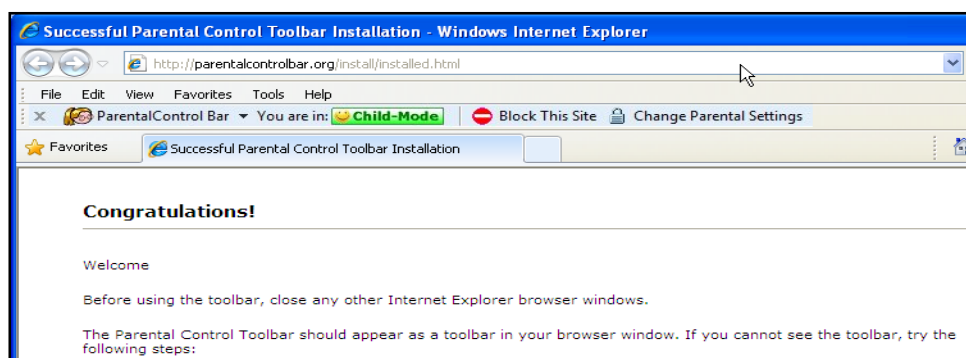


Fig. 43 – Congratulations page

For assistance with the product features follow the directions below:

1. In the address bar you will need to key in <http://www.parentalcontrolbar.org> so that you are directed to the main website page.
2. You will notice the 'Product Features' tab where you have to click.
3. As you see on the Fig. 44 shown on the next page, the 'Control Bar Help Menu', 'The Child Mode', 'Easily Block Adult Sites' and 'Change Parental Settings'. These all include detailed instructions that help you fully understand how to keep your child Cyber Safety.



Fig. 44 Forgotten Password Assistance

## 2-6-2-4 Know why it may be appropriate to create different user accounts with different access and privileges for each account.

There are several important reasons why it may be appropriate to create different user accounts.

- User accounts separate email accounts, providing more privacy.
- Preferences of themes, view options, and other customizable settings are saved for each user.
- There is improved security because access can be different for each user limiting children from certain access and forcing approval by an Administrator account prior to application installation reducing potential virus attacks.
- It reduces file-sharing problems since each user obtains his/her own folder.

### **2-6-2-5 Know why you would set up a child email account and direct incoming emails to parental inbox for review.**

For the same reason that you would set up different user accounts, each child should also have their own email account.

Among the controls that can be put on an email account include:

- Restrict incoming emails to a white list of approved contacts.
- Send a copy of all incoming emails to a parent account.
- Send a copy of all outgoing emails to a parent account.

These features provide an additional layer of security and filtration that reduces the risk of your child receiving inappropriate content, as well as providing additional insights into his/her personal life ensuring they remain safe.

### **2-6-2-6 Be aware of the criteria to consider when choosing parental filtering software. How applicable is it to different types of devices, such as smartphones, or gaming consoles?**

Beyond the benefits of parental filtering software there are several criteria to consider prior to investing in a software application.

- Invisibility – monitoring can only be effective if your child is not aware and does not feel the presence of the software. The child should not be allowed to disable or remove the programme as well.
- Data filtration – it is very easy to be overwhelmed by data that is collected through the normal course of your child's Internet use. It is key to find good filtration that provides meaningful information that could be triggered by the use of certain words or the opening of particular websites.
- Data access – once this data is collected it can be accessed either remotely or locally on the computer. If your child solely uses the device it makes more sense to receive the data remotely via email or a link because regular seizure of your child's computer for inspection will push them to find other devices for their unpermitted activities.
- Monitoring capability – the software application should provide monitoring for multiple applications including Internet browsers, chats, messaging, videos watched, music heard, and other social networking portals. As well as multiple devices, if possible, including the computer and smart devices such as a tablet or mobile phone.

### **2-6-2-7 Be aware how young people may hide online activity.**

Young people may seek to hide their online behaviour by clearing their Web browser history or minimizing the browser when teachers or parents walk in or pass close by the computer they are using. They may create 'private' email accounts or social media profiles that parents do not know about. Added to this, mobile devices may be used to access websites that are not permitted or maintain social media discussions.

Smart phones can also be used to carry on Instant Messaging activity, or to download videos. At worst young people may download illegal or pirated content, which may in itself be criminal behaviour. Parents need to engage in a positive dialogue and be open and encouraging about what is safe and acceptable and what is not to minimise exposure to risks.

### **2-6-2-8 Know ways to protect against young people hiding online activity.**

Teachers and parents need to be engaged with children as they learn about and use the Internet. By indicating they appreciate the benefits with the online world, with social media and technology, parents show they are in tune with things. On the other hand teachers and parents need to outline the wide range of risks and set down clear boundaries about what is safe and acceptable and what is not. Teachers and parents need to sustain an open and encouraging conversation about online behaviour while applying parental control software or other safeguards to filter and monitor that behaviour.

Parents in particular need to say clearly to their children that if there is something troubling or upsetting them online, that they can come to them or their teacher. Parental guidance and controls can help reduce the potential risks to children and young people as a result of interacting with social media networks and other interactive content. Such risks include:

- Bullying by people they consider friends.
- Posting personal information that can identify them offline.
- Inappropriate befriending, exploitation, abuse, and contact with strangers.
- Exposure to unsuitable content.
- Involvement in making illegal or explicit adult content.
- Exposure to racist or hate mail.
- Glorifying activities such as drug taking or drinking alcohol.
- Leaving home as a result of contacts made online.

Parents are encouraged to establish clear ground rules and keep communication open with their children. It is better to have your child as an ally than an adversary.

**2-6-2-9 Be aware that filtering software is not a substitute for proper parental supervision and open discussion with children and teens.**

Although filtering software can provide a lot of monitoring and security it can never be a substitute for parental supervision. Children are curious and that curiosity can inadvertently expose them to online risks that are effectively handled by the filtering software but at the end of the day we are physical beings living on this planet and most issues that are discovered online relate to our personal and real lives. Parents should try to maintain an open dialogue with their children so that real problems are discovered and addressed prior to release on the Internet.

## 2-6-2-10 Know how to create an Internet User Agreement for parents and children.

A great way of creating this agreement is to have an open family discussion with input from each member. This will set the groundwork for an agreement that will be more strongly honoured by everyone. A sample agreement is provided on the following page. You can find additional links online including tips on how to engage your children in the process. See Fig. 45

**Staying Safe Online:  
A Young Person's Contract**

1. I will ALWAYS tell a parent or another adult immediately, if something is confusing or seems scary or threatening.

2. I will NEVER give out my full name, real address, telephone number, school name or location, schedule, password, or other identifying information when I'm online. I will check with an adult for any exceptions.

3. I will NEVER have a face-to-face meeting with someone I've met online. In rare cases, my parents may decide it's OK, but if I do decide to meet a cyberpal, I will make sure we meet in a public place and that a parent or guardian is with me.

4. I will NEVER respond online to any messages that use bad words or words that are scary, threatening, or just feel weird. If I get that kind of message, I'll print it out and tell an adult immediately. The adult can then contact the online service or appropriate agency. If I'm uncomfortable in a live chat room, I will use the "ignore" button.

5. I will NEVER go into a new online area that is going to cost additional money without first asking permission from my parent or teacher.

6. I will NEVER send a picture over the Internet or via regular mail to anyone without my parent's permission.

7. I will NOT give out a credit card number online without a parent present.

Young Person\_\_\_\_\_ Date\_\_\_\_\_

Parent/Guardian\_\_\_\_\_ Date\_\_\_\_\_

Fig.45 Internet User Agreement between Parents and Children

## 2-6-3 Online Addiction

### **2-6-3-1 Understand how Internet use can interfere with daily life, work and relationships.**

While time spent on the Internet can be productive, compulsive Internet use can be disruptive to your daily life, work and relationships. What begins as innocent use for work or personal life can quickly turn into an addiction and potential psychological damage.

### **2-6-3-2 Recognise the concept of Internet Addiction Disorder (IAD) and the different types of addiction problems: inappropriate content, chat rooms, online gaming, and compulsive web surfing.**

IAD, short for Internet Addiction Disorder is also commonly known as Problematic Internet Use (PIU) or Compulsive Internet Disorder (CIU). Basically any online related compulsive behaviour that interferes with normal living can be classified as IAD.

Common problems (excessive use) of IAD are:

- Computer addiction – excessive use and time spent on a computer
- Information overload – web surfing for information but leading to lower work productivity
- Net Compulsions – gaming, shopping, auction websites, gambling and other services offered online
- Cyber-relationships – social networking, chat rooms, and messaging to the point where virtual relationships are more important than the real world
- Inappropriate content abuse – compulsive use of adult content websites negatively impacting social and marital relationships

IAD might receive a future psychological disorder classification due to its high prevalence in our society today.

### **2-6-3-3 Recognise some of the symptoms of IAD: losing track of time online, isolation from family and friends, defensive about Internet use, trouble completing other tasks, sleep disturbances.**

Signs and symptoms vary but here are some general warning signs to pay attention to;

- Losing track of time online – finding yourself online longer than you intended, minutes turn into hours, or becoming cranky if online time is interrupted.
- Isolation from family and friends – your social life might be suffering, neglecting family and friends, no one understands but your ‘online’ friends.
- Defensive about your Internet use – sick of people complaining about your use of the computer, hide your Internet use from those that are close to you.
- Trouble completing tasks – house chores might be piling up, work tasks seem to be slipping, and perhaps you are working late to catch up or staying later to use the Internet freely.
- Sleep disturbances – trouble sleeping, having thoughts at night that prompt you to research it online immediately, finding yourself up later than normal on a regular basis.

### **2-6-3-4 Know how to help a child with Internet addiction: encourage other interests and social activities, monitor computer use and set clear limits, use apps to limit child’s Smartphone use, discuss underlying issues with the child, get professional help.**

There are three steps every parent should undertake to properly tackle IAD with their children. The first step, complete an online addiction test as provided in the next section or from any other credible source online. Upon completion of this test and the results point to IAD behaviour then proceed to do the next step of providing personal help as described in this section. Finally, should the parent’s guidance produce very little or no improvement in the child’s behaviour, seek professional help to address possible underlying psychological issues.

Personal guidance from parents – with the help of teachers – should look to do several things for the child.

1. Provide limits just like any other activity a child undertakes. Those limits should include time and the type of permitted content.
2. Monitor child’s online use utilising the recommendations in Chapter 2-6, including the use of software and apps to protect the child.



3. Open discussion with the child to gain more insight into the source of the addiction, which could be more serious than the addictive behaviour and could include bullying and depression.

### **2-6-3-5 Understand that there are Online Addiction Quizzes available to determine a child's potential level of addiction.**

The addiction test provided within is a parent-child test from [www.healthyplace.com](http://www.healthyplace.com) but there are many tests available online for adults and children. A link to a credible online source is provided below:

<http://www.globaladdiction.org/dldocs/GLOBALADDICTION-Scales-InternetAddictionTest.pdf>

#### **Parent-Child Addiction Test**

All questions should be answered using the answer key below. The number to the left of each answer is the value given, for example, if you answered 'Frequently' for Question 1, then attach a value of 3 to that question. Once you have completed all the questions and attached a value add the total for all questions. Based on that total value there is a table at the bottom of the questionnaire that provides the definition of your test score.

Answer key:

1. N/A or Rarely
  2. Occasionally
  3. Frequently
  4. Often
  5. Always
- 
1. How often does your child disobey time limits you set for on-line use?
  2. How often does your child neglect household chores to spend more time on-line?
  3. How often does your child prefer to spend time on-line rather than with the rest of your family?
  4. How often does your child form new relationships with fellow on-line users?
  5. How often do you complain about the amount of time your child spends on-line?
  6. How often do your child's grades suffer because of the amount of time he or she spends on-line?
  7. How often does your child check his or her e-mail before doing something else?
  8. How often does your child seem withdrawn from others since discovering the Internet?

9. How often does your child become defensive or secretive when asked what he or she does on-line?
10. How often have you caught your child sneaking on-line against your wishes?
11. How often does your child spend time alone in his or her room playing on the computer?
12. How often does your child receive strange phone calls from new "on-line" friends?
13. How often does your child snap, yell, or act annoyed if bothered while on-line?
14. How often does your child seem more tired and fatigued than he or she did before the Internet came along?
15. How often does your child seem preoccupied with being back on-line when off-line?
16. How often does your child throw tantrums with your interference about how long he or she spends on-line?
17. How often has your child choose to spend time on-line rather than doing once enjoyed hobbies and/or outside interests?
18. How often does your child become angry or belligerent when you place time limits on how much time he or she is allowed to spend on-line?
19. How often does your child choose to spend more time on-line than going out with friends?
20. How often does your child feel depressed, moody, or nervous when off-line which seems to go away once back on-line?

### **Scoring:**

20-49: (Your child is an average on-line user. He/she may surf the Web a bit too long at times, but you have control over their usage.)

50-79: (Your child is experiencing occasional or frequent problems because of the Internet. You should consider the full impact on your child's life and how this has affected the rest of your family.)

80-100 (Internet usage is causing significant problems in your child's life and most likely your family. These issues need to be addressed now.)

# Quiz

---

**Q1. Which URL helps with limiting access to certain websites?**

- a. [www.computercontrolbar.com](http://www.computercontrolbar.com)
- b. [www.controlbar.com](http://www.controlbar.com)
- c. [www.datachecker.com](http://www.datachecker.com)
- d. [www.parentalcontrolbar.org](http://www.parentalcontrolbar.org)

**Q2. Where is the best place to locate the computer at home?**

- a. Central and open place
- b. Isolated place
- c. Very busy place
- d. Private place

**Q3. Which Microsoft Windows feature helps adults secure children's activity on the computer?**

- a. Access controls
- b. Kids controls
- c. Parental controls
- d. Computer controls

**Q4. True or False: A parent should never read their child's email.**

- a. True
- b. False

---

**Answers Overleaf**

# Answers

---

**Q1. d.** [www.parentalcontrolbar.org](http://www.parentalcontrolbar.org)

**Q2. a.** Central and open place

**Q3. c.** Parental Controls

**Q4. b.** False

## Chapter 2-7

### Virtual Behaviour

2-7-1 Communicating

2-7-2 Cyberbullying

## 2-7 Virtual Behaviour

### 2-7-2 Cyberbullying

#### 2-7-1-1 Understand what Netiquette means.

Netiquette is a combination of net (from the Internet) and etiquette - the informal rules of behaviour when using the Internet. While social media websites have their own formal rules of use, informal practices have developed over the years for using the Internet and include:

- Write clearly, check spelling and use appropriate words - not all users of sites speak the same first language as you do.
- Avoid sentences typed in all capitals.
- Be courteous and polite online.
- Do not send abusive messages or content.
- Remember that your posts are public - they can be read by anyone including your partner, your children, your parents, or your employer.
- Do not spam - do not repeatedly post the same advertisement for products or services.
- Do not post copyrighted material to which you do not own the rights.

Your behaviour online is a representation of you - if you are positive and polite then you will be shown respect.

#### 2-7-1-2 Understand the concept of no take backs once information is posted.

Once information is posted online it stays online; even if it is deleted or modified, the original will never be completely deleted. Never post anything or publish pictures that might later cause you or someone else embarrassment. A friend with access to your social network page can copy private information or an embarrassing photo and post it somewhere else.

Think before you post. If there is any doubt in your mind about what you can or cannot say, keep it to yourself. For example, when you post to Facebook (see Fig. 46 below), think carefully before you post 'What's on your mind?'

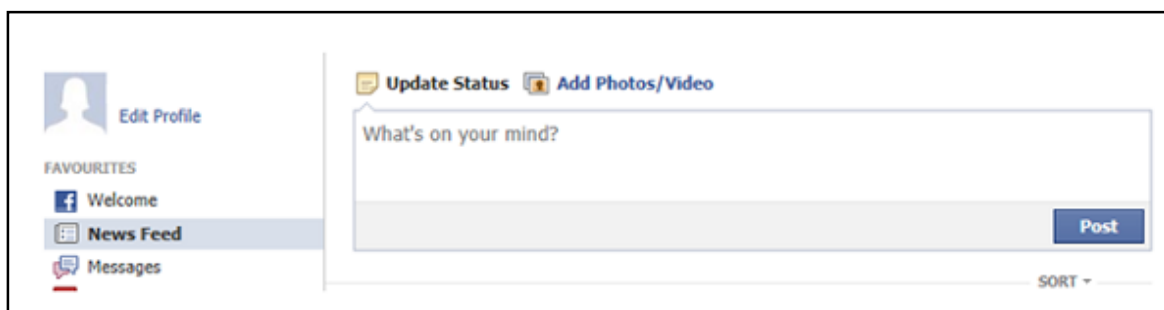


Fig. 46 Facebook - What's on your mind? Post screen.

### **2-7-1-3 Know why smart online user names that reveal only limited personal information are used.**

A good username is reasonably easy to remember but does not reveal any sensitive information about yourself, such as your full name, address, or telephone number. A username containing too much of your name makes it easy to look you up and obtain information about you. You may also consider a creative variation on your name that you will remember, but that others may not recognise.

Username can be used for all kinds of purposes – from relatively straightforward ones like marketing to malicious ones like identity theft. Your personal information could be used by online predators to expose users to inappropriate content.

By adopting a smart online name you do not need to disclose personal information about yourself.

### **2-7-1-4 Recognise why protecting personal information, and maintaining privacy is always important.**

Sharing too much personal information online can lead to identity theft that could result in criminals being able to obtain credit, goods and services in your name. If an online predator were to get enough information about a child, the predator could identify their home address or school, this could make the child a possible victim of cyberbullying, stalking, physical abuse and possibly kidnapping.

Always protect your personal information, and that of your children.

### **2-7-1-5 Beware of adding strangers to Buddy/Friend lists, and the risks.**

Friends are not always friends, 'friend' is just a word for a contact, true friends are people you meet face to face and can trust. Remember that every new friend can access your profile and adding friends of friends increases the chance of strangers seeing your personal information.



## 2-7 Virtual Behaviour

### 2-7-2 Cyberbullying

#### 2-7-2-1 Recognise and understand cyberbullying.

Cyberbullying is the use of the Internet and related technologies, such as social media, to harm other people in a deliberate, repeated and hostile manner. Examples of what constitutes cyberbullying include communications that seek to intimidate, control, manipulation, putting someone down, falsely discrediting someone, or humiliating the recipient. This could include:

- Continuous unsolicited email to a person.
- Inappropriate text or SMS messages.
- Humiliating a person within a forum.
- Disclosing a person's personal details.
- Impersonating another person.

Social media platforms raise awareness of cyberbullying to help protect users, for example Google+ users have set up a community group called STOP Cyberbullying (see Fig. 47 below) to engage users to share ideas about how to stop it.

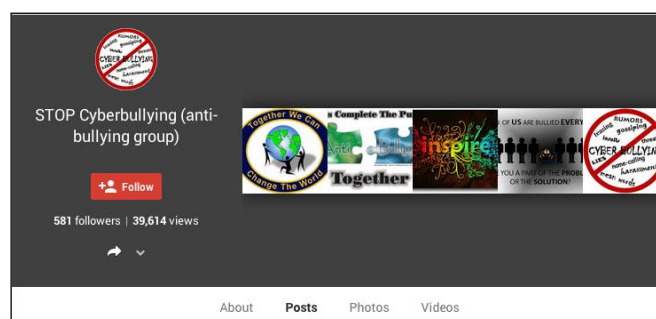


Fig. 47 Google+ Community Group - STOP Cyberbullying  
<https://plus.google.com/114933068076498476678/posts>

#### 2-7-2-2 Understand the media through which cyberbullying can occur.

Cyberbullies use all Internet technologies to attack their victims, these includes all social media networking sites, text messages, email, instant messaging (IM), chatrooms, online polls, websites, picture messages, and message boards - used through PCs, laptops, tablets, smartphones, or any device that is connected to the Internet.

### **2-7-2-3 Understand the speed with which information / pictures can spread and the impact of cyberbullying.**

A text message or a photograph on a smartphone can be sent to all contacts in the phonebook at once. If one person sends a message to 16 people who in turn send it to another 16 who each then send it to another 16 people (16x16x16) - over 4,000 will see the message.

Cyberbullying can cause anxiety, depression and there are well-documented cases that have resulted in the suicide of the victim.

Ryan Halligan was a 13-year-old boy who took his own life as a result of being bullied online is just one example of a young person who could not cope with the severe emotional impacts of being victimised by cyberbullying, (<http://www.ryanpatrickhalligan.org/index.htm>).

### **2-7-2-4 Understand the consequences of cyberbullying. Understand the motives for bullying online, such as anonymity or the bully feeling they are 'above the law'. Understand that online bullying can also be a two way process.**

Cyberbullying has consequences on the perpetrator, and of course the victim. Those consequences could be legal, emotional and possibly physical if the two parties know each other personally. Also remember that bullying is not always a one-way street, which means the initial victim might end up bullying back worse than the initial instigator.

It can be easier for bullies to do so online due to the 'anonymity' factor allowing them to set up false identities, which gives the bully a sense of being able to get away with it without consequence.

Motives for cyberbullying differ and therefore the responses are different to each of the reasons motivating the child. Motives could be:

- Anger
- Frustration
- Revenge
- Boredom
- Entertainment
- Power

### **2-7-2-5 Recognise the warning signs of cyberbullying.**

Cyberbullying is not something your children might be able to escape or avoid; therefore it is vital that you monitor their behaviour and their normal use of technology.

A child might be experiencing cyberbullying if he or she:

- Experiences mood swings or could be anxious especially after using the Internet or a mobile phone
- Increasingly reports symptoms of illness
- Appears uneasy about going to school or outside in general
- Becomes abnormally withdrawn from social activities
- Gradually begins to drop in grades or academic performance
- Appears upset after using a computer or being online with a phone or mobile device

### **2-7-2-6 Know how to counter cyberbullying, how to record it and report cyberbullying concerns to the appropriate authorities.**

What else can you do to protect yourself and your friends from cyberbullies?

- Only open emails and texts from people you know.
- Don't forward chain emails or hoaxes.
- Don't post anything that is very private.
- Never respond to bullying emails or texts, this will only encourage the cyberbully.
- Block the bully – many apps have settings that block emails, SMS, or texts from specific people.
- Keep the messages – you do not have to read them but they are evidence of such messages.
- Report abuse to the website or mobile phone operator, report serious issues to the police, or show someone in authority the type of communication you have received and let them decide on the next step.
- Limit the information you post online.
- Set your privacy settings very carefully.

When people, particularly children and young people, are the targets of bullying via mobile phones or the Internet, they can feel alone, particularly if the adults around them do not understand cyberbullying and its effects. By encouraging other students to report cyberbullying to a responsible adult or to a report it to a local or online authority and never responding directly to a cyberbully, you take control of the situation.

### **2-7-2-7 Understand how to deal with children who bully others online.**

If your child is a bully, that doesn't necessarily mean you are a bad parent. You should just keep in mind that traditional punishment including grounding them in their room is not very effective.

There are several things as a parent that you can do initially to try to stop this behaviour.

- Ensure the child understands that the behaviour of cyberbullying is unacceptable. Ask them how they would feel if someone did the same thing to them?
- Try to understand why the cyberbullying occurred. Some situations evoke strong emotions and this might be a single instance such as your child being bullied and it was a defensive reaction.
- Explain the severity of their actions and indicate that law enforcement or school authorities might be involved.
- Ask them to stop this behaviour immediately.
- Monitor their activity online including their mobile devices such as a smart phone.

Things you should do for future reference:

- Increase your knowledge of technology. If you don't understand the tools your child uses you cannot protect them from the potential threats they are exposed to on a daily basis.
- Learn about relevant legal issues by researching online through government and third party websites.
- Share your concerns with your child's school teacher, counsellor, and principal when necessary.
- Understand that the problem could be more serious and involves emotional or developmental issues that need to be addressed by a medical practitioner.

### **2-7-2-8 Recognise that adults can also suffer from cyberbullying.**

Adult bullying is more prevalent than most want to admit. In one case, a parent felt the need to put some of her secrets (good and bad) online, and that was rebroadcast publicly until her own children saw those posts! Another involved women taking to Facebook to criticise pictures of toddlers they felt inappropriate. These are all forms of bullying and can detrimentally affect the victims. Cyberbullying is the same for all age groups and can be conducted through social networking sites, emails, messages or any other online forums.

Cyber stalking is another dilemma faced by people. Stalking in general is the act of an individual following, watching, and bothering someone constantly in a manner that is frightening or dangerous. This can also occur online through repeated messaging, constant monitoring and unwelcomed interactions. Cyber stalking is typically accompanied by real-time stalking. In both cases they tend to be criminal offenses and you can seek protection from your local authorities.

Social engineering, as described in Section 2-4-4-3 differs from cyber stalking in one main and important point. Social engineering is a method that attracts the trust of the person and creates a relationship based on that trust, while cyber stalking is an act that is blatant and quickly becomes an annoyance and later a potential danger.

# Quiz

---

**Q1. What term describes how a photo cannot completely be removed once posted online?**

- a. No call back
- b. No take back
- c. No post back
- d. No delete back

**Q2. If you are using just your first name on an online forum, what is it called?**

- a. Smart username
- b. Partial username
- c. Anonymous username
- d. Abbreviated username

**Q3. You have received some very hurtful and offensive text messages on your phone. What is this called?**

- a. Cyberbullying
- b. Harassing
- c. Aggravating
- d. Pharming

**Q4. What should you do if you experience cyberbullying?**

- a. Ignore it
- b. Report it
- c. Respond to it
- d. Forget about it

---

**Answers Overleaf**

# Answers

---

**Q1. b. No take back**

**Q2. a. Smart Username**

**Q3. a. Cyberbullying**

**Q4. b. Report it**

## Chapter 2-8

### Policy

2-8-1 Usage

2-8-2 Copyright



## 2-8 Policy

### 2-8-1 Usage

#### 2-8-1-1 Understand what an Acceptable Usage Policy (AUP) is and why it is important in schools.

An Acceptable Usage Policy (AUP) is a set of rules that a user must agree to follow in order to gain access to a network or to the Internet. It is common practice for schools to require you to sign a contract before being granted a network ID. AUPs are designed to protect users and set out what is acceptable and what the sanctions are for breaking the rules.

With the current use of computer technology in the classroom, many schools are facing a greater liability regarding technology and online learning. School AUPs outline rules regarding Internet use on school property, and normally include personal safety, illegal activities, system security, privacy, plagiarism, copyright infringement and access to inappropriate materials. The policy should also state that the school's technology property is for educational purposes only. Students' rights, such as free speech, access to information and due process, should be outlined in the Policy, along with the consequences for violating the AUP.

Social media networking sites have AUPs, Twitter publish theirs under their Rules and Policies, see Fig. 48 below:

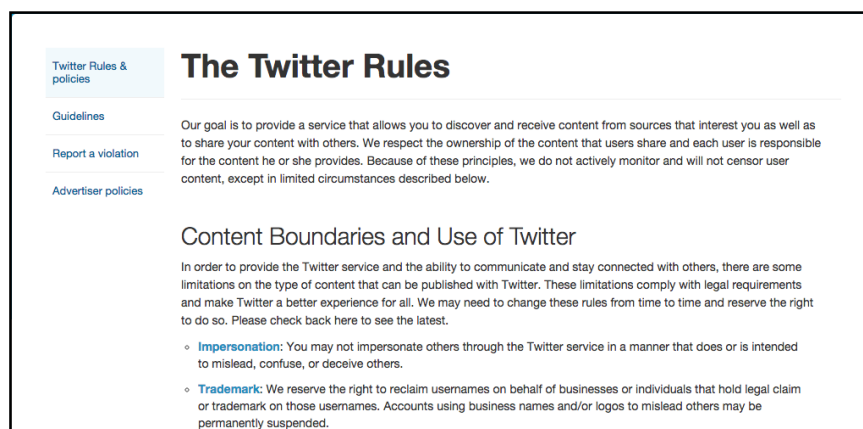


Fig. 48 Example: Acceptable Use Policy - Twitter rules.  
(<https://support.twitter.com/articles/18311-the-twitter-rules>)

### **2-8-1-2 Know the components of a good AUP: educate students, minimise risk, encourage netiquette & appropriate social & ethical behaviour, protect vulnerable children, personal identity, password protection.**

A good AUP should incorporate:

- The use of computers and personal devices, including the use of anti-virus software;
- Access to and the use of the Internet;
- The informal rules of behaviour when using the Internet (netiquette);
- Rules regarding the use of social media networks, creating online identities and protecting usernames and passwords;
- Downloading material including copyrighted content;
- Privacy rules;
- Unacceptable behaviour

Unacceptable behaviour may include, for example, the creation and transmission of offensive documents or images or material which is designed to cause annoyance. Other prohibited behaviour could include anything that infringes the copyright of another person and deliberate unauthorised access to other services using the connection to the Internet.

### **2-8-1-3 Understand mobile operator moderation policies with regard to access to chatrooms or games and control of spam.**

Chatrooms and online games have moderators whose job it is to look for proof of age for new users. Moderators also monitor conversations and can suspend users for profane language, bullying or harassing other users and spamming the chatroom. If you feel that you are being harassed or bullied, inform the moderator immediately.

An example of a chatroom is Google's Paltalk, see Fig. 49 below:



Fig. 49 Mobile chatroom example - Paltalk <http://www.paltalk.com/>

Paltalk publishes policies for moderating chats, the following is an extract from <http://www.paltalk.com/support/RoomAdmin.html>:

Most chatrooms will have moderators or administrators ('admins' for short). A chatroom admin is distinguished by having an @ sign precede their name. A chatroom admin helps to control the room, they direct the topic of conversation or control who gets to speak to the room on the microphone next.

Admins of chatrooms have various controls that allow them to control features and speaking order in the room. They can use the red dot to control who can speak, send video, or send messages in text. A chatroom admin can also bounce or ban a user from the room if they are being offensive or disruptive.

All mobile operators have similar policies which aim to moderate conversations.

## 2-8 Policy

### 2-8-2 Copyright

#### **2-8-2-1 Be aware of copyright laws and their impact for illegal downloads using file sharing services.**

Copyright is the exclusive right of an author to make copies, license, and otherwise exploit a literary, musical, or artistic work. An author can transfer the copyright to a publisher or to another person. Only the copyright holder has the right to make copies, everyone else needs permission which is usually granted for a fee, known as royalties.

The illegal downloading of content has become one of the greatest problems of the digital age. Its impact is being felt across all forms of digital media and content: film, music, books etc. Downloading involves clicking on a music, video or book file from legitimate service providers such as iTunes and Amazon, paying a fee for use of the file and then downloading it to a computer system and reusing it on iPods, game machines, mobile phones or computers, depending on the licence issued.

#### **2-8-2-2 Recognise that pirating of music, movies and software is illegal, along with its implications.**

Some material on the Internet is in the public domain which means that it can be copied and used without restriction; this includes literature, music, images (including movies) and software. If material is copyrighted it is illegal to make copies of any sort. If you do you are liable to prosecution in the courts and in some countries you can have your Internet service suspended.

Online piracy is a growing problem in the online community; an average iPod contains pirated music worth \$800.

Visit the Online Piracy in Numbers blog site for more information: - <http://www.go-gulf.com/blog/online-piracy/>

# Quiz

**Q1.** The document that details the rules of use and that you must agree to before obtaining access to a network has the acronym AUP. What does AUP stand for?

- a. Acceptable Use Principles
- b. Acceptable Usage Program
- c. Acceptable User Policy
- d. Acceptable Usage Policy

**Q2.** Consider the following statement: Everything on the Internet is free. Indicate whether you think this is true or false.

- a. True
- b. False

**Q3.** Who has the right within an online forum or chatroom to suspend a conversation thread?

- a. Controller
- b. Moderator
- c. Leader
- d. User

**Q4.** What is the term used to describe the exclusive right to duplicate or license literary or artistic work?

- a. User's right
- b. Printing right
- c. Copyright
- d. Artistic right

---

Answers Overleaf

# Answers

---

**Q1. d.** Acceptable Usage Policy (AUP)

**Q2. b.** False

**Q3. b.** Moderator

**Q4. c.** Copyright

## Exercises

**2-E-1 Facebook**

**2-E-2 Twitter**

**2-E-3 YouTube**

**2-E-4 Google+**

**2-E-5 LinkedIn**

**2-E-6 Blogs**


***Note: Instructions and images contained in this chapter should be used as guidance in accomplishing the objectives. Social media platforms can change the order or content of each step at anytime. Therefore, we recommend you review each exercise entirely to understand the objective prior to performing the activities.***

# Social Media (Facebook)

## Exercises

After you have set up your account on Facebook and started adding friends, friends of friends, people you know and others you might not, you need to consider your own safety online. A couple of privacy and safety issues are addressed in the exercise below. Read the steps and let the images guide you through the process.

### Safety Measures on Facebook:

1. On your Facebook homepage, click the little security lock-like symbol link (  ) on the top right window of home menu, where you can see Privacy Shortcuts.

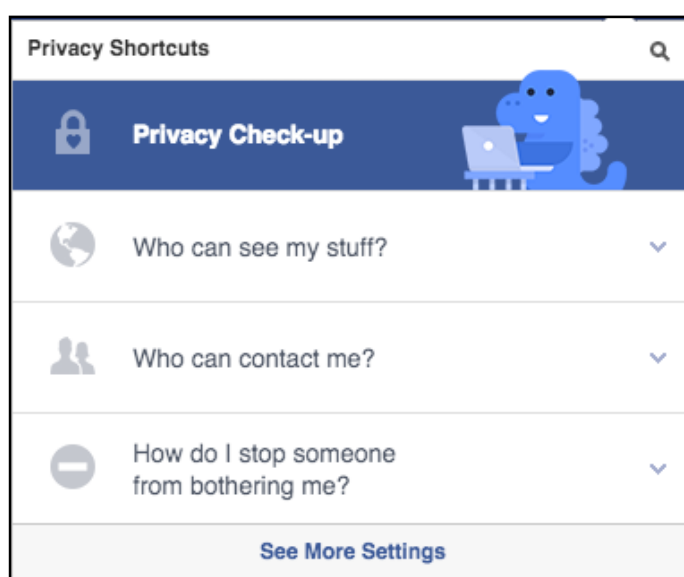


Fig. 50 Facebook Privacy page

2. The first thing you see under the title (as it appears in the Fig. 50) is 'Privacy Check-up', but instead click on 'Who can see my stuff?' and another question will appear about your posts where it's set by default to 'Public'. Here you should click the arrow again and set it to 'Friends' who will be the only ones to see your posts. (See Fig. 51).



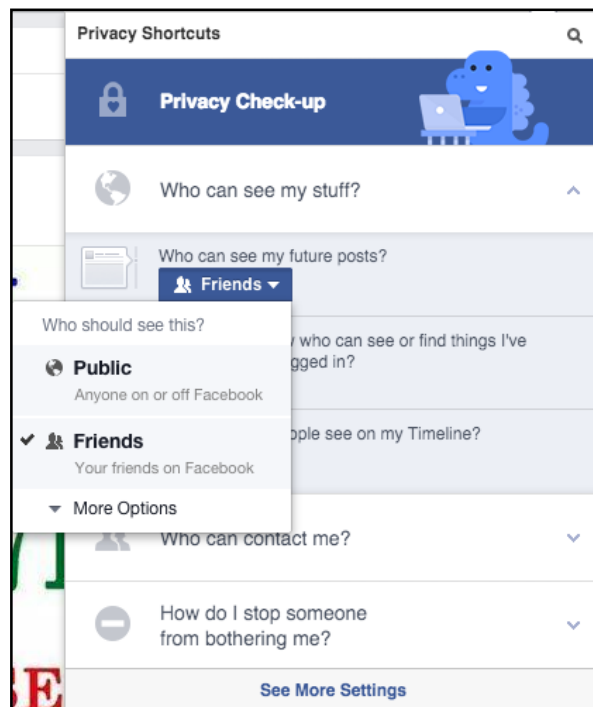



Fig. 51 Facebook Privacy page

3. We learned how to use shortcuts to privacy in the above exercise but now click the 'See More Settings' at the bottom where you will select from the dropdown list 'Privacy' settings; you will notice that there are some common points with the 'Privacy Shortcut' section. (Look at Fig. 52).

<ul style="list-style-type: none"> <li>General</li> <li>Security</li> <li><b>Privacy</b></li> <li>Timeline and Tagging</li> <li>Blocking</li> <li>Notifications</li> <li>Mobile</li> <li>Followers</li> <li>Apps</li> <li>Adverts</li> <li>Payments</li> <li>Support Dashboard</li> <li>Videos</li> </ul>	<b>Privacy Settings and Tools</b>			
	<b>Who can see my stuff?</b>	Who can see your future posts?	Friends	Edit
		Review all your posts and things you're tagged in		Use Activity Log
		Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	<b>Who can contact me?</b>	Who can send you friend requests?	Everyone	Edit
		Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
	<b>Who can look me up?</b>	Who can look you up using the email address you provided?	Everyone	Edit
		Who can look you up using the phone number you provided?	Everyone	Edit
		Do you want other search engines to link to your Timeline?	No	Edit

Fig. 52 Facebook Settings and Tools

4. In the 'Privacy Settings and tools', click on 'Review all your posts and things you're tagged in' which will take you to your timeline page and shows all posts and places where you were tagged a month or even a year ago. If you find that your tag should not appear to all anywhere you can click on the pencil button (  ) and choose the 'Remove Tag' option.
5. Use the 'Who can look me up?' section if you want to limit people searching for your email or phone number on Facebook, or if you want reduce spam from unknown sources. Click on the edit box and choose 'Friends of Friends' or the more limited 'Friends' option. (As in Fig. 53).

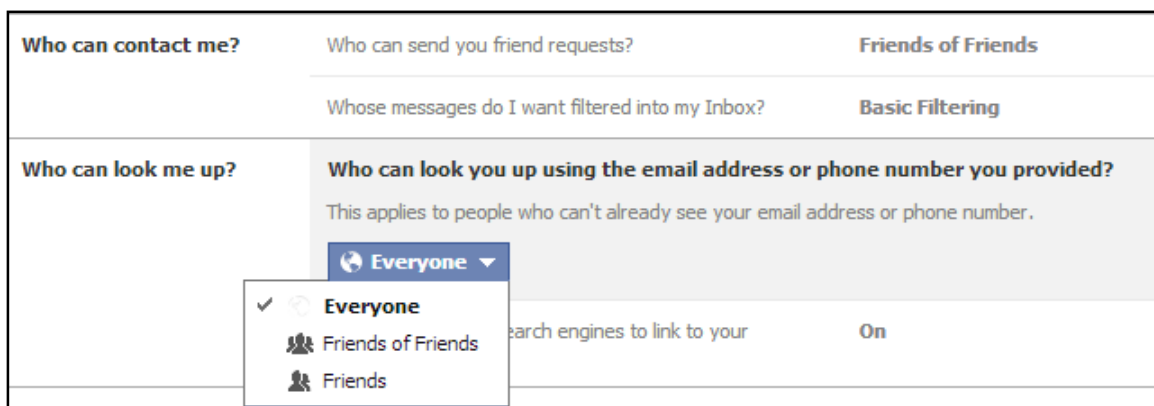


Fig. 53 Who can look me up?

6. 'Who can look me up?' determines if others can look you up through any search engine like Google for example. To make your profile private make sure that the check mark is REMOVED from the box next to the phrase 'Let other search engines link to your timeline'. (Box with checkmark is shown in Fig. 54).

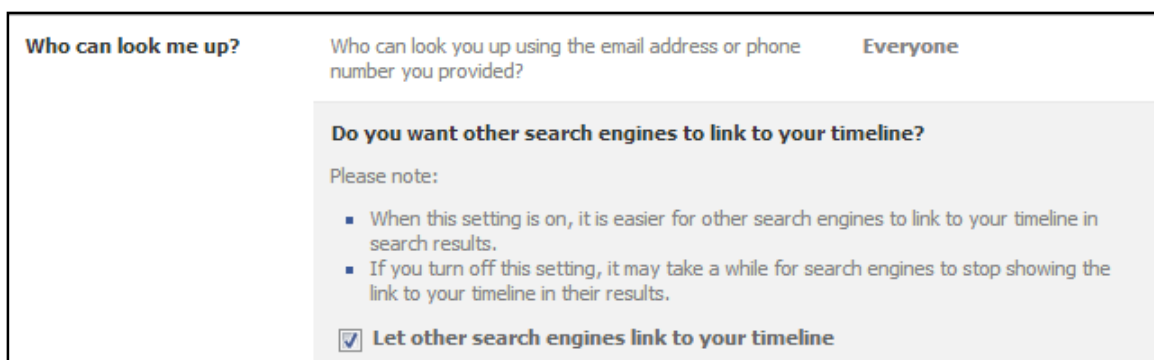


Fig. 54 Facebook privacy settings

7. Another major privacy category is found on the dashboard on the left side of the screen under 'Timeline and Tagging Settings' section where you can control exactly who sees what on your timeline. Note that the timeline is typically a graphic design displaying a list of activities, events, projects, trends, etc. labelled with dates according to a chronological order. When you enter into this section there will appear a table of settings. (Look at Fig. 55).

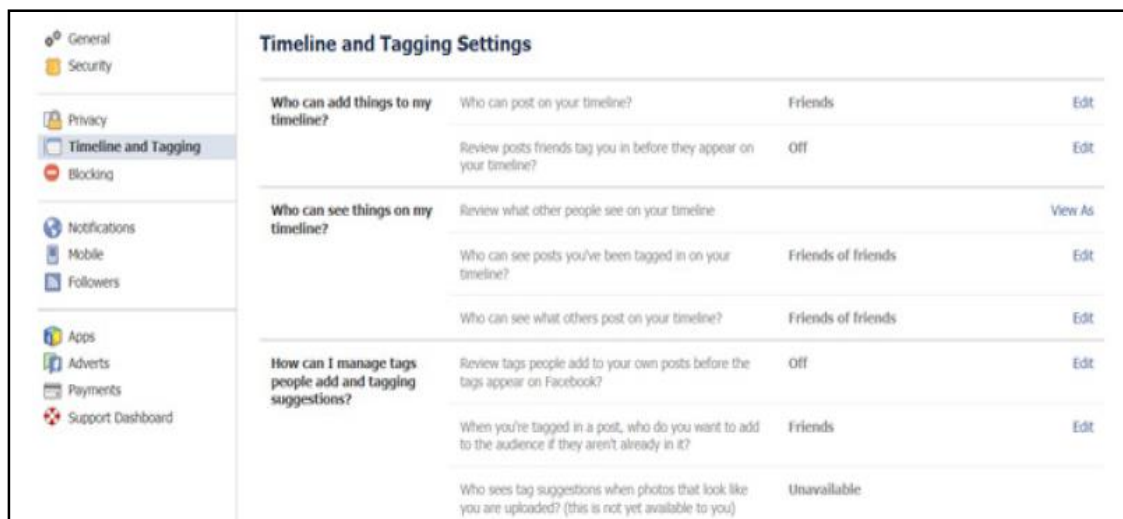



Fig. 55 Timeline and Tagging Settings

8. Under the section 'Who can add things to my timeline?' you can see who is allowed to post on your timeline. To make more private, change this setting to Friends.
9. The 'Review all your posts and things you're tagged in' allows you, as implied in the title, to approve any photos or posts you are tagged in before they appear on your timeline. Once you click 'Edit' to the right you can choose the enabled option from the drop-down menu.
10. Click the  icon to Privacy Shortcuts and scroll down to who can send my friend requests under who can contact me and choose the Friends of Friends option to restrict receiving requests from everyone. (Look at Fig. 56).

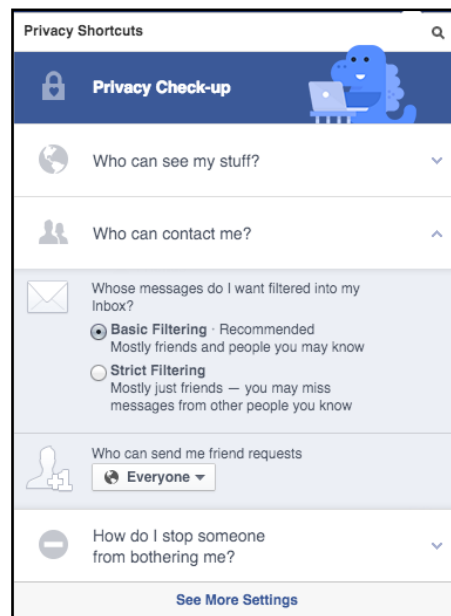


Fig. 56 Facebook Privacy shortcuts

11. The last setting that appears on the Privacy Shortcuts down-drop menu is concerned with blocking issues. Click the arrow near to the question ‘How do I stop someone from bothering me?’ and simply key in the name or the email of the person whom you want to block to unfriend or prevent from starting conversation with or see things you post on your timeline. This setting is of specific importance for parents where they can go through more details under the Privacy Settings option mentioned above to provide their kids with further security. See Fig. 57

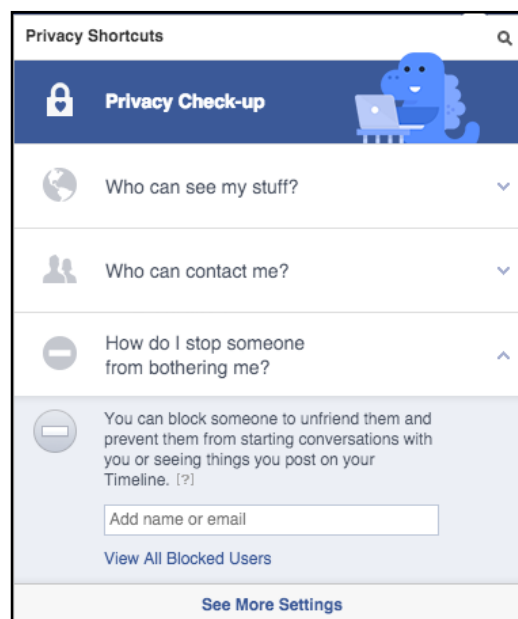


Fig. 57 Add email to block

# Social Media (Twitter)

## Exercises

To manage your privacy settings on Twitter, log in to your account and review several of the default settings. Go to the gear icon at the top right of the screen and select Settings from the pull-down menu. (Look at Fig. 58 below).

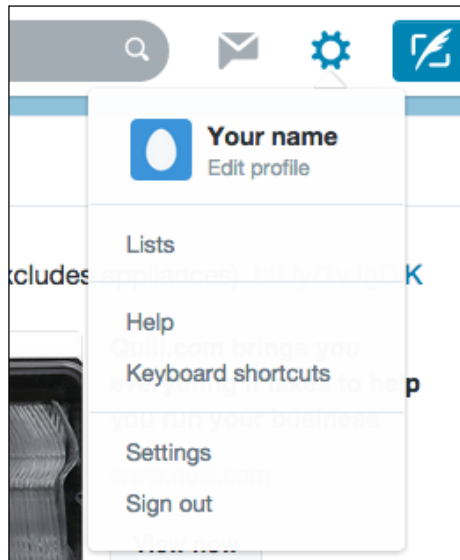


Fig. 58 Twitter Privacy page

1. You will see several setting categories listed on the left, the first of which is 'Account' that is already opened on the right of your screen.
2. Click on 'Security and Privacy' on the right side column, locate the 'Discoverability' option that allows others to find you by your email address at the bottom of the page. It is up to you to choose to check the box or not. (Look at Fig. 59).

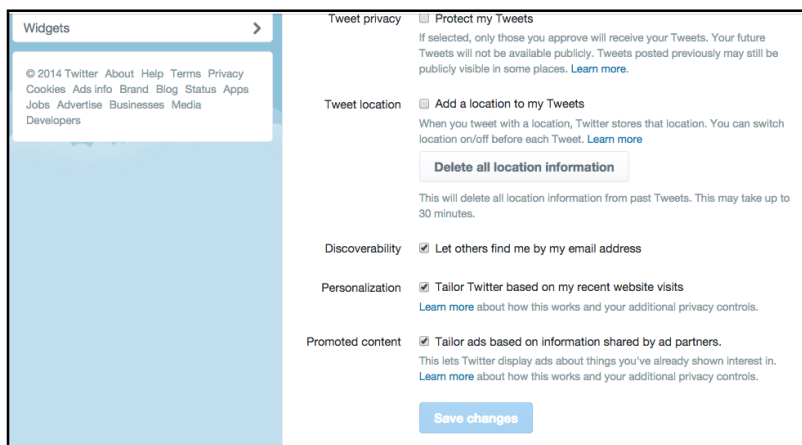


Fig. 59 Twitter Security and Privacy

Under the 'Security' and 'Privacy' sections, you can choose whether to show your location when tweeting through checking the square box to the left of Add location to my Tweets. (As in Fig. 60 below). Note that adding location to your tweets can leave you exposed to predators, so it is recommended to leave this box unchecked.

Fig. 60 Twitter Photo tagging


3. Under the 'Tweet Privacy' option, if you choose to protect your tweets then you are tweeting a specific group of people whom you approve while prohibiting the public from seeing them. This is of great importance to parents to protect their teens from people they are interacting with on Twitter.
4. Do not forget to 'Save Changes' when you are done editing. You may need to re-enter your password as confirmation.


The next settings category on the left menu is 'Password' where you can change your password if necessary.

1. Type your current password.
2. Type a new one and confirm it making sure that you have chosen a complicated one not easily guessed.
3. Saving changes is a must.

Selecting 'Profile' from the left side menu shows several options. (As in Fig. 61below)

**Profile**  
This information appears on your public profile, search results, and beyond.

**Photo**  **Change photo** ▾  
This photo is your identity on Twitter and appears with your Tweets.

**Header**  **Change header**  
Recommended dimensions of 1252x626  
Maximum file size of 5MB  
Need help? [Learn more](#).

**Name**   
Enter your real name, so people you know can recognize you.

**Location**   
Where in the world are you?

**Website**   
Have a homepage or a blog? Put the address here.

**Bio**   
About yourself in 160 characters or less. 160

Fig. 61 Twitter profile settings

1. Your photo comes first. Choosing to add a photo or changing the old one or even leaving it blank is your choice completely.
2. You can fill in the categories accordingly following the on screen guide. Take into consideration while doing so what you are revealing on your Twitter page.
3. As with previous options, you need to 'Save Changes' at the end.

**Save changes**

Because tweets are limited to a maximum of 140 characters, people often use links shortened services to reduce websites URLs. However, as a result, the reader cannot immediately see the true link destination and can sometimes be directed to malicious websites.

### As a precautionary measure:

Hover your mouse over the link in the tweet and check the website destination that appears before clicking it. (As you can see in Fig. 62).



Fig. 62 Hover to check link

Do not forget to 'Sign Out' of the site when you are done.

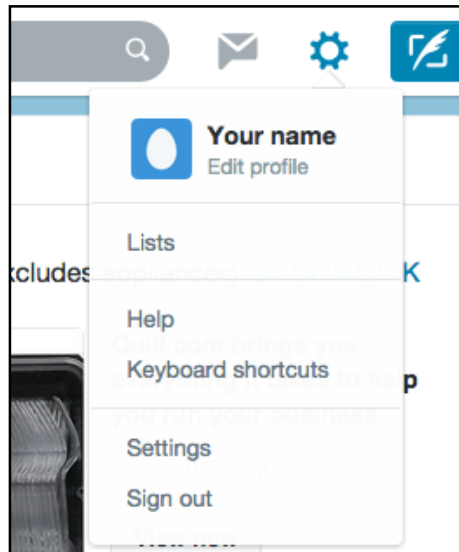


Fig. 63 Sign Out



# Social Media (YouTube)

## Exercises

Once you log into your YouTube account, you can enjoy a multitude of features on the site and maintain your privacy at the same time.

As with other social media platforms discussed earlier, you have to:

1. Click on your profile photo on the right upper side of the screen and select YouTube settings from the YouTube list.

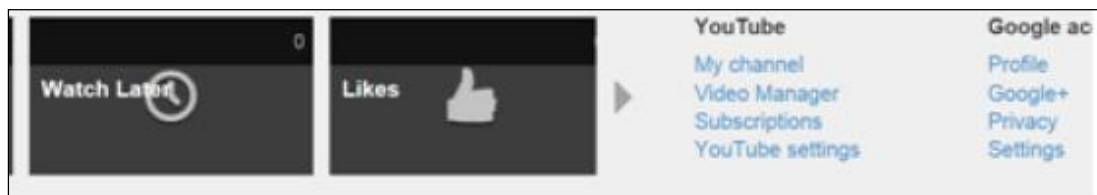


Fig. 64 YouTube settings

2. Select the 'Privacy' option from left side dashboard under 'Account Settings'.
3. You may check the Keep all my subscriptions private under 'Likes and Subscriptions', if you do not want to share them with others. (As shown in Fig. 65 below).

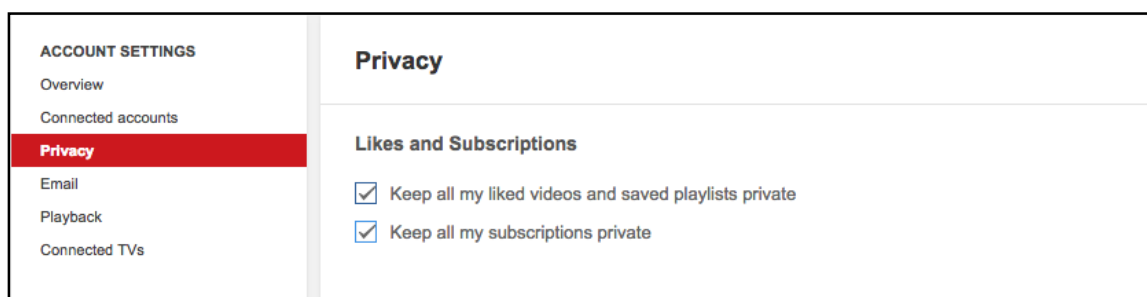



Fig. 65 YouTube Privacy

4. Do not forget to save changes you have made.
5. Remember that signing out of any account contributes to your safety online. You can simply do that by going back to your profile photo clicking on it and selecting the sign out option.

# Social Media (Google +)

## Exercises

As with any social networking service, it's important to understand the potential risks of what you share with others. Here are some recommendations that might be of great help.

1. From the Home screen on Google+ click on  Home on the top left hand just below Google+ and choose 'Settings' from the drop down list. (See the Fig. 66 below).

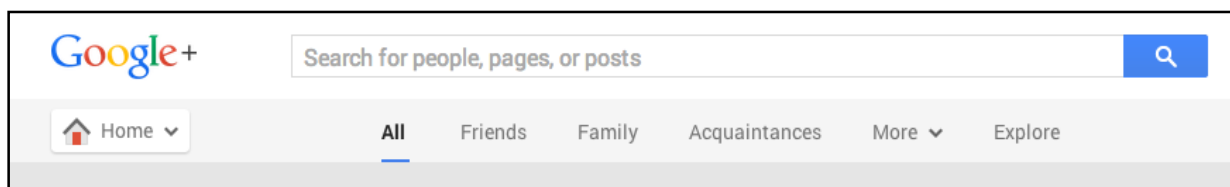


Fig. 66 Google Plus Settings

2. Scroll down to 'Profile'.

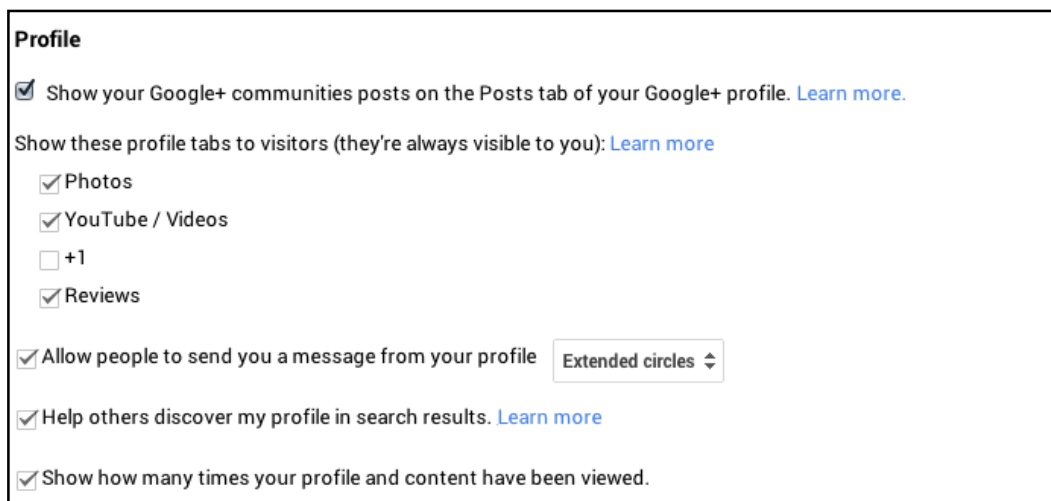




Fig. 67 Google Plus Profile

3. Uncheck the 'Help others discover my profile in search results' in the figure above to create a more private profile on Google+. This will stop Google and other search engines from indexing your profile.

On the 'People' screen accessed from the Home screen on Google+ click on  Home  on the top left hand just below Google+, you have to click on the 'Your circles' button.

1. Clicking on this button will take you to another Circles page (See Fig. 68 below). You choose any of the persons in any of the shown circles.

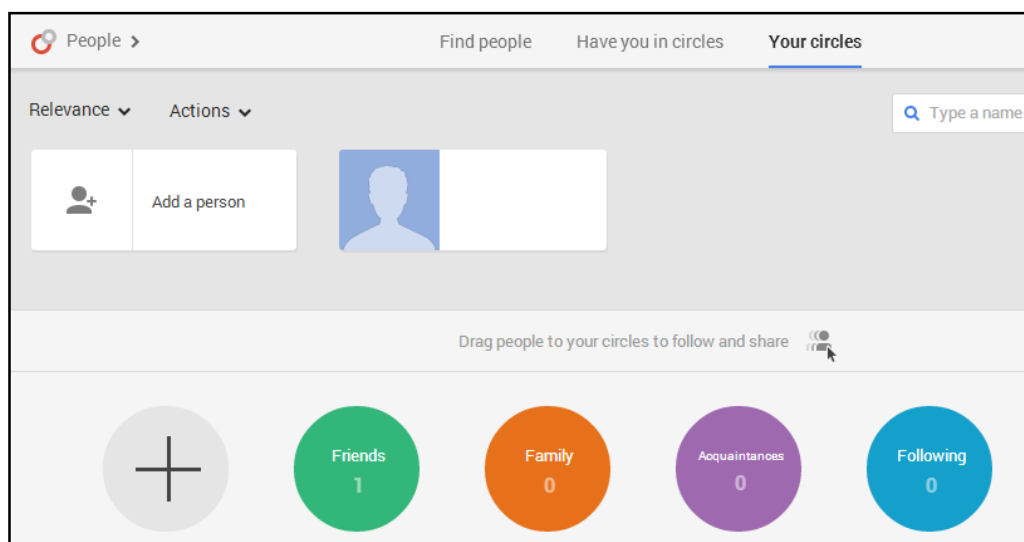


Fig. 68 Google Plus Settings

2. Then, you have to click on the down-arrow inside the 'Actions' button on the upper left corner of the screen.
3. You can select whether you want to (remove/view profile/block, etc.) the chosen person. (See Fig. 69 below).

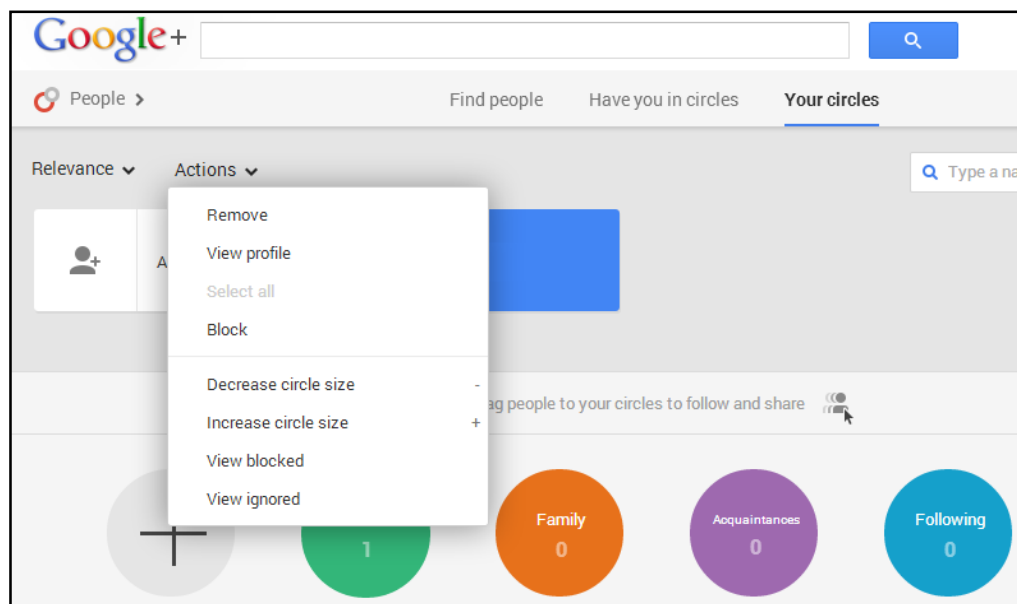


Fig. 69 Google Plus Remove/View profile/Block

4. You can within the same option ('Actions') choose to view the blocked and ignored persons as well.

Under 'Photos and Videos' category on the 'Settings' page, you can make modifications to access and options. (Look at Fig. 70 below)

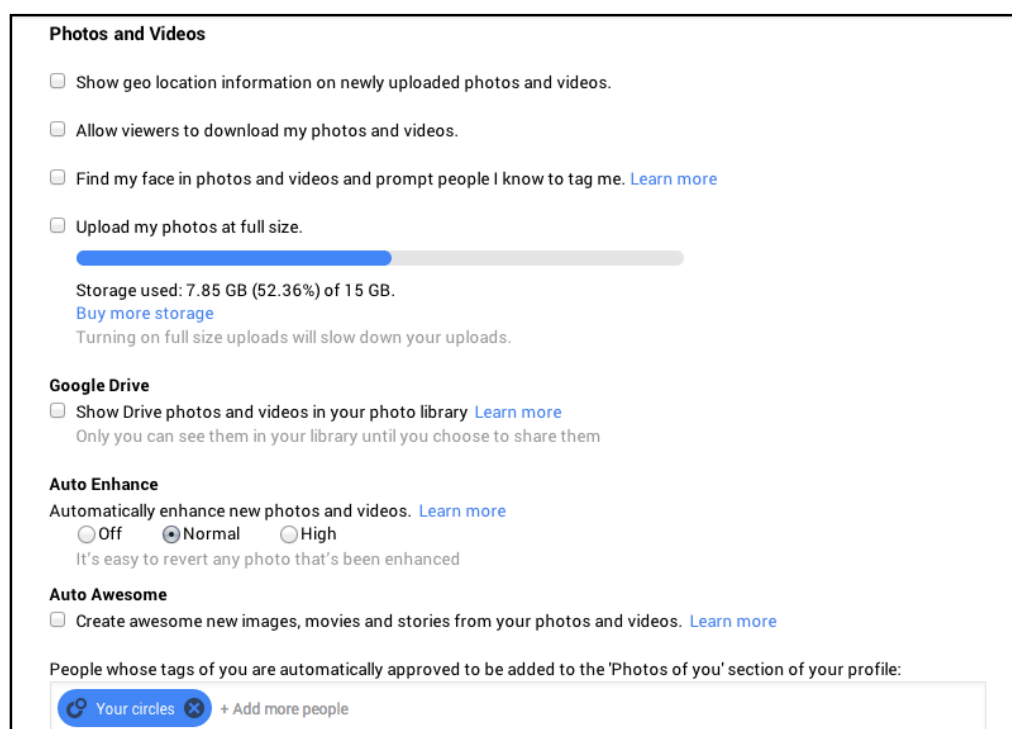


Fig. 70

1. Now move up to the top of the 'Settings' page concerning interaction and posts. Click the button next to the first question, with the double directed arrows where you can choose from the dropdown menu the groups who can send you notifications. (As shown in Fig. 71 below).

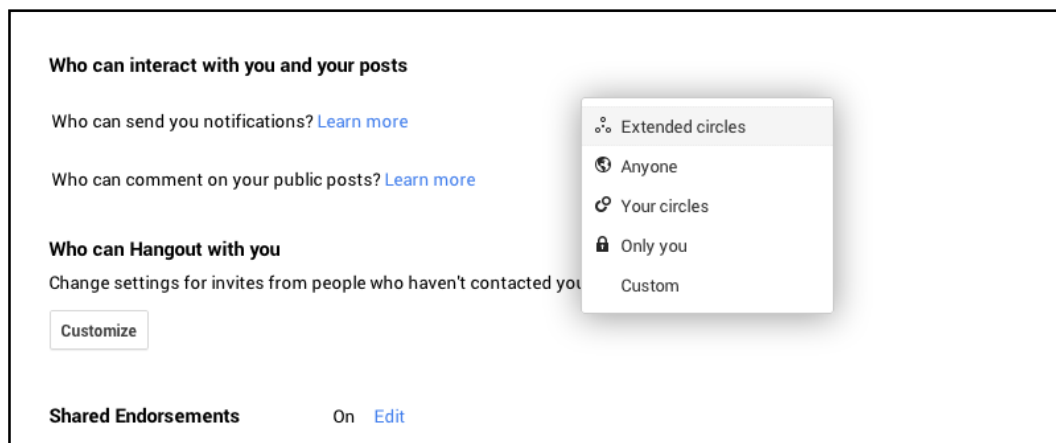


Fig. 71

2. Typical setting option is 'Extended circles' but you can also hit the "Anyone" button to allow anyone to send you notifications. It is recommended to choose 'Your Circles' option for a more private profile.
3. You should look at the rest of the list to understand the options available and make adjustments appropriate to your comfort levels.

Don't forget to log out of the site when done by clicking on your name on the upper right hand of the screen and selecting the 'Sign Out' button.

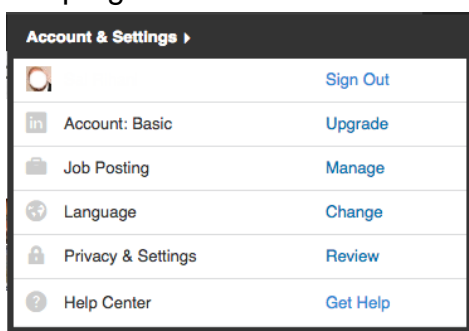
# Social Media (LinkedIn)

## Exercises

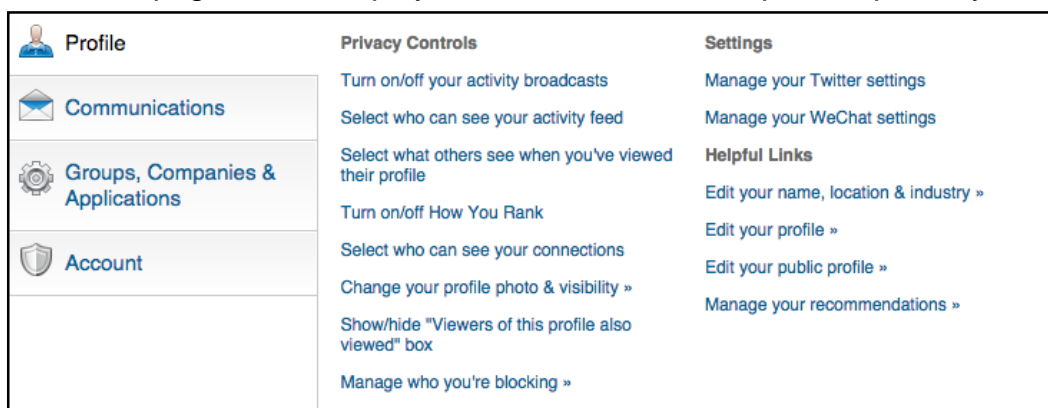
LinkedIn is a professional networking where 'faux pas' (mistakes) can damage your career and ignored privacy issues can jeopardize the whole profession.

It's crucial to follow the steps below for your own protection and safety online, knowing that we introduce the concept along with practical steps and leave the rest for you to explore on your own.

1. After you log onto your LinkedIn account, you need to hover your mouse on top of your profile picture on the top right of the screen and choose 'Privacy & Settings'.



2. Another page will be displayed on the screen with options open to you.



### Profile

Under 'Profile' 'Privacy Controls', click 'Turn on/off your activity broadcasts' option. A window with the sentence 'Let people know when you change your profile, make recommendations, or follow companies' (see the figure below)

**Activity broadcasts** [X]

By selecting this option, your activity updates will be shared in your activity feed.

☒ Let people know when you change your profile, make recommendations, or follow companies

Note: You may want to turn this option off if you're looking for a job and don't want your present employer to see that you're updating your profile.


[Save changes](#) or [Cancel](#)

If you choose to turn this option on by checking inside the small box, then every one of your direct connections will be notified on every change to your profile. However if you'd rather keep it off in case you don't want your current employer to get alerted on any perfection on your LinkedIn profile. Note that you have to 'Save Changes' for any of the two options.

3. Select "What others see when you've viewed their profile" setting another window will display on your screen three options:


**What others see when you've viewed their profile** [X]

☒ Your name and headline (Recommended)

 **Firas**  
--  
United Arab Emirates

☐ Anonymous profile characteristics such as industry and title

Note: Selecting this option will disable Profile Stats. Whenever you switch to anonymous, your viewer history gets erased.

 **Someone on LinkedIn**

☐ You will be totally anonymous.

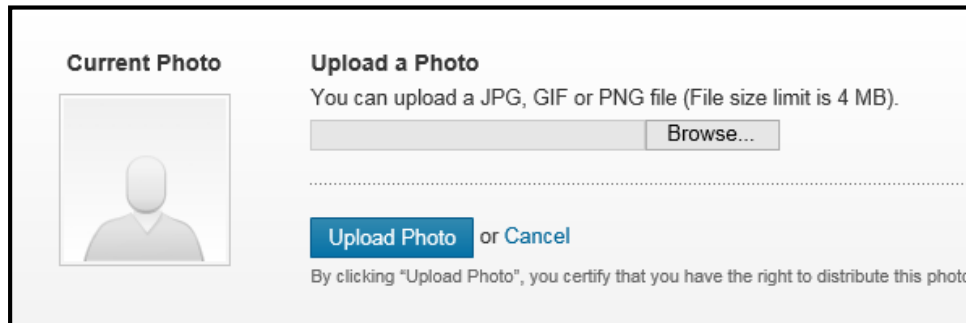
Note: Selecting this option will disable Profile Stats. Whenever you switch to anonymous, your viewer history gets erased.

[Save changes](#) or [Cancel](#)

- Your name and headline (this is the only option recommended, by clicking inside the circle, just to let the person who's profile you have viewed know that you have been by).
- Anonymous profile characteristics will only show the industry and title.
- Totally anonymous is the third option, which you may select as well that erases all history that you viewed someone's profile.

4. Don't forget to 'Save Changes' in the end.

Under 'Change your profile photo & visibility' option, you have the ability to:  
(See the figure below)

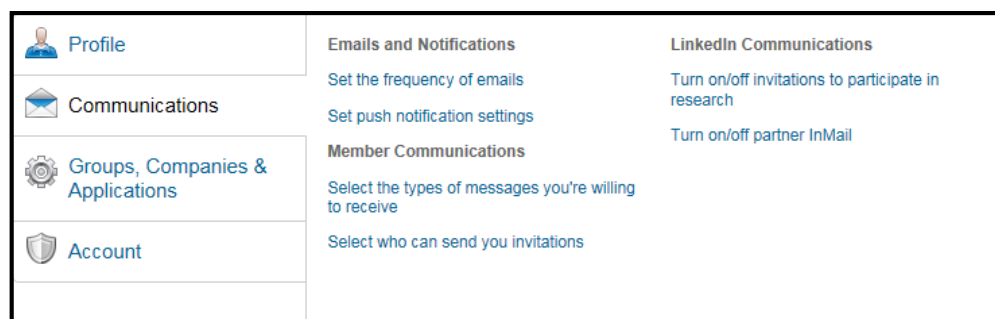


The screenshot shows the 'Current Photo' section with a placeholder image of a person. To the right, the 'Upload a Photo' section includes a text prompt: 'You can upload a JPG, GIF or PNG file (File size limit is 4 MB)'. Below this is a 'Browse...' button. Further down, there are 'Upload Photo' and 'Cancel' buttons. At the bottom, a disclaimer states: 'By clicking "Upload Photo", you certify that you have the right to distribute this photo'.

1. Upload one (keeping in mind the professional appearance) and
2. Choose to whom you want it to be visible (everyone option is recommended).
3. 'Save Changes' is a must.

## Communications

You will notice under 'Communications' three main titles,  
(See the figure below):



The screenshot displays the 'Communications' settings page. On the left is a sidebar with four menu items: 'Profile', 'Communications' (which is selected), 'Groups, Companies & Applications', and 'Account'. The main content area is divided into three columns. The first column, 'Emails and Notifications', contains links for 'Set the frequency of emails', 'Set push notification settings', and 'Member Communications'. The second column, 'LinkedIn Communications', contains links for 'Turn on/off invitations to participate in research' and 'Turn on/off partner InMail'. The 'Member Communications' section in the first column includes links for 'Select the types of messages you're willing to receive' and 'Select who can send you invitations'.

- **Emails and Notifications**
- **Member Communications**
- **LinkedIn Communications**

1. Click on 'Select the types of messages you are willing to receive' under 'Member Communications'.
2. In the window that appears on your screen, it's recommended that you choose the 'Introductions and InMail only' option; checkmark the opportunities suitable for you; and 'Save Changes'.



**Types of messages you're willing to receive** [X]

MESSAGES

☒ Introductions and InMail only (Recommended)

☐ Introductions only

OPPORTUNITIES

<input checked="" type="checkbox"/> Career opportunities	<input checked="" type="checkbox"/> New ventures
<input checked="" type="checkbox"/> Expertise requests	<input checked="" type="checkbox"/> Personal reference requests
<input checked="" type="checkbox"/> Consulting offers	<input checked="" type="checkbox"/> Job inquiries
<input checked="" type="checkbox"/> Business deals	<input checked="" type="checkbox"/> Requests to reconnect

ADVICE TO PEOPLE WHO ARE CONTACTING YOU

Include advice on your availability, types of projects or opportunities that interest you, and what information you'd like to see included in a request. [See examples.](#)

Save changes or [Cancel](#)

The 'Select who can send you invitations' setting allows you three options: (See the figure below)

**Who can send you invitations** [X]

☒ Anyone on LinkedIn (Recommended)

☐ Only people who know your email address or appear in your "Imported Contacts" list

☐ Only people who appear in your "Imported Contacts" list





Save changes or [Cancel](#)

3. LinkedIn recommends choosing the first option and 'Save Changes'.

## Groups, Companies & Applications

Moving to 'Groups, Companies & Applications' you will notice four categories: (See the fig on following page)





- **Groups**
- **Companies**
- **Applications**
- **Privacy Controls**

 <b>Profile</b>	<b>Groups</b>	<b>Applications</b>
 <b>Communications</b>	<a href="#">Select your group display order »</a>	<a href="#">View your applications »</a>
 <b>Groups, Companies &amp; Applications</b>	<a href="#">View your groups »</a>	<a href="#">Add applications »</a>
 <b>Account</b>	<a href="#">Set the frequency of group digest emails</a>	<b>Privacy Controls</b>
	<a href="#">Turn on/off group invitations</a>	<a href="#">Turn on/off data sharing with 3rd party applications</a>
	<a href="#">Turn on/off notifications when joining groups</a>	
	<b>Companies</b>	
	<a href="#">View companies you're following »</a>	

You may go through each on your own and customize your LinkedIn account accordingly.

## Account

The 'Account' setting includes: (See the figure below)

 <b>Profile</b>	<b>Privacy Controls</b>	<b>Email, Phone &amp; Password</b>
 <b>Communications</b>	<a href="#">Manage Advertising Preferences</a>	<a href="#">Add &amp; change email addresses</a>
 <b>Groups, Companies &amp; Applications</b>	<b>Settings</b>	<a href="#">Manage phone numbers</a>
 <b>Account</b>	<a href="#">Change your profile photo &amp; visibility »</a>	<a href="#">Change password</a>
	<a href="#">Show/hide profile photos of other members</a>	<b>Helpful Links</b>
	<a href="#">Customize the updates you see on your home page</a>	<a href="#">Upgrade your account »</a>
	<a href="#">Select your language</a>	<a href="#">Request an archive of your data »</a>
	<a href="#">Manage security settings</a>	<a href="#">Close your account »</a>


- **Privacy Controls**
- **Settings**
- **Email & Password**
- **Helpful Links**

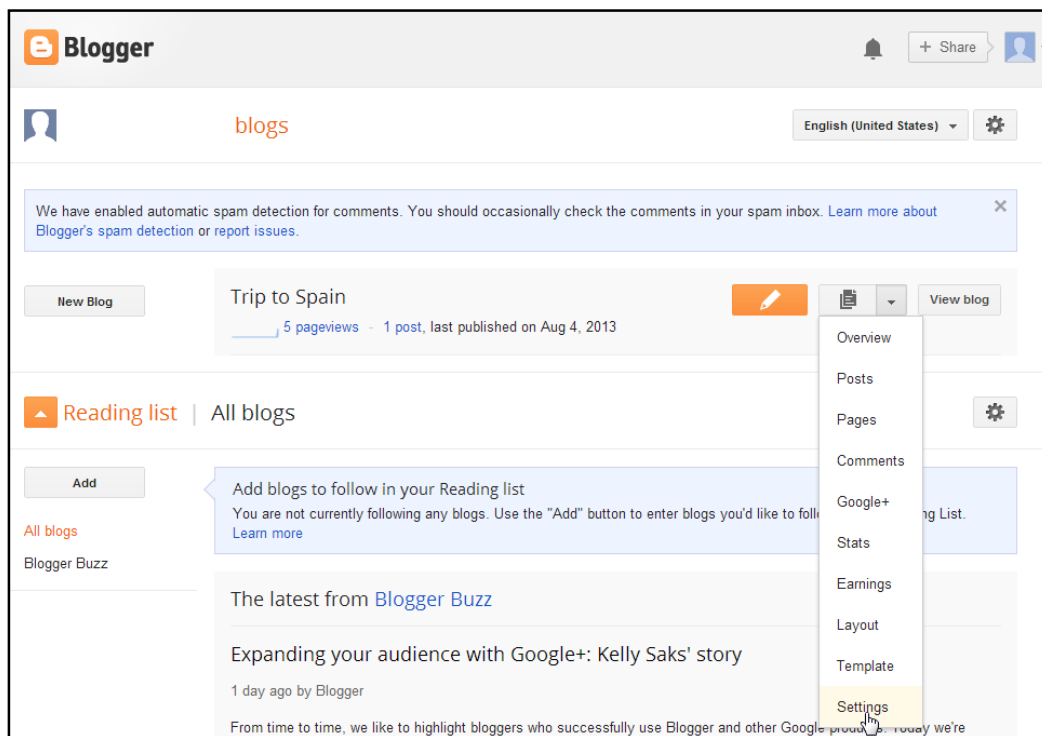
1. You can 'Add & change email addresses' Under 'Email, Phone & Password' section.
2. Under the same title you can 'Change password' by hitting the option and keying in your old one, choosing a new one, making sure that you have chosen a strong password that can't be decrypted easily, and confirming it.

# Social Media (Blogs)

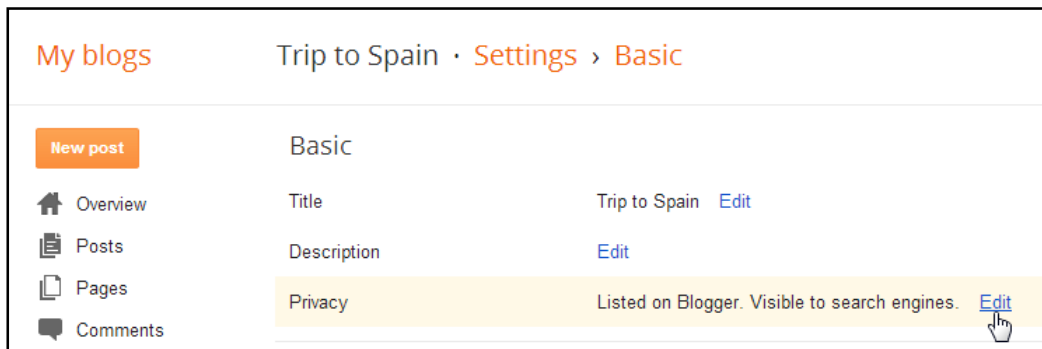
## Exercises

After logging into your blog account:

- 1- Click on the down arrow next to Go to post list (  ) button on the Blogger Dashboard page.
- 2- Select 'Settings' from the dropdown menu. (As shows in the figure. below).



- 3- Click on Edit button parallel to 'Privacy' tab on 'Settings' page. (Look at the figure. below).

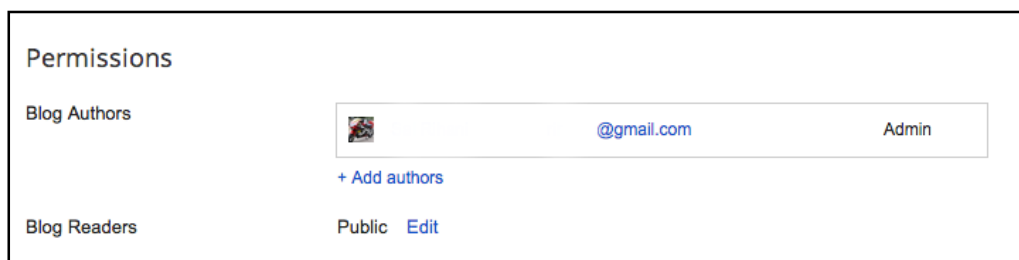


- 4- It is recommended that you choose the 'Yes' option in both questions. (As in the figure. below).

- 5- Save changes.

Scroll down to 'Permissions' tab:

- 1- You will notice that next to 'Blog Readers', it is set by default to 'Public'.
- 2- If you want unrestricted access to readers, it is recommended to keep this option and save changes.



Don't forget to log out each time for safety.