



2020-1-IT02-KA201-079433

RE-EDUCO

IO4 - ACTIVE LEARNING FOR DIGITAL INNOVATION MODULE 1A

ONLINE ESSENTIALS



The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Nicosia, Cyprus, 2022

Responsible Organisation: Cyprus Computer Society ([www.ccs.org.cy](http://www.ccs.org.cy))

Content based on the ECDL/ICDL Online Essentials Module

Author: Dr. George Melillos

Editing: Toumazis Toumazi

Contact: [info@ccs.org.cy](mailto:info@ccs.org.cy)

## TABLE OF CONTENTS

1.	Web Browsing Concepts.....	4
1.1.	Key concepts.....	4
1.1.1.	Understand the structure of a web address. Identify common types of domains like: geographical, organisation (.org, .edu, .com, .gov).....	4
1.2.	Security and Safety .....	5
1.2.1.	Recognise ways to protect yourself when online: purchase from secure reputable websites, avoid unnecessary disclosure of personal and financial information, log off from websites	5
1.2.2.	Define the term encryption .....	6
1.2.3.	Identify a secure website: https, lock symbol.....	7
1.2.4.	Define the term digital certificate .....	7
1.2.5.	Recognise options for controlling Internet use like: supervision, web browsing restrictions, download restrictions .....	8
2.	Web Browsing .....	9
2.1.	Tools and Settings .....	9
2.1.1.	Understand the term pop-up. Allow, block pop-ups .....	9
2.1.2.	Understand the term cookie. Allow, block cookies.....	9
2.1.3.	Delete history, temporary internet files, saved form data. ....	10
2.2.	Bookmarks .....	11
2.2.1.	Add, delete a bookmark / favourite. ....	11
2.2.2.	Show bookmarks / favourites .....	12
2.2.3.	2.2.3.3 Create, delete a bookmarks / favourites folder. Add web pages to a bookmarks / favourites folder.....	12
3.	Web-Based Information .....	14
3.1.	Critical Evaluation .....	14
3.1.1.	Understand the importance of critically evaluating online information. Understand the purpose of different sites like: information, entertainment, opinion, sales .....	14
3.1.2.	Outline factors that determine the credibility of a website like: author, referencing, up-to-date content.....	14

3.1.3.	Recognise the appropriateness of online information for a particular audience .....	14
3.1.4.	Copyright, Data Protection .....	15
3.1.5.	Define the terms copyright, intellectual property. Recognise the need to acknowledge sources and/or seek permission as appropriate .....	16
3.1.6.	Recognise the main data protection rights and obligations in your country .....	16
4.	Communication Concepts .....	17
4.1.	Online Communities .....	17
4.1.1.	Understand the concept of an online (virtual) community. Identify examples like: social networking websites, Internet forums, web conferencing, chat, online computer games.....	17
4.1.2.	Outline ways that users can publish and share content online: blogs, microblogs, podcasts, images, audio and video clips .....	17
4.1.3.	2.4.1.3 Recognise ways to protect yourself when using online communities: apply appropriate privacy settings, restrict available personal information, use private messaging when appropriate, disable location information, block/report unknown users .....	17
4.2.	Communication Tools .....	18
4.2.1.	Recognise good practice when using electronic communication: be accurate and brief, use clear subject headings, do not inappropriately disclose personal details, do not circulate inappropriate content, spell check content.....	18
4.3.	<b>E-mail Concepts</b> .....	18
4.3.1.	Be aware of possible problems when sending file attachments like: file size limits, file type restrictions .....	18
4.3.2.	2.4.3.4 Outline the difference between the To, Copy (Cc), Blind copy (Bcc) fields and recognise their appropriate use.....	18
4.3.3.	2.4.3.5 Be aware of the possibility of receiving fraudulent and unsolicited e-mail. Be aware of the possibility of an e-mail infecting the computer .....	18
4.3.4.	Define the term phishing. ....	19
5.	Using E-mail .....	20
5.1.	<b>Sending E-mail</b> .....	20
5.1.1.	Enter an appropriate title in the subject field and enter, paste text into the body of an e-mail 20	
5.2.	<b>Tools and Settings</b> .....	21
5.2.1.	Create and insert a text e-mail signature. ....	21

## 1. WEB BROWSING CONCEPTS

### 1.1. KEY CONCEPTS

#### 1.1.1. UNDERSTAND THE STRUCTURE OF A WEB ADDRESS. IDENTIFY COMMON TYPES OF DOMAINS LIKE: GEOGRAPHICAL, ORGANISATION (.ORG, .EDU, .COM, .GOV)

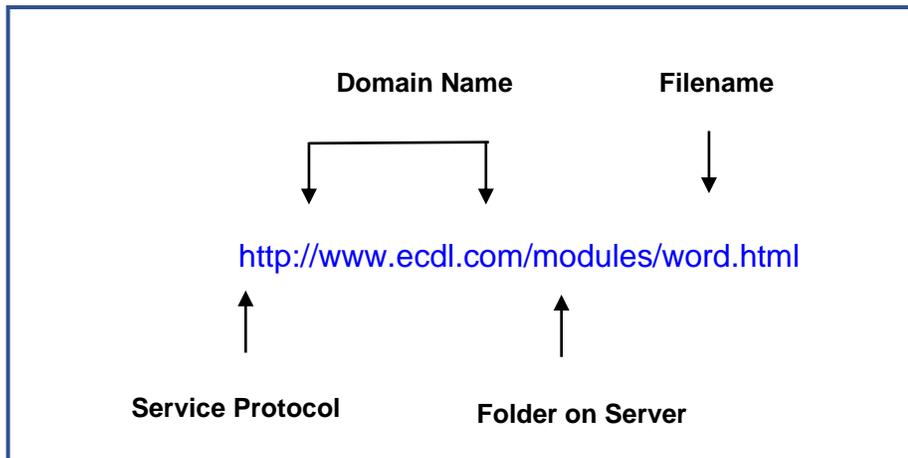
The Uniform Resource Locator (URL) is a standard address that tells your browser how to locate a file or other resource on the Web. This is also known as an Internet address or Web address. Every Web page is assigned an address e.g:

<https://www.icdleurope.org/>

The URL contains all the useful information about the site that you are looking for.

From the URL it is possible to know what type of organisation has put up the site, and also an indication of where the organisation is based.

The URL of a Web page is made up of 3 distinct components:



**Service Protocol** – Thousands of computers on Internet communicate with each other by sending packets of data back and forth. The diversity and multitude of computers on the Internet dictate a standard procedure or protocol (set of rules) for the reading of Web pages. `http://` is the language used by the web browser to request Web pages from a Web server.

**Domain Name** – This identifies the name of the organisation where the information is stored.

The following table shows some geographical domains:

Domain	Area	Domain	Area
<b>at</b>	Austria	<b>fr</b>	France
<b>au</b>	Australia	<b>gr</b>	Greece
<b>ca</b>	Canada	<b>ie</b>	Ireland
<b>ch</b>	Switzerland	<b>jp</b>	Japan
<b>de</b>	Germany	<b>mt</b>	Malta
<b>dk</b>	Denmark	<b>nz</b>	New Zealand
<b>it</b>	Italy	<b>uk</b>	United Kingdom

The following table shows the types of organisations that may be found on Internet:

Folder & Filename (the File Path) - This shows the location of the Web page on the Internet server and the

Organisation	Meaning
<b>com</b>	Commercial organisation
<b>edu/ac</b>	Educational institution
<b>gov</b>	Government body or department
<b>net</b>	Networking organisation
<b>org</b>	Non-profit making organisation (unions or charities)

name of the document that is being requested. The file 'ecd1' ends with the extension '.html' – short for hypertext markup language.

## 1.2. SECURITY AND SAFETY

### 1.2.1. RECOGNISE WAYS TO PROTECT YOURSELF WHEN ONLINE: PURCHASE FROM SECURE REPUTABLE WEBSITES, AVOID UNNECESSARY DISCLOSURE OF PERSONAL AND FINANCIAL INFORMATION, LOG OFF FROM WEBSITES



Information about yourself. Consider what you're going to post on the internet or send in an email. Anyone can see what you put on the internet. One of the biggest risks you face online is sharing personal information with someone you don't know. Sharing personal information like your address, phone number, family members' names, car information, passwords, work history, credit status, social security numbers, birth date, school names, passport information, driver's licence numbers, insurance policy numbers, loan numbers, credit/ debit card numbers, PIN numbers, and bank account information is dangerous and should be avoided. Consider removing your name from websites that disclose your personal information (phone number,

address, social networking avatars, and photos) collected from public databases with anybody on the internet.

**Photos.** Photos taken with smartphones include GPS coordinates, allowing others to see where the snap was taken and perhaps allowing them to locate you. When uploading images to social media sites, keep this in mind. Remember that unless you utilise privacy settings to limit who has access to your images, they can be duplicated, edited, and shared with a large number of people without your knowledge or agreement.

**Emails, Phishing, and Malware** are all things that you should be aware of. When opening emails from unknown senders or sources, be cautious, particularly if they are unsolicited. By clicking on links or downloading attachments, you risk infecting your computer or being a victim of fraud, malware, or a scam. Some viruses cause damage to your computer, while others might steal your personal information and, ultimately, your identity. When you receive emails that appear to come from your bank or another financial organization, be cautious, especially if they require you to confirm or submit personal or financial information. Be wary of frauds that send you to a website or give you a phone number to call using links in emails. Some email links are misleading.

The most used system nowadays is HTTPS (Hypertext Transfer Protocol Secure). It instructs your online browser to encrypt any information you type onto the website, such as passwords or credit card numbers, so that thieves cannot read it.

Before entering your username and password in any screen, you should routinely check that the web address of the page displayed in the browser begins with **“https://”**.

Be cautious with email messages asking you to send your username and password. Reputable organisations will never ask for these details and other personal information (e.g. financial details) to be sent by email or phone.

It is important to sign out/log off and close all browser windows when you are done with your online shopping, e-banking etc.

### 1.2.2. DEFINE THE TERM ENCRYPTION



Encryption is a method of securing digital data by the use of one or more mathematical procedures, as well as a password or "key" to decrypt the data. The encryption process converts data into unreadable form using an algorithm. By scrambling the content, encryption improves the security of a message or file.

Public-key encryption is one type of computer encryption system. This uses a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public

key. Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her.

### 1.2.3. IDENTIFY A SECURE WEBSITE: HTTPS, LOCK SYMBOL.

The lock sign and related URLs that begin with "https" merely indicate that the connection between your web browser and the website server is encrypted, which is crucial. A padlock icon next to the site name indicates that the site is secured with a digital certificate. This means that any data passed between your browser and the website is encrypted and cannot be intercepted or read by third parties while in transit. The Site Identity button (a padlock) appears to the left of the web address in the address bar when you visit a website. You can rapidly determine whether the connection to the website you're seeing is secure.



When users try to access secure web sites, the browser prompts for a username and a password. The Web sites will be displayed if the correct username and password are entered.

### 1.2.4. DEFINE THE TERM DIGITAL CERTIFICATE

Internet users are often concerned about online purchases. Normally payments for online purchases are made by a credit-card. Here are some important facts that you should know before submitting your credit number:

- Information travelling between your computer and a server can be routed through many computer systems.
- Any one of these computer systems can capture and misuse your information. Each of these computers can eavesdrop and make copies of your information.
- An intermediary computer could even deceive you and exchange information with you by representing itself as your intended destination.



If you decide to shop or do banking on the Internet, protect yourself by dealing with secure sites. Browsers display security warnings when you are about to enter a secure site. You can tell when you have a secure connection by looking at the URL. Secure sites have URLs starting with "https:" not "http://".

A secure Web site has a digital certificate confirming that it is secure and genuine. It ensures that no other Web site can assume the identity of the original secure site. When you are sending personal information over the Internet, you should check the certificate of the Web site you are using to ensure that it will protect your personally identifiable information.

Digital certificates are issued by a certificate authority. When you visit a secure Web site, the site automatically sends you its digital certificate. Digital certificates are used by organisations involved in online monetary transactions. The certificates ensure that credit card details will not be intercepted as these travel

from the buyer's computer to the webserver. Digital certificates can be viewed by double-clicking on the padlock icon in the Web browser.

---

#### 1.2.5. RECOGNISE OPTIONS FOR CONTROLLING INTERNET USE LIKE: SUPERVISION, WEB BROWSING RESTRICTIONS, DOWNLOAD RESTRICTIONS

Parental controls are software or device-specific features that allow parents to keep an eye on their children's internet usage. They protect youngsters from accessing online content that is inappropriate, unsuitable, or illegal. They can be used by your ISP, search engines, video streaming services, chat applications, and more. The following preventative techniques can be used by parents:

- Limit or prohibit your child's access to video games.
- Only allow pre-approved websites to be viewed in web browsers.
- Limit the use of certain services by children.
- Limit what a child can search for on the internet by using search engines.
- Organize the many categories of searchable videos.

## 2. WEB BROWSING

### 2.1. TOOLS AND SETTINGS

#### 2.1.1. UNDERSTAND THE TERM POP-UP. ALLOW, BLOCK POP-UPS



A pop-up is a small web browser window that appears on top of the website you are viewing. Pop-up windows often open as soon as you visit a website and are usually created by advertisers.

Pop-up Blocker feature lets you limit or block most pop-ups. You can choose the level of blocking you prefer, from blocking all pop-up windows to allowing the pop-ups that you want to see. When Pop-up Blocker is turned on, the Information bar displays a message saying "Pop-up blocked. To see this pop-up or additional options click here."

By default, Chrome will notify you when a pop-up is blocked and give you an option to see it. To turn off pop-up blocker, follow these instructions:

- Click the **Customize and control Google Chrome** menu (the three dots in the upper right corner)
- Select **Settings**.
- Click **Advanced** at the bottom.
- Under **Privacy and security**, click the **Site Settings** button.
- Select **Pop-ups and redirects**.
- To disable the pop-up blocker, uncheck the **Blocked (recommended)** box.
- To enable pop-ups on specific sites, check **Blocked (recommended)** and click **Add** next to **Allow** and enter the URL(s).

#### 2.1.2. UNDERSTAND THE TERM COOKIE. ALLOW, BLOCK COOKIES

Cookies are text files that save information regarding particular websites. They may save information, shopping cart contents, or user preferences.

When a Web browser requests a Web page from a Web server, the latter can store a piece of text on the user's computer. The text is sent back to the server each time the browser requests a page from that server.

The main purpose of cookies is to identify users and possibly prepare customised Web pages for them. When you enter a Web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.



Many websites require that you enable cookies in order for the website to be properly viewed.

### Clear all cookies

- 1) On your computer, open Chrome .
- 2) At the top right, click More  > Settings .
- 3) Click Privacy and security > Cookies and other site data.
- 4) Click See all site data and permissions > Clear all data.
- 5) To confirm, click Clear.

### Delete cookies from a site

- 1) On your computer, open Chrome .
- 2) At the top right, click More  > Settings .
- 3) Click Privacy and security > Cookies and other site data.
- 4) Click See all site data and permissions.
- 5) At the top right, search for the website's name.
- 6) To the right of the site, click Remove .
- 7) To confirm, click Clear.

### Allow or block cookies

You can allow or block all cookies by default. You can also allow cookies from a specific site but block third-party cookies in ads or images on that web page.

- 1) On your computer, open Chrome .
- 2) At the top right, click More  > Settings .
- 3) Under "Privacy and security," click Cookies and other site data.
- 4) Select an option:
  - **Allow all cookies.**
  - **Block all cookies (not recommended).**
  - **Block third party cookies in Incognito.**
  - **Block third-party cookies.**

If you block third-party cookies, all cookies and site data from other sites are blocked, even if the site is allowed on your exceptions list.

---

#### 2.1.3. DELETE HISTORY, TEMPORARY INTERNET FILES, SAVED FORM DATA.

Keeping your Internet browser optimized for maximum performance means routinely deleting temporary Internet files, cookies, and browsing history. Your internet history isn't completely erased when you delete it. If you have a Google account, it tracks not only your searches and visits to websites but also the videos you view and the places you visit. While temporary internet files make it easier to visit websites, they consume a lot of space on your hard drive.

The cache is a special folder on the hard disk that stores Web pages accessed by your browser. The first time visit a Web page, your browser retrieves all content (text, images, audio etc.) and a copy of these will be stored on the hard disk. The next time you visit the same Web page, your browser checks if the last modified dates of the files on the Internet are newer than the ones stored or cached. If the dates are the same, your browser uses the files on your hard disk instead of downloading them again from the Web server. Thus, the cache speeds up the browsing of Web pages. The files stored in the cache are known as temporary Internet files.

You can recover significant storage space by removing these files by following the steps below:

- 1) Open Google Chrome
- 2) Click Tools
- 3) Select Options
- 4) Click the Under the Hood tab
- 5) Click Clear Browsing Data
- 6) Select the Empty the Cache check box
- 7) Select the Clear Browsing History check box
- 8) Select the Delete Cookies check box
- 9) Click the Clear Browsing Data button

## 2.2. BOOKMARKS

### 2.2.1. ADD, DELETE A BOOKMARK / FAVOURITE.

The bookmarks, referred to Favourites that enable you to store the URLs of Web pages that you frequently visit. It is a list of URLs of frequently visited Web pages. Through the favourites list you can return to a Web page without having to remember and retype its URL. Once you add a URL to the favourite list, the item stays until you remove it or edit the list.

Google Chrome lets you add or remove Bookmarks to your favourite web pages. It's easy to add Bookmarks and just as simple to remove Bookmarks from Google Chrome.

#### How to add a Bookmark to Chrome

##### ADD A BOOKMARK

- 1) On your computer, open Chrome.
- 2) Go to the site you want to visit again in the future.
- 3) To the right of the address bar, click Star .

##### DELETE A BOOKMARK

Important: After you delete a bookmark, you can't get it back.

- 1) On your computer, open Chrome.
- 2) At the top right, click More  > Bookmarks > Bookmark Manager.
- 3) To the right of a bookmark, click the Down arrow  > Delete.

The Bookmarks bar runs below the address bar and makes for super-quick bookmarking. To swiftly place a webpage on the bar, left click in the address bar to highlight the current address of a page, and then hold and drag the address on to the Bookmarks bar. The Bookmark will now appear on the bar for easy access.

### 2.2.2. SHOW BOOKMARKS / FAVOURITES

Important: The easiest way to open a bookmark is to click on it in the Bookmarks bar. To turn the bookmark bar on or off, click More  > Bookmarks > Show bookmarks bar.

If you don't have the bookmarks bar turned on, there are 2 ways to find your bookmarks:

From the menu:

- 1) On your computer, open Chrome.
- 2) At the top right, click More  > Bookmarks.
- 3) Click a bookmark.

From the navigation panel:

- 1) At the top right of your browser, click Side panel .
- 2) Click Bookmarks.

### 2.2.3. 2.2.3.3 CREATE, DELETE A BOOKMARKS / FAVOURITES FOLDER. ADD WEB PAGES TO A BOOKMARKS / FAVOURITES FOLDER

By right clicking the bookmarks bar and selecting "Add Folder," you can create a folder.

- More Bookmarks can be found in the top right corner. Bookmark Manager is an application that allows you to manage your bookmarks

Start Chrome on your machine.

- More Bookmarks can be found in the top right corner. Bookmark Manager is an application that allows you to manage your bookmarks
- Select More from the drop-down menu at the upper right. A new folder will be created.

Chrome for Windows and Macintosh is a web browser that is available for both Windows and Macintosh computers.

- Go ahead and open Google Chrome as usual.
- Go to the website you want to save to your Bookmarks Bar and click Add to Bookmarks Bar (e.g. google.com)

Macintosh: Bookmark this Page... can be found under the Bookmarks menu. Click the right-hand star in the address bar on Windows.

### HOW REMOVE A BOOKMARK FROM CHROME

- To remove a Bookmark from the Bookmarks bar, **right-click** the Bookmark and then left-click on **Delete**.
- To remove a Bookmark from Other Bookmarks, **left-click** on **Other Bookmarks**, find the Bookmark to remove, **right-click** and then click on **Delete**.

### 3. WEB-BASED INFORMATION

#### 3.1. CRITICAL EVALUATION

##### 3.1.1. UNDERSTAND THE IMPORTANCE OF CRITICALLY EVALUATING ONLINE INFORMATION. UNDERSTAND THE PURPOSE OF DIFFERENT SITES LIKE: INFORMATION, ENTERTAINMENT, OPINION, SALES

All websites should be assessed against a variety of criteria, especially if you intend to use the information on them in a course project or other scholarly research. When analyzing web material, you'll search for many of the same qualities you seek for in other resources, as well as some extra factors like the website's host and functioning. It's especially vital to evaluate websites while utilizing them for research tasks, but it's also necessary to evaluate websites critically even if you're just doing research for fun. When you evaluate information, you should consider the source's credibility, validity, correctness, authority, timeliness, point of view, and bias. This isn't always the case with public-access content on the Internet.

There is no oversight agency or editorial process that ensures the accuracy, objectivity, or currency of information on the Internet. As a result, evaluating information obtained via the Internet is very critical. Accuracy refers to the content's consistency, accuracy, and correctness. What sources do you have for the data?

##### 3.1.2. OUTLINE FACTORS THAT DETERMINE THE CREDIBILITY OF A WEBSITE LIKE: AUTHOR, REFERENCING, UP-TO-DATE CONTENT

The credibility of your website determines whether a visitor contacts you, makes a purchase, or simply leaves and moves on to the next page. Credibility is "perceived trustworthiness + perceived expertise," according to a Stanford research on web credibility. Accuracy, Authority, Objectivity, Currency, and Coverage are five criteria for evaluating websites. Authors who are well-known in their fields of study write trustworthy sources. Authors who are responsible and reputable will mention their sources so that you may verify their accuracy and substantiate their claims.

##### 3.1.3. RECOGNISE THE APPROPRIATENESS OF ONLINE INFORMATION FOR A PARTICULAR AUDIENCE



The World Wide Web offers information and data from all over the world. Anyone can write a Web page. This means that the Web has high-quality information and information of a dubious nature. It is therefore important to critically evaluate the online information.

- **Purpose of online information** – It is important to understand the purpose of the site. Is it meant to present factual information? Is it presenting the personal opinion of the author? Is it presenting information for entertainment purposes? Is it presenting commercial, sales or marketing information?
- **The credibility of online information** – Who is the author of the web page? What qualifications does this person have on this topic? Are there any references on the web page to other credible pages? Is the information up to date?

- **Target audience** – Is the information intended for primary school children, university students, adults etc.?

### 3.1.4. COPYRIGHT, DATA PROTECTION



Computer users should be aware of the copyright issues with regard to software and files such as graphics, text, audio and video. A copyright is the exclusive legal right that prohibits the copying of intellectual property without the permission of the copyright holder.

Computer software is considered as intellectual property and is protected by copyright law.

The Internet and the World Wide Web present tremendous opportunities for sharing information but it is important to remember that what is freely available does not imply that it can be copied. You should assume that images, text, logos, software, sounds, movie clips, email and postings to newsgroups are copyrighted. Under copyright law, you cannot copy work/files unless you have been given permission to do so. In some cases, there may be permission statements included with the work/files that allow you to use the work/files for the stated purposes.

The ease with which computers can process, store and transfer data (including personal data) has necessitated some form of legislation to protect the privacy of individuals. Computer users dealing with personal data will soon be required to treat this data according to the legal framework outlined in the Data Protection Act.

The Data Protection Act (2001) attempts to make provisions for the protection of individuals against the violation of their privacy and personal integrity by the processing of personal data.

Data controllers (users having personal data on their computer) should ensure that:

- Personal data is processed fairly and lawfully;
- Personal data is always processed in accordance with good practice;
- Personal data is only collected for specific, explicitly stated and legitimate purposes;
- Personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- Personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- No more personal data is processed than is necessary having regard to the purposes of the processing;
- Personal data that is processed is correct and, if necessary, up to date;
- All reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;
- Personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

### 3.1.5. DEFINE THE TERMS COPYRIGHT, INTELLECTUAL PROPERTY. RECOGNISE THE NEED TO ACKNOWLEDGE SOURCES AND/OR SEEK PERMISSION AS APPROPRIATE

Intellectual property (IP) is a legal term that refers to a set of legal rights that protect people's ideas and creative work. Copyright is a type of IP that includes patents, trademarks, and registered designs. The rights provided to creators or holders of copyright to original works are referred to as copyright. Recognizing someone's copyright isn't enough to qualify as "permission." If you want to use an excerpt of someone's work for commercial purposes, "Fair Use" regulations don't apply, and you'll need to ask the copyright owners for permission. The term "copyright" (sometimes known as "author's right") refers to the legal rights that authors and artists have over their literary and artistic works. Books, music, art, sculpture, and films, as well as computer programmes, databases, and advertisements, are all examples of works protected by copyright.

### 3.1.6. RECOGNISE THE MAIN DATA PROTECTION RIGHTS AND OBLIGATIONS IN YOUR COUNTRY

Everyone has a right to privacy when it comes to personal information about them. Such information must be processed equitably, for specific purposes, and on the basis of the person's consent or another legal basis. Article 14A states that every citizen has the right to access information as defined by law, which includes information kept by the state, a ministry, or any other government department, statutory body, or local authority that is necessary for the exercise or protection of a citizen's right. Individuals have the right to be informed and have access to information under the GDPR.

## 4. COMMUNICATION CONCEPTS

### 4.1. ONLINE COMMUNITIES

#### 4.1.1. UNDERSTAND THE CONCEPT OF AN ONLINE (VIRTUAL) COMMUNITY. IDENTIFY EXAMPLES LIKE: SOCIAL NETWORKING WEBSITES, INTERNET FORUMS, WEB CONFERENCING, CHAT, ONLINE COMPUTER GAMES

The most well-known sort of virtual community is social networking services. They are either a website or a software platform that focuses on the development and maintenance of relationships. Virtual communities such as Facebook, Twitter, and Myspace exist. A virtual community is a group of people who meet online or through other collaborative networks to share mutual interests, ideas, and sentiments. When it comes



down to it, the fact that you have already formed each of the relationships is what makes a social network a social network. Your pre-existing connections were formed one at a time, one by one, by you, and an online social network is where those ties might come together. The term "virtual" refers to something that lives only in one's head, existing in essence but not in reality, and is not manufactured by a computer. A virtual friend is a good illustration of this. A world built by a computer video game is a good example of virtual.

#### 4.1.2. OUTLINE WAYS THAT USERS CAN PUBLISH AND SHARE CONTENT ONLINE: BLOGS, MICROBLOGS, PODCASTS, IMAGES, AUDIO AND VIDEO CLIPS

Both blogs and podcasts can be used to advertise content. Content marketing may help you build customer trust and loyalty, boost conversions, engage customers, and generate prospects. In today's world, audiences expect continuous, high-quality content from their favourite influencers and brands. Users and brands can exchange audio-visual content such as photographs, videos, music, and live broadcasts through media sharing platforms, as the name implies. Because photos and videos have a wider reach than text, the major purpose of these platforms is to engage users through disseminating media. Make a blog post with a podcast preview. In your blog, incorporate quotes from the podcast. Everything should be repurposed and written as a blog article. Make audio episodes from of blog entries and more.

#### 4.1.3. 2.4.1.3 RECOGNISE WAYS TO PROTECT YOURSELF WHEN USING ONLINE COMMUNITIES: APPLY APPROPRIATE PRIVACY SETTINGS, RESTRICT AVAILABLE PERSONAL INFORMATION, USE PRIVATE MESSAGING WHEN APPROPRIATE, DISABLE LOCATION INFORMATION, BLOCK/REPORT UNKNOWN USERS

An Internet Service Provider (ISP) keeps track of your online activities, which can be hacked. While customers have little control over ISP-level attacks, cookies, which are small bits of text downloaded and saved by your browser, can be used to track the web pages you visit. Browser plugins can track your online activities across multiple websites. What's the big deal? Cookies are used to customise online experiences, including targeted advertising. However, as evidenced by the usage of unique identifiers appended to

cookies across several services and marketing platforms, such tracking can go too far. Invasion of privacy is a common criticism of these techniques.

## 4.2. COMMUNICATION TOOLS

### 4.2.1. RECOGNISE GOOD PRACTICE WHEN USING ELECTRONIC COMMUNICATION: BE ACCURATE AND BRIEF, USE CLEAR SUBJECT HEADINGS, DO NOT INAPPROPRIATELY DISCLOSE PERSONAL DETAILS, DO NOT CIRCULATE INAPPROPRIATE CONTENT, SPELL CHECK CONTENT

Written business communication necessitates a high level of proficiency and knowledge. The way you use the written word, from letters to reports, matters. Written documents serve as a record of a correspondence, which is important in cases where legal issues may develop. It's critical in situations like this to be able to show that the message was delivered and received, as well as the dates on which they occurred. Regardless of the type of message you're conveying, the written communication you produce represents you and your business, so make it clear, succinct, and professional. This article will introduce you to five different forms of written business documents that you will come across in your career. Email, memos, letters, fax cover sheets, and brief reports are examples of this type of communication. You'll also learn how to use the acronym FAST to keep track of your document's Format, Audience, Style, and Tone.

## 4.3. E-MAIL CONCEPTS

### 4.3.1. BE AWARE OF POSSIBLE PROBLEMS WHEN SENDING FILE ATTACHMENTS LIKE: FILE SIZE LIMITS, FILE TYPE RESTRICTIONS

This error message appears because the default attachment size limit for Internet email accounts in Outlook 2013 and later versions is 20 megabytes (20480 KB). This limit prevents your computer from repeatedly attempting to upload excessively large attachments that surpass most Internet service provider's upload limits. The Internet is another reason why IT departments limit attachment sizes. Even if the software that runs mail servers improves, there's no guarantee that another mail server will be able to handle larger files. It could be older, out-of-date, or equipped with additional security.

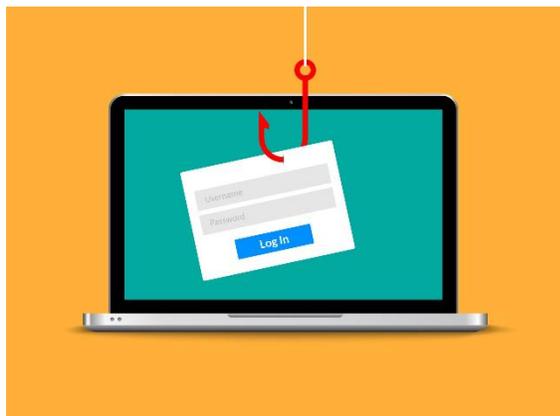
### 4.3.2. 2.4.3.4 OUTLINE THE DIFFERENCE BETWEEN THE TO, COPY (CC), BLIND COPY (BCC) FIELDS AND RECOGNISE THEIR APPROPRIATE USE

The letters Cc and Bcc stand for "carbon copy" and "blind carbon copy," respectively, in email jargon. Carbon copy (CC) receivers are accessible to all other recipients, whereas BCC recipients are not visible to anyone. The term "blind carbon copy" refers to a copy that is not visible to the naked eye. BCC is the same as CC in that it allows you to send copies of an email to many recipients. The difference is that with CC, you can view a list of recipients, whereas with BCC, you can't. Bcc stands for blind carbon copy and is similar to Cc in that the recipients' email addresses are not included in the received message header.

### 4.3.3. 2.4.3.5 BE AWARE OF THE POSSIBILITY OF RECEIVING FRAUDULENT AND UNSOLICITED E-MAIL. BE AWARE OF THE POSSIBILITY OF AN E-MAIL INFECTING THE COMPUTER

It's possible that you've just got a gut feeling. You should report any suspicions you have. Your notification of a phishing email will allow us to respond immediately, protecting many more people. The National Cyber Security Centre (NCSC) will investigate the suspicious email as well as any websites it links to. Phishing is when an Internet thief sends an email that looks like it came from a reputable source. The message is intended to get you to reveal sensitive or private information. What will be done with your email address if scammers get their hands on it? Once a fraudster obtains your email address, they will exploit it in whatever way they can. Many may send you spam email in the hopes of obtaining personal information like credit card numbers.

#### 4.3.4. DEFINE THE TERM PHISHING.



Phishing is a type of social engineering in which an attacker sends a phoney message to entice a victim into disclosing sensitive information or allowing dangerous software, such as ransomware, to be installed on the victim's system. Phishing is one of several new computer-related phrases that have entered the common vernacular in the last decade or two. Its "ph" spelling is influenced by an older word for committing a crime: "phreaking." Phreaking is thought to be a contraction of "phone freak," and it entails fraudulently utilising an electronic device to avoid paying for telephone calls. Sending emails that look to be from banks and ask

recipients to verify their accounts by inputting personal information is a popular phishing scam.

## 5. USING E-MAIL

### 5.1. SENDING E-MAIL

#### 5.1.1. ENTER AN APPROPRIATE TITLE IN THE SUBJECT FIELD AND ENTER, PASTE TEXT INTO THE BODY OF AN E-MAIL

To create a new email:



1. In the Home tab, click **New E-mail** button. The Untitled Message window will be displayed - here you will type the message to send.

2. Type the email address of the person you want to send the message to in the To: field. If you want to send the same message to several people, press **ENTER** key after typing the first address and type another email address.

An address in an address list can have one of the following recipient types:

**To:** Primary recipients of your message.

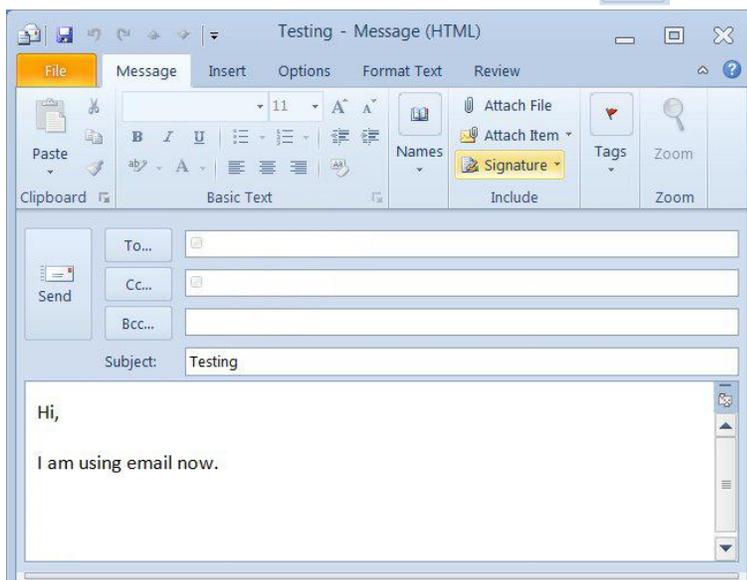
**Cc:** Carbon Copy, for secondary recipients i.e. the persons whom you decide to keep informed.

**Bcc:** Blind Carbon Copy, email addresses typed in this field are not visible.

3. Type the subject of your message in the Subject: field.

4. Click in the lower part of the window and type in the message. You can copy and paste text from other programs such as MS Word etc.

5. Click **Send** button to send your message.



Note that:

- By default, the email message sent is stored in the Sent Items folder.
- To discard your message without sending it, just close the window.

## 5.2. TOOLS AND SETTINGS

### 5.2.1. CREATE AND INSERT A TEXT E-MAIL SIGNATURE.

You can create personalized signatures for your email messages that include text, images, your electronic business card, a logo, or even an image of your handwritten signature.

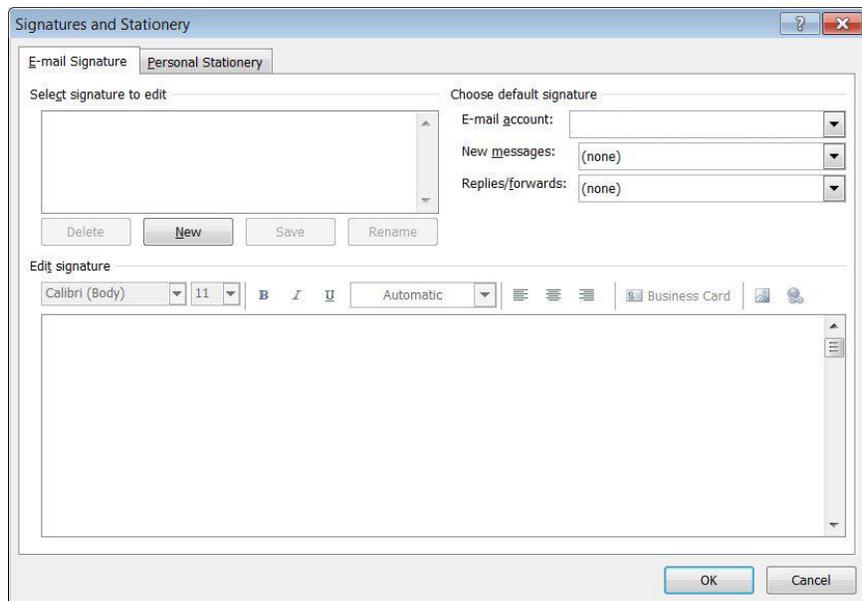
Your signature can automatically be added to outgoing messages, or you can manually add the signature to only the messages that you choose.

To create a signature:

1. Open a new message.
2. In the Include group, click the **Message** tab.
3. Click **Signature** button.
4. Click **Signatures...**



5. In the E-mail Signature tab, click **New** button.
6. Type a name for the signature.
7. Click **OK** button.
8. In the Edit signature box, type the text that you want to include in the signature.
9. To format the text, select the text, and then use the style and formatting buttons to select the options that you want.
10. To finish creating the signature, click **OK** button.



Note that:

- The signature that you just created or modified won't appear in the open message; it must be inserted into the message.

To insert a signature manually:

1. In a new message, on the Message tab, in the Include group, click the **Signature** button.
2. Click the signature to insert.

Note that:

- To remove a signature from an open message, select the signature in the message body, and then press the **DELETE** key.