SECTION 5. FACES OF THE INTERNET

LEARNING OBJETIVES

- *To acquire vocabulary related to the Internet and email.*
- *To understand how the Internet works.*
- *To understand the anatomy of an email.*
- *To be able to form different types of questions correctly.*
- *To recognize the basic features of the Web.*
- *To use collocations related to the Web and the Internet.*
- *To acquire vocabulary related to the Web, e-commerce and online banking*
- *To understand the basic ideas related to security and privacy on the Internet.*

Contenido

1 INTRODUCTION

By the early 1990's, people were using computers in many different ways. Computers were already installed in most schools, offices, and homes. They were commonly used for writing papers, playing games, financial accounting, and business productivity applications. But very few people used them for **communication**, **research**, and shopping the way we do now. A man named **Tim Berners-Lee** changed all that. In 1990, Lee added an exciting **hypertext** and **multimedia** layer to the Internet and called it the **World Wide Web**. The rest, as they say, is history.

The Web was not built for geeks. It was built for everyone. It was built with very high ideals. No single company, government, or organization controls it. It was new and exciting. New ideas and words appeared almost daily. Obscure technical terms became household words overnight. First it was **email**. Then it was **URL** and domain name. Then rather quickly came **spam, homepage, hyperlink, bookmark, download, upload, cookie, e-commerce, emoticon, ISP, search engine,** and so on. Years later we are still making up new words to describe our online world. Now we "**google**" for information. We "**tweet**" what's happening around us to others. The new words never seem to stop!

Just because the web seems so chaotic and unorganized compared to more structured companies and governments, doesn't mean it's total anarchy.

In 1994, Tim Berner's Lee started the **W3C**, a worldwide organization dedicated to setting standards for the Web. This group is probably the most respected authority for what should and should not be Web standards. W3C's mission is to lead the Web to it's full potential.

As a student of English and Technology, you will hear people use the words 'Internet' and 'World Wide Web' almost interchangeably. They are, of course, not the same thing. So what is the difference between the two? Perhaps a simple answer is that the Internet is the biggest network in the world, and the World Wide Web is a collection of software and protocols on that network. I guess a more simple way to put it is, the World Wide Web is an application that runs on The Internet.

I personally feel lucky to be alive in the age of the Web. It is one of the coolest things ever invented. It is unlikely that such another wonderful and major revolutionary invention will occur in our lifetime. But I can still dream about the Next Big Thing. And who knows? Maybe you will invent it.

2 The internet

The Internet (portmanteau of interconnected network) is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

The original **backbone** of the Internet is based on an old military network called **ARPANET** which was built by ARPA in the late 1960's. ARPANET was built so information could withstand a nuclear war. The idea was not to have a single point of failure. This means if part of the ARPANET was blown up in a nuclear war, the rest of it will still work! What made ARPANET so successful was it's packet-switching technology, invented by Lawrence Roberts. The idea is that "**packets**" of information have a "from" address and a "to" address. How they get from point "a" to point "b" depends on what roads are open to them. Packet switching is a very elegant thing. Without it, the Internet would simply not work.

The Internet has no single centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies. The overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol address (IP address) space and the Domain Name System (DNS), are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

2.1 Connecting to the internet

The internet is a worldwide system of interconnected computer networks. When you connect your computer to the internet via your Internet Service Provider (ISP) you become part of the ISP's network.

To connect to the internet the following are needed:

- a computer
- modem and/or router
- an ISP (Internet Service Provider)

Hardware needed

Modem

Once you have your computer, you really don't need much additional hardware to connect to the Internet. The primary piece of hardware you need is a **modem**.

The type of Internet access you choose will determine the type of modem you need. **Dial-up** access uses a **telephone modem**, **DSL** service uses a **DSL modem**, **cable** access uses a **cable modem**, and **satellite** service uses a **satellite adapter**. Your ISP may give you a modem—often for a fee—when you sign a contract, which helps ensure that you have the **right type** of modem. However, if you would prefer to shop for a **better** or **less expensive** modem, you can choose to buy one separately.

Router

A **router** is a hardware device that allows you to connect **several computers** and **other devices** to a single Internet connection, which is known as a **home network**. Many routers are **wireless**, which allows you to create a **home wireless network**, commonly known as a **Wi-Fi network**.

You **don't necessarily need to buy a router** to connect to the Internet. It's possible to connect your computer directly to your modem using an Ethernet cable. Also, many modems include a **built-in router**, so you have the option of creating a Wi-Fi network without buying extra hardware.

If you want to connect a computer that does not have built-in Wi-Fi connectivity, you can purchase a **Wi-Fi adapter** that plugs into your computer's USB port.

Types of Internet service

Internet connection options vary by Internet Service Provider and by region. Customers should consider some of the following factors before selecting an Internet package: speed or bandwidth, cost, availability, reliability and convenience.

In today's age, there are numerous ways to connect laptops, desktops, mobile phones, gaming consoles, e-readers and tablets to the Internet. Some of the most widely used Internet connections are described below.

- **Dial-up** connections require users to link their phone line to a computer in order to access the Internet. This particular type of connection—also referred to as analog—does not permit users to make or receive phone calls through their home phone service while using the Internet.

  This is generally the slowest type of Internet connection, and you should probably avoid it unless it is the only service available in your area. Dial-up Internet uses your **phone line**, so unless you have multiple phone lines you will not be able to use your **landline** and the Internet at the same time.
- **Broadband**: This high-speed Internet connection is provided through either cable or telephone companies. One of the fastest options available, broadband Internet uses multiple data channels to send large quantities of information. The term broadband is shorthand for broad bandwidth. Broadband Internet connections such as DSL and cable are considered high-bandwidth connections. Although many DSL connections can be considered broadband, not all broadband connections are DSL.
- **DSL**, which stands for Digital Subscriber Line, uses existing 2-wire copper telephone line connected to one's home so service is delivered at the same time as landline telephone service. Customers can still place calls while surfing the Internet.

  DSL service uses a **broadband connection**, which makes it much faster than dial-up. DSL connects to the Internet **via a phone line** but does not require you to have a landline at home. And unlike dial-up, you'll be able to use the Internet and your phone line at the same time.
- **Cable** Internet connection is a form of broadband access. Through use of a cable modem, users can access the Internet over cable TV lines. Cable modems can provide extremely fast access to the Internet.

- **Satellite**: In certain areas where broadband connection is not yet offered, a satellite Internet option may be available. Similar to wireless access, satellite connection utilizes a modem.

  It connects to the Internet **through satellites orbiting the Earth**. As a result, it can be used almost anywhere in the world, but the connection may be affected by weather patterns. Satellite connections are also usually slower than DSL or cable.
- **ISDN** (Integrated Services Digital Network) allows users to send data, voice and video content over digital telephone lines or standard telephone wires. The installation of an ISDN adapter is required at both ends of the transmission—on the part of the user as well as the Internet access provider.

  There are quite a few other Internet connection options available, including T-1 lines, T-3 lines, OC (Optical Carrier) and other DSL technologies.
- **Wireless**: Radio frequency bands are used in place of telephone or cable networks. One of the greatest advantages of wireless Internet connections is the "always-on" connection that can be accessed from any location that falls within network coverage. Wireless connections are made possible through the use of a modem, which picks up Internet signals and sends them to other devices.
- **Mobile:** Many cell phone and smartphone providers offer voice plans with Internet access. Mobile Internet connections provide good speeds and allow you to access the Internet.

  4G and 5G service is most commonly used with mobile phones, and it connects **wirelessly** through your ISP's network. However, these types of connections **limit the amount of data** you can use each month, which isn't the case with most broadband plans.
- **Hotspots** are sites that offer Internet access over a wireless local area network (WLAN) by way of a router that then connects to an Internet service provider. Hotspots utilize Wi-Fi technology, which allows electronic devices to connect to the Internet or exchange data wirelessly through radio waves. Hotspots can be phone-based or free-standing, commercial or free to the public.

As you decide what Internet connection is the best fit for your needs, you may wish to narrow down your selection based your preferred download and upload speeds, or based on deals and pricing options. Reliably fast speeds and comprehensive coverage make it easier than ever to stream your favorite TV shows and movies, share photos, chat with friends and play games online.

Most ISPs offer several tiers of service with different Internet speeds, usually measured in **Mbps** (short for **megabits per second**). If you mainly want to use the Internet for **email** and **social networking**, a slower connection (around 2 to 5 Mbps) might be all you need. However, if you want to **download music** or **stream videos**, you'll want a faster connection.

You'll also want to **consider the cost** of the service, including installation charges and monthly fees. Generally speaking, the faster the connection, the more expensive it will be per month.

Once you've chosen an ISP, most providers will **send a technician to your house** to turn on the connection. If not, you should be able to use the instructions provided by your ISP—or included with the modem—to set up your Internet connection.

After you have everything set up, you can open your **web browser** and begin using the Internet. If you have any problems with your Internet connection, you can call your ISP's **technical support** number.

Watch the video below to learn about connecting to the Internet.

https://youtu.be/hMX6dVa61t0

2.2 What can you do on the internet?

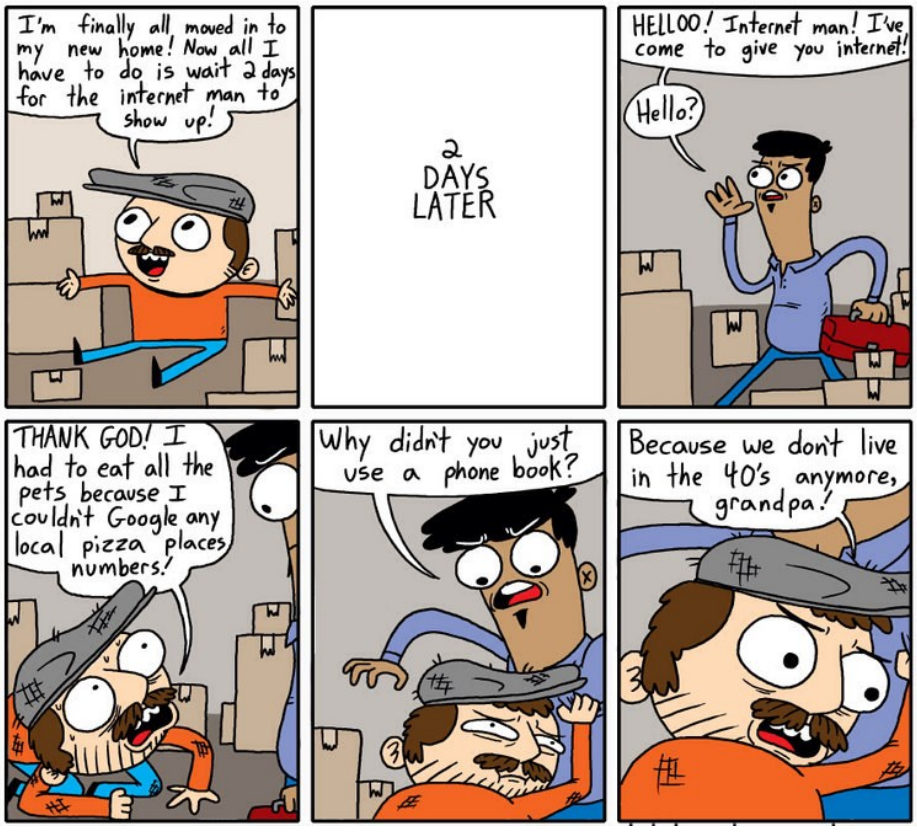
In the year 1999, the Internet suffered it's first financial crash. Many companies selling products and services on the Web were not living up to sales expectations. This was known as the Dot Com Bubble. There were many reasons why this happened, but perhaps the two most important reasons were a combination of slow connection speeds and too much optimism. Very few people had fast internet connections and many people thought the Internet was "just a passing fad". But we know now that the Internet is not a fad. So what happened? Web 2.0 happened!

What is Web 2.0? It's very hard to say. It's just a phrase to describe a transition from the pre-existing state of 'Web 1.0', which was slow, static, and unusable, to a new, 'second web', which was faster, more dynamic, and more usable for the average person. How did these things happen? Easy. **Broadband modems** enabled sites like **video-streaming** YouTube to become possible. Better design and development practices enabled **social media** sites like MySpace and then Facebook to attract hundreds of millions of users. Finally, **search engine** technology improved on sites like Google where people could actually find the information they were looking for.

There are many other things you can do on the Internet too. There are thousands of ways to keep up with news or shop for anything online. You can pay your bills, manage your bank accounts, meet new people, watch TV, or learn new skills. You can learn or do almost anything online. In conclusion, of the many things available to do on the internet, you can:

- browse websites
- send and receive email
- download media files, eg Mp3s or video files
- watch streamed video, eg BBC iPlayer, YouTube etc
- check your bank balance and make payments
- buy goods from online shops
- access educational material from your school's Virtual Learning Environment (VLE)
- create, store, edit and share your documents using web-based applications, eg Google Docs
- interact with friends on social networking sites, eg Bebo, MySpace, Facebook etc
- write a blog
- sign-up to forums and discuss topics that interest you with like-minded individuals
- game with friends
- instant message family and friends
- share photos and videos

But, what would we do without internet?



2.3 Email

One of the best features of the Internet is the ability to communicate almost instantly with anyone in the world. Email is one of the oldest and most universal ways to communicate and share information on the Internet, and billions of people use it.

Electronic mail (email or e-mail) is a method of exchanging messages ("mail") between people using electronic devices. Invented by Ray Tomlinson, email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email.

Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages.

Originally an ASCII text-only communications medium, Internet email was extended by Multipurpose Internet Mail Extensions (MIME) to carry text in other character sets and multimedia content attachments.

The history of modern Internet email services reaches back to the early ARPANET, with standards for encoding email messages published as early as 1973.

There are two main types of email, client-based email and webmail.

- **Client-based** email is often used by business users and involves the email being downloaded from a server to an application (such as Microsoft Outlook or Mozilla Thunderbird) on the user's computer.

  To set up this type of email you need an email application, eg Outlook, Thunderbird or Entourage, users can download their emails and read them offline to keep costs down.

- **Webmail**, as its name suggests, is web-based email. To use webmail, you do not need any email software - just a computer connected to the internet and a browser. Webmail accounts are usually free.

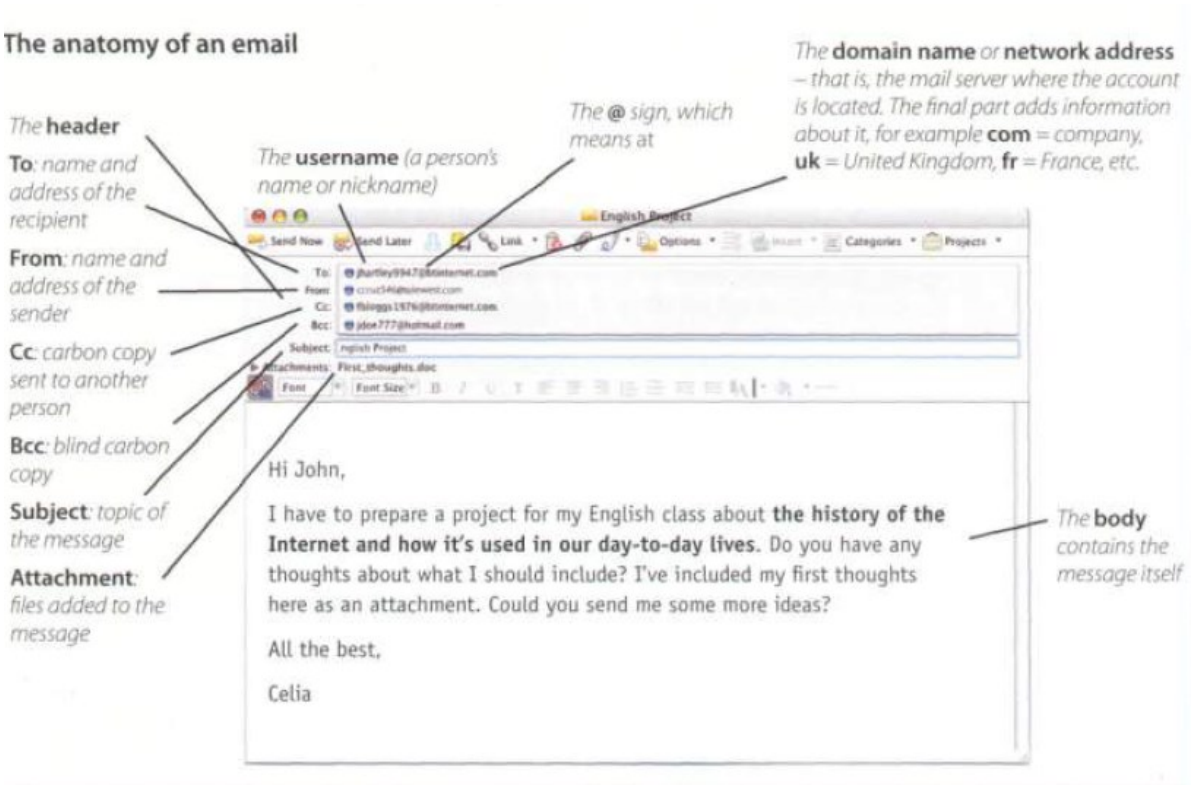
  Users simply sign up to a webmail service such as Google mail, Hotmail or Yahoo. They are then given a unique user name, password and a personal mailbox. The mailbox is accessed by visiting a specific web address and logging in. Once logged in, users can send and receive messages.

  The advantage of webmail is that users can receive and send email from any computer in the world with internet access and a browser.

Message format

Internet email messages consist of two major sections, the message header, and the message body, collectively known as content.

- The **header** is structured into fields such as From, To, CC, Subject, Date, and other information about the email. In the process of transporting email messages between systems, SMTP communicates delivery parameters and information using message header fields.
- The **body** contains the message, as unstructured text, sometimes containing a signature block at the end.



3 The web

The internet and the web are not exactly the same thing, then? No, actually. The internet has been around since the early 1970s – twenty years longer than the web. It is basically a huge network made up of smaller networks of computers. The World Wide Web is built on top of the internet. It's a way of sharing information in the form of webpages, using a kind of computer language called HTTP. That's why URLs often start http://www – because http is the language and www means World Wide Web. By the way, no one knows why web addresses use //. Even the web's inventor, Tim Berners-Lee, says these 'forward slashes' are not really necessary and if he could go back in time thirty years and invent the World Wide Web again, he would take them out.

In 1989, when British scientist Tim Berners-Lee invented the web, he was working at CERN in Switzerland. They had computers, of course, and email already existed (Queen Elizabeth II sent an email in 1976). The idea of domain names – web addresses showing the name of the organisation they belong to (like 'britishcouncil.org') – also existed. They used hypertext to jump from one document to another, but none of these things worked together so they weren't very useful.

Berners-Lee was frustrated at CERN because all the scientists had different kinds of computers that couldn't 'speak' to each other. If you wanted information you had to remember exactly which computer that information was on and know how to use the specific programs for that computer. Berners-Lee had an idea for an 'imaginary information system which everyone can read'. He wrote a report that suggested a way of putting the internet, domain names and hypertext together into one system. His idea was so abstract that his boss called it 'vague but exciting'. Two years later, in 1991, the world's first website was built at CERN, http://info.cern.ch (the site you can see now is a copy made in 1992).

Today, thirty years later, that idea is no longer vague and is part of many people's everyday reality. The web connects about 55 per cent of the world's population to the rest of the world via the internet. But because only half the world is connected, there is a 'digital divide' between communities with regular internet access and those without. In North America, 95 per cent of people have internet access and so do 85 per cent of Europeans. Compare this with Asia, where only half the population has internet access, and Africa, at 36 per cent. In some of the least developed countries, young people are three times more likely to be online than older adults.

3.1 Websites

Most information on the Internet is on **websites**. Once you are connected to the Internet, you can access websites using a kind of application called a **web browser**.

A **website** is a collection of related text, images, and other resources. Websites can resemble other forms of media—like newspaper articles or television programs—or they can be interactive in a way that's unique to computers. The purpose of a website can be almost anything: a news platform, an advertisement, an online library, a forum for sharing images, or an educational site like us!

Websites often have **links** to other sites, also called **hyperlinks**. These are often parts of the text on the website. They are usually coloured blue, and sometimes they are underlined or bold. If you click the text, your browser will load a different page. Web authors use hyperlinks to connect relevant pages. This web of links is one of the most unique features of the Internet, lending to the old name World Wide Web.

The **World Wide Web** (WWW or 'web' for short) is the part of the internet that you can access using a web browser such as Internet Explorer or Firefox. It consists of a large number of web servers that host websites. Each website will normally consist of a number of web pages. A web page can contain text, images, video, animation and sound.

People view the World Wide Web through a software application called a **web browser** or simply a "browser" for short. A **web browser** allows you to connect to and view websites. Some popular examples of web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari. Browsers allow people to search, view, and even add and edit data on the World Wide Web.

When you're looking for specific information on the Internet, a **search engine** can help. A search engine is a specialized website that's designed to help you find other websites. If you type keywords or a phrase into a search engine, it will display a list of websites relevant to your search terms.

A typical web browser has a toolbar that shows all the navigation icons, which let you **go back one page(a)** or **go forward one page(b)**. You can also **go to the home page(d)** or **stop the current transfer(f)** when the circuits are busy.

Tab buttons let you view different sites at the same time, and the built-in **search box(g)** helps you look for information, if the **feed button(h)** lights up, it means the site offers RSS feeds, so you can automatically receive updates. When a web page won't load, you can **refresh(e)** the current page, meaning the page **reloads** (downloads again). lf you want to mark a website address so that you can easily revisit the page at a later time, you can add it to your **favourites(k)** (favorites in American English), or **bookmark** it. When you want to visit it again you simply click show favourites.

On the web page itself, most sites feature **clickable image links(j)** and **clickable hypertext links(i)**. Together, these are known as hyperlinks and take you to other web pages when clicked. Web pages are connected by hypertext links. When a link is clicked you will be taken to another page which could be on another server in any part of the world.

Most sites have a page that links the user to the other main areas of the site. This is called the **homepage**.

You can access a website or web page by typing its **URL (Uniform Resource Locator)** into the address bar of your browser.

A typical **URL address(c)** looks like this: http://www.bbc.co.uk/radio/.In this URL:

- **http**// means Hypertext Transfer Protocol and tells the program to look for a web page.

  Https is the secure version of http. When you use https any data you send or receive from the web server is encrypted. For example, when banking online https is used to keep your account details safe.

  Some sites begin ftp://, a file transfer protocol used to copy files from one computer to another.
- **www** means world wide web.
- **bbc.co.uk** is the domain name of the server that hosts the website - a company based in the UK; other top-level domains are .com (commercial site), edu (education), .org (organization) or .net (network); radio is the directory path where the web page is located. The parts of the URL are separated by . (dot), / (slash) and : (colon).

4 Internet Security

There are many benefits from an open system like the Internet, but one of the risks is that we are often exposed to **hackers**, who break into computer systems just for fun, to steal information, or to spread viruses.

Security is crucial when you send **confidential** information online. Consider, for example, the process of buying a book on the Web. You have to type your credit card number into an order form which passes from computer to computer on its way to the online bookstore. If one of the intermediary computers is infiltrated by hackers, your data can be copied. To avoid risks, you should set all security alerts to high on your web browser. Mozilla Firefox displays a lock when the website is secure and allows you to disable or delete cookies - small files placed on your hard drive by web servers so that they can recognize your PC when you return to their site.

If you use online banking services, make sure they use digital certificates - files that are like digital identification cards and that identify users and web servers. Also be sure to use a browser that is compliant with SSL (Secure Sockets Layer), a protocol which provides secure transactions.

Similarly, as your email travels across the Net, it is copied temporarily onto many computers in between. This means that it can be read by people who illegally enter computer systems.

The only way to protect a message is to put it in a sort of virtual envelope - that is, to encode it with some form of encryption. A system designed to send email privately is Pretty Good Privacy, a freeware program written by Phil Zimmerman.

Private networks can be attacked by intruders who attempt to obtain information such as Social Security numbers, bank accounts or research and business reports. To protect crucial data, companies hire security consultants who analyse the risks and provide solutions. The most common methods of protection are passwords for access control, **firewalls**, and **encryption** and decryption systems. Encryption changes data into a secret code so that only someone with a key can read it. Decryption converts encrypted data back into its original form.

Malware (malicious software) are programs designed to infiltrate or damage your computer, for example viruses, worms, Trojans and spyware. A virus can enter a PC via a disc drive - if you insert an infected disc - or via the Internet.

An internet user can be tricked or forced into downloading software that is of malicious intent onto a computer. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- A **worm** is a self-copying program that spreads through email attachments; it replicates itself and sends a copy to everyone in an address book.
- A **Trojan** horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user will be convinced to download it onto the computer.
- **Spyware** refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

  One particular kind of spyware is key logging malware. Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard.

  Most spyware and **adware** (software that allows pop-ups - that is, advertisements that suddenly appear on your screen) is included with 'free' downloads.
- Computer **Viruses** are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.
- **Ransomware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.
- **Scareware** is scam software of usually limited or no benefit, containing malicious payloads, that is sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.

If you want to protect your PC, don't open email attachments from strangers and take care when downloading files from the Web. Remember to update your anti-virus software as often as possible, since new viruses are being created all the time.

Watch the video below from IBM Social Media to learn more about common online threats and how to avoid them.
https://youtu.be/GCWBf7WKYyA
Watch the video below to learn how to protect your computer from viruses, as well as how to back up your files.
https://youtu.be/U4lweHnf71E

4.1 Cybercimes

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information.

4.2 Types of Cybercrime

Computer crime encompasses a broad range of activities.

- **Piracy** - the illegal copy and distribution of copyrighted software, games or music files
- **Plagiarism and theft of intellectual property** - pretending that someone else's work is your own
- **Spreading of malicious software**
- **Phishing** (password harvesting fishing) - getting passwords for online bank accounts or credit card numbers by using emails that look like they are from rea) organizations, but are in fact fake; people believe the message is from their bank and send their security details
- **IPspoofing** - making one computer look like another in order to gain unauthorized access
- **Cyberstalicing** - online harassment or abuse. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.
- **DDoS Attacks:**devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

- **Botnets** are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.
- **Identity Theft:** This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.
- **Social Engineering:** Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.
- **PUPs** or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.
- **Prohibited/Illegal Content**: This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.
- **Online Scams:** These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

4.3 The history of hacking

Hacking, this is the practice of manipulating network connections and connected devices including but not limited to unauthorized access and acquisition of information.

Originally, all computer enthusiasts and skilled programmers were known as **hackers**, but during the 1990s. the term hacker became synonymous with **cracker** - a person who uses technology for criminal aims.

Today the term hacker generally refers to anyone with the technical ability, and using it, to penetrate, evade, intercept, acquire or otherwise interfere with another network, device, software or hacker. The group has been split into **Black Hats and White Hats**. The Black Hats are the bad guys, the enemies of the public good. The White Hats are the good guys, the sheriffs of the Internet

Hacking has been around pretty much since the development of the first electronic computers. Here are some of the key events in the last decades of hacking.

1960s: The Dawn of Hacking: The first computer hackers emerge at MIT. They borrow their name from a term to describe members of a model train group at the school who "hack" the electric trains, tracks, and switches to make them perform faster and differently. A few of the members transfer their curiosity and rigging skills to the new mainframe computing systems being studied and developed on campus.

1970s: Phone Phreaks and Cap'n Crunch. Phone hackers (phreaks) break into regional and international phone networks to make free calls. One phreak, John Draper (aka "Cap'n Crunch"), learns that a toy whistle given away inside Cap'n Crunch cereal generates a 2600-hertz signal, the same high-pitched tone that accesses AT&T's long-distance switching system.

Draper builds a "blue box" that, when used in conjunction with the whistle and sounded into a phone receiver, allows phreaks to make free calls.

Shortly thereafter, Esquire magazine publishes "Secrets of the Little Blue Box" with instructions for making a blue box, and wire fraud in the United States escalates. Among the perpetrators: college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer, who launch a home industry making and selling blue boxes.

1980: Hacker Message Boards and Groups. Phone phreaks begin to move into the realm of computer hacking, and the first electronic bulletin board systems (BBSs) spring up.

The precursor to Usenet newsgroups and e-mail, the boards -- with names such as "Sherwood Forest" and "Catch-22" -- become the venue of choice for phreaks and hackers to gossip, trade tips, and share stolen computer passwords and credit card numbers.

1981 - Ian Murphy, a 23-year-old known as Captain Zap on the networks, hacked into the White House and the Pentagon.

1987 - The IBM international network was paralysed by a hacker's Christmas message.

1988: The Morris Worm: Robert T. Morris, Jr., a graduate student at Cornell University and son of a chief scientist at a division of the National Security Agency, launches a self-replicating worm on the government's ARPAnet (precursor to the Internet) to test its effect on UNIX systems.

The worm gets out of hand and spreads to some 6,000 networked computers, clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years' probation and fined $10,000.

1988 - The Union Bank of Switzerland almost lost £32 million to hackers. Nicholas Whitely was arrested in connection with virus spreading,

1989 - A fifteen-year-old hacker cracked the US defence computer.

1991 - Kevin Poulsen, known as Dark Dante on the networks, was accused of stealing military files.

1992 - David L Smith was prosecuted for writing the Melissa virus, which was passed in Word files sent via email.

1997 - The German Chaos Computer Club showed on TV how to obtain money from bank accounts.

2000 - A Russian hacker attempted to extort $100.000 from online music retailer CD Universe.

A Canadian hacker launched a massive denial of service attack against websites like Yahoo! and Amazon.

The I Love You virus cleverly disguised as a love letter, spread so quickly that email had to be shut down in many companies. The worm overwrote image and sound files with a copy of itself.

In one of the biggest denial-of-service attacks to date, hackers launch attacks against eBay, Yahoo!, CNN.com., Amazon and others.

2001 - The Code Red worm infected tens of thousands of machines.

DNS Attack: Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to Microsoft's Web sites are corrupted. The hack is detected within a few hours, but prevents millions of users from reaching Microsoft Web pages for two days.

2006 - Hackers stole the credit card details of almost 20.000 ATAT online customers. However, subscribers to its service weren't affected.

2008: Project Chanology; Anonymous attacks Scientology website servers around the world. Private documents are stolen from Scientology computers and distributed over the Internet.

2009: Conficker worm infiltrated millions of PCs worldwide including many government-level top-security computer networks.

2011: An "external intrusion" sends the PlayStation Network offline, and compromises personally identifying information (possibly including credit card details) of its 77 million accounts, in what is claimed to be one of the five largest data breaches ever.[66]

2012: The social networking website LinkedIn has been hacked and the passwords for nearly 6.5 million user accounts are stolen by cybercriminals.

2015: the records of 21.5 million people, including social security numbers, dates of birth, addresses, fingerprints, and security-clearance-related information, are stolen from the United States Office of Personnel Management (OPM).

2016: Hacker Ardit Ferizi is sentenced to 20 years in prison after being arrested for hacking U.S. servers and passing the leaked information to members of ISIL terrorist group back in 2015.

2017: WannaCry ransomware attack started on Friday, 12 May 2017, and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries.

Hackers demand $7.5 million in bitcoin to stop pre-releasing HBO shows and scripts, including Ballers, Room 104 and Game of Thrones.

2020: Anonymous hacked the United Nation's website and created a page for Taiwan, a country which has not had a seat at the UN since 1971. The hacked page featured the Flag of Taiwan, the KMT emblem, a Taiwan Independence flag, the Anonymous logo, and embedded YouTube videos such as the Taiwanese national anthem and the closing score for the 2019 film Avengers: Endgame titled "It's Been a Long, Long Time", along with a caption.

4.4 How To Protect From Hackers

Here are some steps you can take to protect you from hackerx.

1. Use a firewall: The two major computer operating systems have built-in firewalls, software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you of any intrusion attempts. The first thing to do with a new computer (or the computer you now use) is to make sure the firewall is enabled before you go online.

2. Install antivirus software: Computer viruses, keyloggers and Trojans are everywhere. Antivirus programs immunize your computer against unauthorized code or software that threatens your operating system. Viruses have various effects that may be easy to spot: They might slow your computer to a halt or delete key files. Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. After you install an antivirus program, don't forget to use it. Run or sched**ul**e regular virus scans to keep your computer virus-free.

3. Install an anti-spyware package: Anti-spyware concentrates exclusively on this part of the nuisance spectrum but is often included in major antivirus packages like Webroot, McAfee and Norton. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

4. Use complex passwords: Using secure passwords is the most important way to prevent illegal intrusions onto your computer network. The more secure your passwords, the harder it is for a hacker to invade your system.

More secure often means longer and more complex: Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Don't reuse passwords either; if you have too many passwords to remember, consider using a password manager like Dashlane, Sticky Password, LastPass or Password Boss.

5. Keep your OS, apps and browser up to date: Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data.

6. Ignore spam: Beware of email messages from unknown parties, and never click on links or open attachments that accompany them.

7. Back up your computer: Backing up your information is critical in case disaster strikes and hackers do get through and trash your system.

8. Shut it down: Switch off your machine overnight or during long stretches of time when you're not working. Always being on makes your computer a more visible and available target for hackers. Shutting down breaks the connection a hacker may have established with your network and disrupts any possible mischief.

9. Use virtualization: Not everyone needs to take this route, but if you frequent sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment like Parallels or VMware Fusion that sidesteps your operating system to keep it safer.

10. Secure your network: If you've got a new router, chances are it comes with no set security. Always log in to the router and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

12. Use encryption: Even if someone is able to steal your data or monitor your internet connection, encryption can prevent hackers from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker or FileVault, encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt your web traffic. Only shop at encrypted websites – you can spot them immediately by the "https" in the address bar accompanied by a closed padlock icon.

5 Language work

Questions

- In questions, we normally place the auxiliary verb before the subject.

  ***Are** there other ways of accessing the Internet?*

- If there is no other auxiliary, we use **do/does** (present simple) or **did** (past simple).

  ***Did** the internet become popular quickly?*

- There are many question words in English which we use to find out more information than just yes or no.

People

***Who** created the Internet?*

Things

***What** does TCP/IP mean?*

***Which** email program is the best?*

Place

***Where** can you find newsgroups?*

Time

***When** was if created?*

***How often** are web pages updated?*

***How long** has broadband existed?*

Reason

***Why** do you need a modem?*

Quantity

***How much** does broadband access cost?*

***How many** newsgroups are there?*

Manner

***How** do you get online?*

Others

How fast are today's internet connections?

How old is the internet?

Collocations

A collocation is a pair or group of words that are often used together, For example, we say make phone calls, not do phone calls.

Here are some common types of collocation:

- **verb + noun**

  Surf the Web *download music*

- **verb + particle**

  Hack into a computer *log onto a bank account*

- **adverb + adjective**

  highly sensitive information *freely available on the Web*

- **adjective + noun**

  mathematical formulas *up-to-date information*

The word **online** often collocates with other wards and can function as adjective or adverb.

- **Adjective**: They post opinions on online journals.
- **Adverb**: A podcast is an audio recording posted online.

The prefixes e- and cyber-

- The **e-prefix** means **electronic**, and we add it to activities that take place on computers or online, for example **e-business/e-commerce** – business conducted over the Internet. Other examples include: e**-card, e-learning, e-zine. e-voting, e-signature, e-assessment, e-cash, e-book** and **e-pal**.

  There are often spelling variations, with or without a hyphen, so always check your dictionary.

- The **cyber- prefix** comes from cybernetics, and we use it to describe things related to computer networks, for example **cybercafe** - an internet cafe.

  Other examples include: **cybercrime**. **cyberculture**, **cyberslacker** and **cyberspace**.

Past simple

- We use the past simple to talk about a complete action or event which happened at a specific time in the past.

*He **began** hacking in 1974.*

- We form the past simple of regular verbs by adding -(e)d to the infinitive

  *John Draper **discovered** that a whistle ...*

- We form questions and negatives using did/didn't.

  *When **did** Captain Zap hack into the Pentagon?*
  *He **didn't** expect that his most famous explon ..*

- There are many verbs which are irregular in the past simple.
  For a list of irregular verbs, see next page.

  *Kevin Mitnick **began** hacking into ...*

- We form questions and negatives for irregular verbs in the same way as for regular verbs. The exception is be.

  *When **did** Kevin Mitnick begin hacking into. .?*
  *He **didn't** begin hacking until 1974.*

- We form the past passive with the past simple of **be + the past participle**.

  *IBM international **was** paralysed by hackers.*
  *He **wasn't** sent to prison*
  *Why **was** Nicholas Whitely arrested in 1998?*

Infinitive	Past simple	Past participle	Spanish
abide	**abided / abode**	**abided / abode**	**aguantar**
alight	**alighted / alit**	**alighted / alit**	**iluminar**
arise	**arose**	**arisen**	**levantar, erguer**
awake	**awoke / awaked**	**awoken / awaked**	**acordar, despertar**
(to) be	**was, were**	**been**	**ser, estar**
bear	**bore**	**born / borne**	**levar, aguantar**
beat	**beat**	**beaten**	**batir, golpear**
become	**became**	**become**	**hacerse, ponerse**
beget	**begot/begat**	**begotten**	**engendrar**
begin	**began**	**begun**	**comenzar**
bend	**bent**	**bent**	**torcer**
bereave	**bereaved / bereft**	**bereaved / bereft**	**despojar**
beseech	**besought / beseeched**	**besought / beseeched**	**suplicar**
bet	**bet**	**bet**	**apostar**
bid	**bid / bade**	**bid / bidden**	**ofrecer**
bind	**bound**	**bound**	**atar, amarrar**
bite	**bit**	**bitten**	**morder, picar**
bleed	**bled**	**bled**	**sangrar**
blow	**blew**	**blown**	**soplar**
break	**broke**	**broken**	**romper**
breed	**bred**	**bred**	**criar**
bring	**brought**	**brought**	**traer**
broadcast	**broadcast / broadcasted**	**broadcast / broadcasted**	**transmitir, emitir**
build	**built**	**built**	**construir**
burn	**burned / burnt**	**burned / burnt**	**quemar**
burst	**burst**	**burst**	**reventar(se), romper(se)**
buy	**bought**	**bought**	**comprar**

can	**could**		**poder**
cast	**cast**	**cast**	**echar, lanzar**
catch	**caught**	**caught**	**coger, agarrar**
chide	**chided / chid**	**chided / chidden**	**reprender**
choose	**chose**	**chosen**	**elegir**
cleave	**cleft / cleaved, clove**	**cleft / cleaved, cloven**	**lascar, rachar**
cling	**clung**	**clung**	**pegarse, agarrarse**
clothe	**clothed / clad**	**clothed / clad**	**vestir**
come	**came**	**come**	**venir, llegar**
cost	**cost**	**cost**	**costar, valer**
creep	**crept**	**crept**	**arrastrarse**
crow	**crowed**	**crowed / crew**	**cacarear, alardear**
cut	**cut**	**cut**	**cortar**
deal	**dealt**	**dealt**	**tramitar, operar**
dig	**dug**	**dug**	**cavar, excavar**
dive	**dived / dove (US)**	**dived**	**tirarse, sumergirse**
do	**did**	**done**	**hacer**
draw	**drew**	**drawn**	**tirar, sacar**
dream	**dreamt / dreamed**	**dreamt / dreamed**	**soñar**
drink	**drank**	**drunk**	**beber, tomar**
drive	**drove**	**driven**	**conducir**
eat	**ate**	**eaten**	**comer**
dwell	**dwelt / dwelled**	**dwelt / dwelled**	**morar, vivir**
fall	**fell**	**fallen**	**reprobar**
feed	**fed**	**fed**	**alimentar**
feel	**felt**	**felt**	**sentir**
fight	**fought**	**fought**	**luchar, pelear**
find	**found**	**found**	**encontrar**
fit	**fit / fitted**	**fit / fitted**	**quedar (de ropa)**
flee	**fled**	**fled**	**huir**

fling	**flung**	**flung**	**lanzar, arrojar**
fly	**flew**	**flown**	**volar**
forbid	**forbade**	**forbidden**	**prohibir**
forecast	**forecast**	**forcast**	**pronosticar**
forget	**forgot**	**forgotten**	**olvidar**
forgive	**forgave**	**forgiven**	**perdonar, disculpar**
forsake	**forsook**	**forsaken**	**abandonar**
freeze	**froze**	**frozen**	**helar**
geld	**gelded / gelt**	**gelded / gelt**	**castrar**
get	**got**	**got**	**conseguir**
gild	**gilded / gilt**	**gilded / gilt**	**dorar**
give	**gave**	**given**	**dar**
gnaw	**gnawed**	**gnawed / gnawn**	**roer**
go	**went**	**gone**	**ir**
grind	**ground**	**ground**	**moler, picar**
grip	**gripped / gript**	**gripped / gript**	**asir**
grow	**grew**	**grown**	**crecer**
hang	**hung**	**hung**	**colgar**
have	**had**	**had**	**tener**
hear	**heard**	**heard**	**oir**
heave	**heaved / hove**	**heaved / hove**	**tirar, estirar**
hew	**hewed**	**hewed / hewn**	**labrar, tallar**
hide	**hid**	**hidden**	**esconder**
hit	**hit**	**hit**	**golpear**
hold	**held**	**held**	**tener, abrazar**
hurt	**hurt**	**hurt**	**lastimar, perjudicar, doler**
keep	**kept**	**kept**	**guardar**
kneel	**kneeled / knelt**	**kneeled / knelt**	**arrodillarse**
knit	**knitted / knit**	**knitted / knit**	**hacer, tricotar, tejer**
know	**knew**	**known**	**conocer**

lade	**laded**	**laded / laden**	**cargar de**
lay	**laid**	**laid**	**poner, colocar**
lead	**led**	**led**	**llevar, guiar**
lean	**leaned / leant**	**leaned / leant**	**apoyarse**
leap	**leaped / leapt**	**leaped / leapt**	**saltar**
learn	**learnt / learned**	**learnt / learned**	**aprender**
leave	**left**	**left**	**dejar, abandonar**
lend	**lent**	**lent**	**prestar**
let	**let**	**let**	**dejar**
lie	**lay**	**lain**	**tenderse, acostarse**
light	**lit / lighted**	**lit / lighted**	**encender, iluminar**
lose	**lost**	**lost**	**perder**
make	**made**	**made**	**hacer, crear**
may	**might**		**poder**
mean	**meant**	**meant**	**significar**
meet	**met**	**met**	**encontrar**
melt	**melted**	**melted / molten**	**derretir**
misunderstand	**misunderstood**	**misunderstood**	**entender mal**
mow	**mowed**	**mowed / mown**	**segar, cortar**
offset	**offset**	**offset**	**compensar**
outbid	**outbid**	**outbid**	**pujar más alto que**
overtake	**overtook**	**overtaken**	**adelantar**
pay	**paid**	**paid**	**pagar**
pen	**penned / pent**	**penned / pent**	**escribir, redactar**
plead	**pleaded / pled**	**pleaded / pled**	**aducir, suplicar**
prove	**proved**	**proved / proven**	**demonstrar, probar**
put	**put**	**put**	**poner**
quit	**quit**	**quit**	**renunciar, abandonar**
read	**read**	**read**	**leer**
rid	**rid / ridded**	**rid / ridded**	**deshacerse de**

ride	**rode**	**ridden**	**montar, pasear**
ring	**rang**	**rung**	**sonar**
rise	**rose**	**risen**	**levantarse, elevarse**
run	**ran**	**run**	**correr**
say	**said**	**said**	**decir**
saw	**sawed**	**sawed / sawn**	**serrar**
see	**saw**	**seen**	**ver, mirar**
seek	**sought**	**sought**	**buscar**
sell	**sold**	**sold**	**vender**
send	**sent**	**sent**	**enviar**
set	**set**	**set**	**poner**
sew	**sewed**	**sewed / sewn**	**coser**
shake	**shook**	**shaken**	**sacudir, mover**
shall	**should**		**deber**
shave	**shaved**	**shaved / shaven**	**afeitar(se), rasurar(se)**
shear	**sheared**	**sheared / shorn**	**esquilar**
shed	**shed**	**shed**	**derramar**
shine	**shone / shined**	**shone / shined**	**brillar**
shit	**shit / shitted / shat**	**shit / shitted / shat**	**cagar**
shoe	**shod / shoed**	**shod / shoed**	**mostrar**
shoot	**shot**	**shot**	**pegar un tiro a**
show	**showed**	**shown**	**mostrar**
shred	**shred / shredded**	**shred / shredded**	**retalhar, triturar**
shrink	**shrank / shrunk**	**shrunk**	**encoger**
shut	**shut**	**shut**	**cerrar**
sing	**sang**	**sung**	**cantar**
sink	**sank**	**sunk**	**hundir**
sit	**sat**	**sat**	**sentar**
slay	**slew**	**slain**	**matar**
sleep	**slept**	**slept**	**dormir**

slide	**slid**	**slid**	**deslizarse, resbalar**
sling	**slung**	**slung**	**lanzar**
slink	**slinked / slunk**	**slinked / slunk**	**zafarse**
slit	**slit**	**slit**	**cortar, abrir**
smell	**smelt / smelled**	**smelt / smelled**	**oler**
smite	**smote**	**smitten**	**golpear**
sow	**sowed**	**sowed / sown**	**sembrar**
speak	**spoke**	**spoken<**	**hablar**
speed	**sped / speeded**	**sped / speeded**	**correr a toda prisa**
spell	**spelled / spelt**	**spelled / spelt**	**deletrear**
spend	**spent**	**spent**	**gastar**
spill	**spilled / split**	**spilled / split**	**derramar**
spin	**spun**	**spun**	**hacer girar**
spill	**spilled / split**	**spilled / split**	**derramar**
spin	**spun**	**spun**	**hacer girar**
spit	**spitted / spat**	**spitted / spat**	**espetar, soltar**
split	**split**	**split**	**dividir**
spoil	**spoilt**	**spoilt**	**arruinar**
spread	**spread**	**spread**	**tender, desplegar**
spring	**sprang / sprung**	**sprung**	**saltar**
stand	**stood**	**stood**	**pararse, estar de pie**
stave (in/off)	**stove / staved**	**stove / staved**	**evitar, aplazar**
steal	**stole**	**stolen**	**robar**
stick	**stuck**	**stuck**	**pegar**
sting	**stung**	**stung**	**picar**
stink	**stank / stunk**	**stunk**	**apestar**
strew	**strewed**	**strewed / strewn**	**esparcir**
stride	**strode**	**stridden**	**andar a pasos largos**
strike	**struck**	**struck / stricken**	**golpear, pegar**
string	**strung**	**strung**	**ensartar, encordar**
strive	**strove / strived**	**striven / strived**	**esforzarse**

swear	**swore**	**sworn**	**jurar**
sweep	**swept**	**swept**	**barrer**
swell	**swelled**	**swelled / swollen**	**hincharse**
swim	**swam**	**swum**	**nadar**
swing	**swung**	**swung**	**mecer**
take (away)	**took**	**taken**	**tomar**
teach	**taught**	**taught**	**enseñar**
tear	**tore**	**torn**	**rasgar, romper**
telecast	**telecast / telecasted**	**telecast / telecasted**	**televisar**
tell	**told**	**told**	**decir**
think	**thought**	**thought**	**pensar**
thrive	**throve / thrived**	**thriven / thrived**	**prosperar**
throw	**threw**	**thrown**	**arrojar, echar**
thrust	**thrust**	**thrust**	**empujar, clavar**
tread	**trod**	**trod / trodden**	**pisar**
understand	**understood**	**understood**	**entender, comprender**
upset	**upset**	**upset**	**afectar, disgustar**
wake up	**woke up**	**woken up**	**despertar**
wear	**wore**	**worn**	**usar, vestir**
weave	**weaved / wove**	**weaved / woven**	**tejer**
wed	**wed / wedded**	**wed / wedded**	**casar**
weep	**wept**	**wept**	**llorar**
wet	**wet / wetted**	**wet / wetted**	**mojar**
win	**won**	**won**	**ganar**
wind	**wound**	**wound**	**dejar sin aliento, ovillar**
wring	**wrung**	**wrung**	**torcer**
write	**wrote**	**written**	**escribir**

6 SELF-ASSESMENT

1) The standard protocol that allows computers to communicate over the Internet is called
   a) IP address
   b) TCP IP
   c) HTTP
2) Which term describes any fast, high-bandwidth connection?
   a) broadband
   b) dial-up connection
   c) Wi-Fi connection
3) Which device converts computer data into a form that can be transmitted over phone lines?
   a) ADSL
   b) a mobile phone
   c) a modem
4) What does WWW stand for in the context of the Internet?
   a) Wide World Web
   b) Web Wide World
   c) World Wide Web
5) What is a computer that serves web pages called?
   a) Web deliverer
   b) Web server
   c) Web page stream
6) What language are web pages written in?
   a) LOGO
   b) HTML
   c) C++
7) What does URL stand for?
   a) Uniform Resource Locator
   b) Universal Resource Location
   c) Uniform Resource Location

8) What is the first page you access when you visit a website, eg http://www.bbc.co.uk, called?
   a) Homepage
   b) First page
   c) Main page
9) What piece of software do you need to view web pages?
   a) Web viewer
   b) Web screen
   c) Web browser
10) What would you be most likely to use to find web pages about a particular topic?
   a) Phone book
   b) Search engine
   c) Forum
11) What is a company that provides Internet access to customers commonly known as?
   a) ISP
   b) EXE
   c) PDF
12) What does ISP stand for?
   a) Insurance Service Provider
   b) Internet Service Provider
   c) Internet Systems Provision
13) What is email short for?
   a) Extraordinary mail
   b) Electronic mail
   c) European mail
14) What is email that can be accessed from any computer with an internet connection and a web browser known as?
   a) Internet mail
   b) Email
   c) Webmail
15) Which of the following is a valid email address?
   a) John:isp@com
   b) john@isp.com
   c) john@isp/com

16) Which of the following is NOT a feature of email?

a) Electronic signatures can be attached
b) Files, graphics or sound files can be sent as attachments
c) Guarantee that the recipient will read the message instantly

17) What is an email that tries to trick a user into providing personal information such as bank details known as?

a) Hacking
b) Phishing
c) Copyright theft

18) Which of the following is NOT a sensible thing to do if you want to prevent your computer becoming infected with a virus sent by email?

a) Open all attachments sent to you
b) Only open attachments from people you know and trust
c) Regularly update your anti-virus software

19) Unsolicited emails are commonly known as what?

a) Spam
b) Rubbish
c) Viruses

20) What is an email attachment?

a) A forwarded email
b) A file sent with an email
c) A reply to an email

ANSWERS

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
B	A	C	C	B	B	C	A	C	B
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
A	B	B	C	B	C	B	A	A	B

7 BIBLIOGRAPHY

http://www.saberingles.com.ar/lists/irregular-verbs.html

https://edu.gcfglobal.org

https://learnenglishteens.britishcouncil.org

https://en.wikipedia.org

https://www.english4it.com/

https://www.businessnewsdaily.com/

Santiago Remacha Esteras. Infotech, English for computers users Student's Book.