Topic 1. University studies

STUDENT’S LIFE

The common definition of student life refers to a group of people with a common purpose or shared duties at an institution of higher learning who want to receive an education that qualifies them for a life profession.

This summer I passed the entrance examinations in the form of centralized testing and on the basis of the results was admitted to the University. Now I’m a first- year student of the Belarusian State University of Informatics and Radioelectronics where I’m taking programming. I am a full-time student and my day-to-day activities depend on my timetable.

My classes usually begin at 9 a.m. I used to get up at about seven or half past seven when I was at school but nowadays, I get up at half past six and drink one or two cups of strong black tea. After that I take shower and have breakfast. I leave at about 8.15 a.m. It takes me 40-45 minutes to get to the University.

As a rule, my classes start at 9 a.m. I have 3 or 4 classes a day: lectures, seminars, practical classes and lab works. They are usually over at 2 p.m., but it actually depends on the day and the week and may be different from day to day.

When I come home, I usually have a rest, make some house duties and do homework. I go to bed at about ten or half past ten. I think it is very important to go to bed before eleven, because it’s really difficult for me to get up in the morning (before the midday). At weekends I usually get up at 10 a.m. and do the same things I do on weekdays.

I can’t say that my university life if rather different from my school one. Neither can I say that they are very similar:

In the university you are the one who is responsible for your study. It’s only your business to do all homework, all labs and learn extra material. In the university you don’t have much time and you must use time management to do everything on time. One mistake here leads you to unprepared subjects or undone homework and labs which is not very well actually.

In my own opinion, the main difference between the university and a school is a lot of profound and specialized subjects such as Basics of Algorithmization and Programming, for example.

HIGHER EDUCATION

From the 9th form students try to decide where to go and what to do after leaving their schools.

The higher education system in Belarus is seen as prestigious due to its high quality and accessibility. There are 58 higher educational establishments, of which 40+ are state owned, 10+ are private and 2 are run by religious organizations. Every establishment occupies its particular niche in training of highly qualified staff for various branches of national economy.

Classical and profile universities provide a two-level system of higher education with academic degrees of Bachelor and Master.

Graduates both from state and private universities are granted state diplomas of higher education. Institutions of higher education provide both free and fee-paying education.

But it is not that easy to become a student. High demand on higher education leads to high entrance competition regardless of form of study or specialty. Therefore, only the very best can study at budget cost. You have to pass all entrance exams in form of centralized testing well. After that you are to compete with other people for your place in the university.

Most courses run for 4-5 or 6 years. Every year is divided by to terms, during which students go to their lectures, practical and lab classes and get knowledge. At the end of each term they have to pass tests and exams to guarantee that they know the material and can apply it to the solutions of real problems.

Grants are available for full-time students and scholarships are awarded to very gifted students.

BSUIR

Today the BSUIR is the leading Belarusian University in the field of computer science, programming, engineering, radio-electronics, radio- and telecommunications. The University includes 10 faculties, 42 departments, the Institute of Information Technologies, the Research and Development Department. The most popular faculties are the Faculty of Information Technologies and Control; the Faculty of Computer Systems and Networks. The overall number of students is more than 17,000 including international undergraduate and postgraduate students.

The course of study lasts four years. The academic year is divided into two terms. Lectures, seminars, laboratory and practical classes make up the majority of teaching time. Students are usually assessed at the end of each semester through a pass-fail system, written and oral examinations, and through a coursework in the form of projects. The students financially covered by the government are granted studentships. Students from other cities lodge in 4 comfortable dormitories with a local net and Internet-access.

University life is more than just lectures and exams. The Trade Union offers a wide range of entertainment and support for students. The Student Club organizes evening parties, discos, festivals and social events. The University is proud of its Brass Band, Students’ Theatre, a folk group, group of Sport Dances, Bard Songs Club, and (of course) English Speaking Club.

Topic 2. Youth and society

LEISURE TIME ACTIVITY

The basic leisure time activities of the young are travelling, doing sports including extreme sports, visiting discos and night clubs or more passive ways of recreation like listening to music or watching TV and videos, and surfing the Internet. Teenagers normally prefer to do extreme sports, that is sports featuring speed, height and danger as they lead to the so-called «adrenaline rush» in participants. They wish to push themselves to the limits of their physical ability and fear, and push the boundaries of a particular sport, such as bungee jumping, climbing, white-water rafting, surfing, windsurfing, etc. Their tastes in music are normally different kinds of popular music associated with youth subcultures, such as hard rock, hip-hop or rap, punk rock, psychedelic rock and the like. In watching TV and videos or going to the cinema, they prefer film genres which are full of action, movement, colour, cinema effects and have a good soundtrack. They normally like action films, comedies, thrillers and cartoons.

Sometimes the ways young people spend their free time varies according to the country, as they sometimes depend on national traditions. For example, British youngsters are really fond of watching football matches and sorts of races such as horse-racing, boat-racing and even dog-racing, as well as playing football, rugby, golf and taking part in races. They are really fond of pets and often spend some time in the evening taking their dog for a walk. In going out for the evening, they still prefer pubs to restaurants, bars and cafes.

TECH ADDICTION

Modern technologies such as mobile phones and handheld computer games are having a great impact on attention levels. Students are hiding these things under the desks so their concentration cannot be equally divided, they are not focusing on what’s going on in class. They can't get motivated to read for a long period of time and are also getting into a bad habit of plagiarism. For their homework, instead of reading the book, they go on the Internet and lift it, rather than reading, understanding and putting it in their own words. Also, concerns are raised about the text-messaging abbreviations to which young people have grown accustomed. They have invented a new language. Of course, language should evolve but maybe not so quickly.

There is a strong link between heavy Internet use and depression, UK psychologists became ensure. The Internet now plays a huge role in modern life, but its benefits are accompanied by a darker side. There is a small subset of the population who find it hard to control how much time they spend online, to the point where it interferes with their daily activities.

Mental Health charities warn the way people spend their time and the kind of social interaction they engage in could well impact on mental wellbeing. In some ways, the Internet can be helpful. To the extent that the Internet encourages meaningful friendships and social connections it can be a very good influence on people's lives. However, social interaction online should not usually re-place an offline social life. Evidence suggests that active pursuits such as exercise and socializing with people face-to-face are among the factors that help us stay in good mental health. Although excessive Internet use can't be said to cause mental health problems, if a web addict is substituting meaningful friendships and socializing with virtual contact on the Internet, this might have an ad-verse effect on their mental wellbeing.

On average, pupils spent between one and two hours on social networking sites each day, sent more e-mails than they received and the majority sent and/or received up to 20 texts a day. Over a third admitted that text shortcuts damaged the quality of their written language, particularly when it came to spelling.

Lots of people admitted copying chunks of information from the Internet into their homework or projects on a number of occasions because the Internet is by far the largest source of information for such work. Lots of people are «very» or «quite» addicted to the Internet or their mobile phones.

YOUTH ISSUES

Less than a third of young people express any interest in politics, according to an official survey. This research suggested the younger electorate were becoming increasingly disengaged with the democratic system, but it also suggested they were more likely to express themselves politically in other ways, such as boycotting environmentally unfriendly products.

Will Brett, head of media at the Electoral Reform Society, said: "It suggests that young people simply aren't as cynical. It suggests there's an opportunity here. Maybe young people have more faith in the system and the key thing is not to waste that opportunity".

Mr. Brett added that many young people were becoming involved in politics in more informal ways, such as social media campaigns, but he added: "We need to find ways of getting them more interested in our system of representative democracy. It's extremely precious".

Unfortunately, many youths have not received either formal or informal guidance on financial matters. So, they may not be ready to make financial choices, such as building a simple budget, planning shopping, and understanding simple financial processes. A report on the results of a financial literacy exam found that high school seniors scored on average 48 percent correct, showing a strong need for more comprehensive financial education for youth in high school.

Only 27% of youth knew what inflation was and could do simple interest rate calculations. Financial illiteracy is more common among low-income individuals because they typically do not have wide access to accurate financial information. With such illiteracy, youth in low-income households can fall victim later as adults to scams, high-interest rate loans, and increasing debt.

Although a majority of teens wanted to learn about money, more than half wanted to learn in an easy way. This could include strategies that are convenient, utilize technology, and are not time consuming for youth.

Very often youth people don’t have enough time because of job, study or both. That’s why youth people need time management and improving their self-organizing to do everything on time.

GENERATION GAP

There have been generation gaps every time the newest generation develops the ability to think for themselves and every generation has to pass thought that. It is not a modern phenomenon; and in my own opinion there is nothing to do with this problem.

No kid believes his/her parents were kids themselves. More over sometimes even adults forget that they were children long time ago and start being sure that kids are simply “small adults” which is definitely not the case! Their parents have never felt what they are feeling, could have no way of relating to them, etc. And then, because technology does speed along and those who used to be on the cutting edge just don’t care anymore about being up-to-the-minute, the kids think adults are hopeless and can’t possibly understand what they’re dealing with.

And to a degree, they are right. Adults don’t not understand why young people are so attached to their phones for communication. To them, you want to talk, pick up the phone – the actual telephone part – and call. Or better yet, walk over. Parents and grandparents really don’t understand why taking children’s phone away from a week is so stressful to them. They don’t get that this is their connection to the world because it wasn’t theirs. Their phones are just simply phones. It is hard for adults to really understand how completely isolated youths are without technologies now.

Topic 3. Choosing a career

IT INDUSTRY TODAY

Strictly speaking, Information Technology has been influencing society for thousands of years. But these days it’s widely accepted that the forefront of technology lies in digital revolution. Just as machines have extended man’s mechanical power and his convenience and comfort, Information Technology is extending man’s mind or in other words his intellectual power.

Interest in the digital revolution isn’t a technology issue though. It’s necessary to notice that in essence it isn’t an amendment to the core businesses, ideals, ethics or movements. It simply permits them to perform at a larger scale and rather more expeditiously. The benefits of IT in e-business are actually obvious.

What’s the role this technology plays in today’s society?

1. Information technology role in our daily life is to make our life easier. It acts as an assistant.
2. It’s a medium that allows massive volumes of knowledge to be held on, processed or transferred at a lightning speed.
3. There’s a lot of data at hand to create choices, maintain relationships, monitor markets, etc.
4. Social networking websites help people share cultural values and people start to respect each other’s’ culture.

Economy, science, technology, banking, transportation, communication, healthcare, education, culture, defines can’t do without IT nowadays.

Our world now operates within a digital framework. This is going to require more hands-on deck to administer, manage and create technology.

IT training can prepare you for a career in a variety of industries: oil companies, government agencies, manufacturing firms, insurance companies, aviation related companies, construction, hospitality industry, security, healthcare, the fashion industry, government, sports, banking – you name it.

CAREER OPPORTUNITIES

Information Technology (IT) is a broad term that includes all aspects of managing and processing information and related technologies. IT is a field which is comparatively young in comparison with other fields. The professionals of this field are young and enthusiastic and dynamic.

IT has basically two potential zones to work upon. They are the hardware and the software. Hardware includes the maintenance aspects of physical components of computers. Software on the other hand is designing programs in the way of step by step instructions which help companies and other organizations recruiting and dealing with large number of people. While choosing a computer engineer’s position one should focus on job descriptions rather than job titles. Most probable career paths options in software are presented below:

A Computer Engineer

A computer engineer’s job is different from that of a computer hardware engineer. Hardware experts design the actual computers. A computer software engineer develops tests and evaluates software to make computers operational. Computer engineers may also be responsible for constructing and managing an organization's computer system. Most computer engineers work as part of a tech team in an office or laboratory environment. Computer engineers design and develop a wide range of software including business applications, network control systems, operating systems, middle-ware and games. Computer engineers start by analysing user needs. Then engineers develop, design and test software to meet those needs. The process involves detailed flowcharts, diagrams, documents and instructions referred to as algorithms. Conversion of algorithms is typically done by computer programmers.

Computer engineers are divided into two categories. Computer applications software engineers analyse users’ needs to design applications software or specialized utility programs. Computer systems software engineers coordinate construction of an organization’s computer systems and handle maintenance and expansion.

Computer applications software engineers work with various programming languages based on the purpose of the program and where it runs. Some engineers develop package computer applications while others develop completely customized applications for specific organizations and even develop databases.

Marketing, sales, technical resources, logistical and technical support are all possible career options for computer systems software engineers. Quite a number of systems software engineers work for companies that create and install the computer systems for other businesses and organizations.

After computer engineers and system analysts design software programs, computer programmers write them. Programmers also work on updating, modifying, expanding and repairing existing programs. Often programmers work closely with computer engineers to boost productivity through enhanced technology.

Most computer engineer jobs require a bachelor’s degree. For some positions, a master’s degree is preferred. College majors for computer engineers include computer science, mathematics, software engineering, computer information systems. Employers prefer to hire computer engineers who are familiar with the latest technology.

Computer engineers must have certain skills to be employable. Computer engineers need strong analytical skills and the ability to remain focused on multiple tasks at once. Many computer engineers work with clients and must express complex ideas in simple terms. Creativity and ingenuity are important skills for computer engineers designing new software programs. Computer engineers should work well with technical analysis and abstract concepts. Business skills make it possible for computer engineers to advance to management positions.

A Systems Analyst

A systems analyst uses computers and related systems to design new IT solutions, modify, enhance or adapt existing systems and integrate new features or improvements, all with the aim of improving business efficiency and productivity. They must possess a high level of technical expertise and clear insights into current business practices.

They examine existing IT systems and business models; analyse systems requirements; undertake product development; implement, configure and test feasible solutions.

The analyst acts as liaison between the client and the developers. They conduct a cost analysis and agree the timeframe to implement the proposed solution. They specify and shape the system requirements and operations, the user interface and output and present the proposal to the client. They work closely with the client team, including commercial managers and software developers, during both the report and implementation phase.

It is vital to look closely at job descriptions rather than job titles e.g. analysts may be known as systems or business analysts and the trend is currently towards including the term solutions in the job title.

An Information Systems Manager

An information systems manager is responsible for the computer systems within a company.

They oversee installation; ensure backup systems operate effectively; purchase hardware and software; provide the ICT technology infrastructures for an organization; contribute to organizational policy regarding quality standards and strategic planning.

Information systems managers work in every size of organization in the industry and the service sector, usually with a staff of technicians, programmers and database administrators reporting to them. You’ll need experience in the sector, in areas like technical support or operations, before becoming a manager.

Information systems managers are responsible for the implementation of technology within an organization and direct the work of systems and business analysts, developers, support specialists and other computer-related workers.

The post holder will usually be an experienced worker with technical expertise coupled with an understanding of business and management principles. Duties might require an understanding of the capabilities and constraints of technology and resource implications in terms of budgets, as well as the training and recruitment of specialist staff.

Although the title of information systems manager is becoming more common in the ICT sector, job titles may vary. For example, you might be a: service delivery manager; functional manager; systems manager.

A Database Administrator (DBA)

A database administrator (DBA) is responsible for the performance, integrity and security of a database. They will also be involved in the planning and development of the database as well as troubleshooting any issues on behalf of the users. A DBA makes sure that databases have the following qualities: data remains consistent across the database; data is clearly defined; users access data concurrently, in a form that suits their needs; there is provision for data security and recovery control (all data is retrievable in an emergency).

DBA roles vary depending on the type of database, the processes they administer and the capabilities of the DBMS in use.

Web Designers

Web designers plan, create and code web pages, using both non-technical and technical skills to produce websites that fit the customer’s requirements. They are involved in the technical and graphical aspects of pages, producing not just the look of the website but determining how it works as well. Web designers might also be responsible for the maintenance of an existing site.

The term web developer is sometimes used interchangeably with web designer, but this can be confusing. Web developing is a more specialist role, focusing on the back-end development of a website and will incorporate, among other things, the creation of highly complex search functions.

The recent growth in touchscreen phones and tablet devices has dictated a new way of designing websites, with the web designer needing to ensure that web pages are responsive no matter the type of device a viewer is using. Therefore, the need to test websites at different stages of design on a variety of different devices has become an important aspect of the job.

Applications Developers

Applications developers translate software requirements into workable programming code and maintain and develop programs for use in business. Most will specialize in a specific development field – such as mobile phone applications, accounting software, office suites or graphics software – and will have in-depth knowledge of at least one computer language.

The work of an applications developer differs with a systems developer in that systems software allows a computer to actually run. Users interface with the applications software, which is served by the systems software. Applications, or apps, can be written for a particular system, such as Windows or Android, or across numerous platforms, including computers and mobile devices.

Job titles and specific duties may vary between organizations but the role usually involves writing specifications and designing, building, testing, implementing and sometimes supporting applications using programming languages and development tools. Applications developers work in a wide range of business sectors, including finance and the public sector. They often work as part of a team with other IT professionals, such as software engineers and systems analysts, and write programs according to their specifications.

A SUCCESSFUL SPECIALIST TODAY

The IT profession is respected globally because of the impact Information Technology (IT) has on society. IT is used in solving problems and creating solutions. All sectors of the economy require the services of skilled technical IT personnel. Information technology professionals are responsible for designing, developing, supporting and managing computer hardware, computer software, maintaining, installing, configuring and managing IT systems and networks, including the Internet.

IT is a field that emphasizes knowledge and personal contribution. A career in IT offers not only money, but much more than money. A career is about self- actualization issues – knowledge, empowerment, recognition, opportunity, influence, reputation, and self-reliance. But if immediate results are what you are after, then the

IT field might not be what you want. An IT career is more like a marathon than a short sprint.

Most computer related jobs require a bachelor’s degree. For some positions, a master’s degree is preferred. Relevant skills and experience matter. The way to become an IT professional is studying a degree at university which teaches you the fundamentals first.

At the university you not only get the knowledge but also:

– get the stamp on your résumé (Once they open a certain job, organizations use filters to fill it in appropriately, and one of the filters is the university degree);

– create the network of people (meeting different people increases your possibilities to find a good job; getting in contact with professors, lecturers and the like might help you to develop professional projects, the university also offers many channels to get in touch with companies and organizations, including the contact of people working inside the HR department);

– develop the competencies. Apart from the knowledge the university teaches you how to collect, filter, interpret and present information. It also teaches you to communicate clearly, to interact with other people, to take responsibility of your actions, and so on. All those competencies will be useful for the rest of your life regardless of the career you will choose. The knowledge you learn at the university will come and go while competencies stay once you develop them. Knowing what to expect out of something is half way through, so make sure you get it all from your experience at the university.

In IT tomorrow is unpredictable. This is the very field where if you stand still you will go backwards. Once you have more information you are in a better position to know what you want. Be resourceful in finding information and keeping yourself up to date. Keep on learning and acquiring knowledge through the Internet, books, training and practice. Read IT journals and the computer sections of most newspapers and magazines. Talk to people on the job – get info on the good and the bad. As the Chinese proverb states, the stranger that asks questions doesn’t get lost. Visit the workplace, get familiar with and understand the working environments.

Competent IT practitioners are often respected and recognized for their contributions. Becoming respected in IT requires creativity, the ability to handle challenges, to have excellent problem-solving skills, a healthy respect for others and an always-learning attitude.

The profession is respected but each individual must create his or her own path. You can be highly respected in IT if you manage your relationships well. You need to have very good interpersonal skills and know the value of good teamwork. Do you help and encourage others? You know the stuff; you’ve got the certs but how courteous are you in making your demands? Will you treat colleagues, clients and employers with respect? Are you considerate and even-handed in your interactions and working relationships? The way you resolve conflict is also about respect.

MY SPETIALYTY  
(Software Engineer example)

SKILLS AND QUALIFICATIONS

***Common for IT:***

Emotional Intelligence

Working with and Managing Remote Teams

Data Science Expertise

Analytical skills

Creativity

Problem-solving skills

Critical thinking skills

Communication skills

Leadership skills

***For this specialty:***

UML

Application concepts

Unit tests

Co-working systems

Continuous Integration

Frameworks

XML/JSON

Bug-tracking systems

UI (JS, HTML)

Multithreading etc.

WAYS OF PROFETIONAL DEVELOPMENT AND GROWTH

(USE ARTICLE OR CPD)

THE ARTICLE  
(WAYS OF PROFETIONAL DEVELOPMENT AND GROWTH for Software Engineers)

***1. Day Job***

The projects we work on day-to-day always require some research and the implementation of new techniques (optimizing platforms for performance, conducting security reviews, migrating proprietary applications, etc.)

Moreover, we work closely as a team on technical implementations. Folks come up with certain ideas that we evaluate against the business case. We do peer code reviews before deployments, load test solutions, build automated tests and tend to experiment with new libraries or frameworks.

The combination of working on complex projects and collaborating with other tech members is highly valuable unless you work in a dev factory reusing generic code at scale.

***2. Engineering Blogs***

Follow several technical blogs and social media accounts discussing new frameworks, machine learning, programming paradigms and the like. Spending a few hours per week watching blogs + reading a couple of tech books monthly can help you stay up to speed.

***3. R&D***

Whenever you stumble upon a new technique or technology which may come handy at a later point, try to invest some time playing with it, building a test project, or integrating a library into an existing project.

Could be an AI-driven framework, an ad management library, a new IDE, a new profiling tool, configuring the web server or optimizing the database layer.

***4. Pet Projects***

Build some apps that automate certain processes or integrate systems together. For instance, built a simple time tracking tool in Ruby, a Slack bot in Node, a PM wrapper with Electron, a task manager with Java.

Community events may be of help, too. Contributing to Open Source may help you learn a lot about the web development ecosystem at scale.

While participating at large contributor events across the world, you have the opportunity to brainstorm together with hosting agencies, enterprise providers, product development companies, support teams, translation experts, accessibility consultants, and other industry peers solving problems for different industries.

***5. Cultivate Your Engineering Professional Development***

Spend a decade working in 2 or 3 good technical companies.

You can start with a large organization hiring dozens or even hundreds of developers in your area. There are multinational outsourcing companies or non-technical corporations that still need technical manpower.

It may be easier to start with an entry-level job, go through their extensive training process, and take it from there.

At a later point, work for a mid-sized company or a start-up. There are different paradigms and levels of responsibility there. There’s also a higher chance that your company will pull it off, leading to steady and massive growth and a senior management position for yourself (or a VP of Technology and the like).

It’s both a great learning experience and has a chance to substitute your dream with a future in the company that you’ve joined early enough on (and thus help with leading and growing it).

If you have a chance to work for the Big 4 or another widely popular tech company, that would probably be quite exciting as well.

It’s likely that your dream of having your own software engineering company will evolve over time and you may be quite satisfied with your progress to date.

Otherwise, always consider your initial plan at all times. In order to do that, focus on those three areas during your first decade (and further):

***What You Need to Focus On***

Spend a good portion of your time learning and reading. Your jobs teach you so much about an organization and the business. As a technical founder, you want to excel in all areas in the technical landscape as well as all things business. Follow other business owners and senior managers, successful team leaders in large organizations, start-up owners. Read about sales and marketing, hiring, management, operations, investing, financial management and everything else that a business owner has to deal with at first (and oversee later).

Engage in networking – both offline and online. Your colleagues may be your future hires, co-founders, or partners. Your managers may be your vendors or clients. People you meet at conferences may vouch for your commitment and trustworthiness. Grow your network and regularly interact with your peers whenever possible.

Build your personal brand. Developing your brand will not only help you attract clients or recruits if you decide to start a business, but will also help you find great job opportunities, land freelance gigs, or develop other strategic partnerships. It may open the doors to public speaking or even writing a book. All in all, personal branding may speed up the process of founding a company and generating some leads. Becoming a thought leader and an educator in your field (through blogging, social media, Quora participation) you can increase your exposure and value within the community.

If you decide to start your business by then, you’ll already know the foundations and have learned practical lessons over the past decade of learning.

CPD  
(Continuing Professional Development)

The aim of personal and professional development is to help you manage your own learning and growth throughout your career.

Professional development can: increase your confidence and **credibility**; increase efficiency; develop your ability to influence and lead; enable networking; keep your knowledge and skills current; help you to achieve career goals enable you to become a better employee. Professional development is something to be valued, **cherished** and actively pursued. It is proven to enable career development and progression, allowing you to excel and shine within your current role and as you progress.

Continuing Professional Development (CPD) is a process of building, maintaining and enhancing your knowledge and skills. CPD helps you plan your development, review what you have learnt and evaluate the effectiveness of your activity. Your commitment to CPD is important as the activities you choose will help **to underpin your validity** and competence as a professional.

The [Chartered Institute of Personnel and Development (CIPD)](http://www.cipd.co.uk/) describes professional development in this way *‘Continuing Professional Development (CPD) is a combination of approaches, ideas and techniques that will help you manage your own learning and growth. The focus of CPD is firmly on results – the benefits that professional development can bring you in the real world. Perhaps the most important message is that one size doesn’t fit all. Wherever you are in your career now and whatever you want to achieve, your CPD should be exactly that: yours.’*

CPD is not always formal and linear; activities can range from formal educational activities such as instructor-led training courses, **workshops** or seminars to more informal **approaches** such as work-based learning or mentoring. CPD can also include self-directed study such as e-learning courses and structured reading. It’s a record of what you experience, learn and then apply.

CPD helps ensure you have the knowledge and skills necessary to succeed as a professional. It helps you to build professional confidence and, in turn, the reputation of the profession; adapt positively to change by continuously updating skills support any career goals by focusing on relevant training and development; be more productive and efficient by reflecting on your learning and highlighting gaps in your knowledge and experience and planning action accordingly.

Any professional must take ownership of their career and development. The Continuous Professional Development Cycle includes the following steps: identifying your development needs through planning and then carrying out your learning activities, **reflecting on** your learning and then applying it and sharing it with others. It can also be as simple as asking yourself these three questions:

1) Where am I now?

2) Where do I want to be?

3) How am I going to get there?

Professional development is something that can, and invariably does, happen in a variety of ways. Professional development isn’t always a **linear** activity; in fact, almost 80% of your development will be completed in the workplace by undertaking activities that might include special projects, secondments or activities that are new to you.

Training is teaching, or developing in oneself or others, any skills and knowledge that relate to specific useful competencies. Training has specific goals of improving one’s capability, capacity, productivity, and performance. In business, training is the investment of resources in the employees of a company so they are better equipped to perform their job. The types of resources invested may include time and money to develop, **implement**, and evaluate training programs.

The well-trained employee acquires an advantage for him- or herself. By participating in training, employees can deepen or **expand** their existing skill set and increase their understanding of the organization. In addition, a well-trained employee may be able to take advantage of internal promotion opportunities and becomes more **marketable** if he or she leaves the company. Other potential benefits are as follows: increased job satisfaction and morale among employees; increased employee motivation; increased efficiencies in processes, resulting in financial gain; increased capacity to adopt new technologies and methods; increased innovation in strategies and products; reduced employee turnover; enhanced company image, e.g., building a reputation as a ‘great place to work’. Training provides greater skill and knowledge to employees, which translate to improved job performance.

Topic 4. Job hunting

JOB APPLICATION

A CV (also known as a Curriculum Vitae) or résumé is a written overview of your skills, professional qualifications, education, accomplishments, and work experience. You will usually be required to submit your CV/ résumé to be considered for the position. Usually paired with a cover letter, a CV helps you demonstrate your abilities and convince your employer that you are qualified and employable.

Today there’s a lot of debate around cover letters. Many people will say it is not necessary. But a cover letter is a great way to introduce yourself and generate interest from a potential employer. Together with a CV, they work wonders.

**5 Steps How to Write a CV without Work Experience**

**(Closer to our real life)**

Whether you’re a college student or a graduate, the best way to write a CV with no job experience is to get some experience. The second best way is to make the most of the experiences you’ve got. Before anyone will hire you, they want to get to know you. Your CV is a snapshot of the most important things you’ve accomplished in your professional life. It should be specific, organized, and custom-made for the position you’re looking to fill in.

***Format your résumé***

Your CV needs to be well-presented and easy to navigate. Most employers are only spending seconds on their first review of your CV, so break the information into clearly structured sections, use bullet points and a bold header to bring forward significant information.

***Personal Profile***

If you want to create a strong first impression, start your CV with a killer personal statement. It should be a brief paragraph about the type of person you are, your skills, achievements. Describe the reasons you’re looking to enter into a specific sector, tailoring your experiences to the role you’re applying to.

***Education***

Since you’re a university student, your education and qualifications are your strongest selling point and you want to put this section at the top of your CV. You need to be demonstrating the experiences you gained throughout your educational history. Look to add information about university projects, thesis, the coursework you completed. Excellent academic results, conferences or special training are of great importance too. Think outside your classes and even add extra-curriculum activities such as volunteering. There is no need to add every qualification and grade but instead highlight those that are most suited to the industry you are applying for.

***Highlight your Skills***

Key skills may form the body of your CV. Demonstrate your transferrable skills as well such as communication, intellectual, interpersonal, language skills. Use examples from your studies, hobbies, interests, work, even private life. For example, if you look for communication skills, discuss times where you presented a project to your class or got involved in a debate. Remember to also add core skills required in any role such as being a team player or having a strong work ethic.

***Work Experience***

Here you should highlight your professional achievements which are directly connected to the position you are applying for. Consider periods of full-time and part-time employment. You can even highlight the work experience you obtained in school, university. Also, you may add any personal pursuits, professional training, freelance projects you’ve focused on during your education. For example, if you want to start a career in design, then add about any projects where you’ve produced a website or any other designs in your free time. Your past internships/placements, voluntary work are important too.

Putting together a CV with no work experience isn’t easy or fun, especially for a college student. If you feel frustrated, angry, or embarrassed, that’s good. Let that emotion motivate you to drive harder towards your goals. If you’re old enough to get a job, focus your efforts on gaining enough experience to land that first job. A great way to start is by getting a summer internship.

***Cover letter***

A cover letter is a one-page document that you submit as part of your job application (alongside your CV or Resume).

Its purpose is to introduce you and briefly summarize your professional background. On average, your [cover letter should be from 250 to 400 words long](https://novoresume.com/career-blog/how-long-should-a-cover-letter-be).

A good cover letter can spark the HR manager’s interest and get them to read your resume.

A bad cover letter, on the other hand, might mean that your application is going directly to the paper shredder. So, to make sure this doesn’t happen, it’s essential to know how to write a convincing cover letter.

Keep in mind, though, that a cover letter is a supplement to your resume, not a replacement. Meaning, you don’t just repeat whatever is mentioned in your resume.

If you’re writing a cover letter for the first time, writing all this might seem pretty tough. After all, you’re probably not a professional writer.

The thing is, though, you don’t need to be creative, or even any good at writing. All you have to do is follow a tried-and-tested format:

* Header - Input contact information
* Greeting the hiring manager
* Opening paragraph - Grab the reader’s attention with 2-3 of your top achievements
* Second paragraph - Explain why you’re the perfect candidate for the job
* Third paragraph - Explain why you’re a good match for the company
* Formal closing

The plan of the cover letter:

1. Pick the Right Cover Letter Template
2. Start the Cover Letter with a Header
3. Greet the Hiring Manager
4. Write an Attention-Grabbing Introduction
5. Explain why you’re the perfect person for the job
6. Explain why you’re a good fit for the company
7. Wrap up with a call to action
8. Use the right formal closing

JOB INTERVIEW

If you are invited to an interview, you have made it to the shortlist. There are many candidates who have similar qualifications, skills, and experience. So, the interview is your opportunity to prove you are the best candidate for the job.

The science is simple here - the more you prepare for an interview, the more comfortable you’ll be when you walk in, and the better you’ll do. Going into an interview blind is equivalent to walking into an exam without even looking at your textbook. There will be no other time to make your first good impression and be selected in front of your rivals.

Recommended steps:

* prepare questions to ask at the interview;
* do some research on the company you are applying for;
* choose an appropriate outfit;
* practice greeting your interviewer;
* study your resume to know everything about it;
* find out the type of interview you will be going to attend;
* print the direction to the interview to be on time;
* practice interview questions.

Most likely to hear questions:

1. What can you tell us about yourself?
2. How do you work with ‘difficult’ people?
3. Where do you see yourself in five years’ time?
4. What do you know about our company’s products?
5. What are you good at?
6. What are the weaknesses that you have?
7. What university do you attend and why did you choose it?
8. What skills do you have relevant to this job?
9. Did you have any trouble finding our building?

PROFESSIONAL ETHICS

Professional ethics are principles that govern the behaviour of a person or group in a business environment. Like values, professional ethics provide rules on how a person should act towards other people and institutions in such an environment.

Unlike values, professional ethics are often codified as a set of rules, which a particular group of people use.

This means that all those in a particular group will use the same professional ethics, even though their values may be unique to each person.

The Code is an example of a codified set of professional ethics for those who choose to enter the immigration advice profession.

***Ethical principles***

Ethical principles underpin all professional codes of conduct. Ethical principles may differ depending on the profession; for example, professional ethics that relate to medical practitioners will differ from those that relate to lawyers or real estate agents.

However, there are some universal ethical principles that apply across all professions, including:

* honesty
* trustworthiness
* loyalty
* respect for others
* adherence to the law
* doing good and avoiding harm to others
* accountability.

***Codes of conduct***

Professional codes of conduct draw on these professional ethical principles as the basis for prescribing required standards of behaviour for members of a profession. They also seek to set out the expectations that the profession and society have of its members.

The intention of codes of conduct is to provide guidelines for the minimum standard of appropriate behaviour in a professional context. Codes of conduct sit alongside the general law of the land and the personal values of members of the profession.

The primary value of a professional code of conduct is not as a checklist for disciplining non-conforming members, although breaches of a code of conduct usually do carry a professional disciplinary consequence.

Rather, its primary value is to act as a prompt sheet for the promotion of ethical decision-making by members of that profession.

Professional codes of conduct provide benefits to:

* the public, as they build confidence in the profession’s trustworthiness
* clients, as they provide greater transparency and certainty about how their affairs will be handled
* members of the profession, as they provide a supporting framework for resisting pressure to act inappropriately, and for making acceptable decisions in what may be ‘grey areas’
* the profession as a whole, as they provide a common understanding of acceptable practice which builds collegiality and allows for fairer disciplinary procedures
* others dealing with the profession, as the profession will be seen as more reliable and easier to deal with.

***Other contributors to professional ethics***

***Fiduciary duties***

When an adviser agrees to assist a client, they agree to take on a level of responsibility for that person and their immigration matter. The client becomes dependent on the adviser in relation to that assistance. This is a fiduciary relationship between the fiduciary (the adviser) and a principal (the client). Even without a Code this fiduciary relationship means the adviser has certain obligations to their client.

***Contractual obligations***

When an adviser enters into a contract (or written agreement) with a client this creates legally binding obligations to perform the terms of the contract in a particular way. This includes a duty to act with diligence, due care and skill, and also implies obligations such as confidentiality and honesty, even if they are not specifically set out in the contract.

Many ethical issues are likely to stem from advisers’ relationships with clients. Most of these can be overcome by having clear terms in a written agreement about how certain matters will be dealt with, such as the sharing of confidential information, the use of interpreters, refunds and invoicing. More information on written agreements can be found in the Code of Conduct Toolkit.

CORPORATE CULTURE

If you are interested in turning your job hunt into a job offer, it is important to know exactly what employers look for when hiring new full-time employees. During an interview, the hiring manager will ask soft skill questions to determine if you are a good fit for corporate culture. Employees who consistently demonstrate a good work ethic are considered to be valuable assets.

Employers value employees who understand and possess a willingness to work hard. But it is also important to work smart. This means learning the most efficient way to complete tasks and finding creative ways to save time while completing daily assignments. Besides, employers appreciate employees who come to work on time, are responsible for their actions and behaviour.

Employers seek employees who take the initiative and have the motivation to get the job done in a reasonable period of time. A positive attitude gets the work done and motivates others. Being open to changes provides an opportunity to complete work assignments more efficiently. While employees often complain that changes in the workplace don’t make sense or make their work harder, often these complaints are due to a lack of flexibility.

Employers respect employees who maintain a sense of honesty and integrity above all else. Good relationships are built on trust. They want to know that they can trust what you say and what you do.

Employers hire applicants who have a positive attitude, are not afraid to ask questions, can take the lead, and the most important, keep up with the advancements in the field. All these will make you a vital asset for the company’s success.

WORK AREA SAFETY

Workplace safety should never be taken lightly with any business. Doesn’t matter if you’re 1,000 employees strong or 10. Any businesses, regardless of size, must account for safety regulations, steps, and more detailed options for their staff from the get-go. Preventative measures against accidents and/or workplace-related deaths are key for fostering a healthy, safe work environment.

There are some companies out there who may not be fully versed in workplace safety regulations or might not be equipped in every area of the office to handle any unforeseen circumstances.

For instance, let’s say you’re a towing and shipping company and most of your workforce is tied up in manual labour sectors where lifting, packing and stacking heavy shipments will occur more frequently. Or, on the opposite end of the spectrum, you’re an accounting firm where there’s hardly any lifting or physically demanding labour going on.

Both examples still must heed similar safety rules, have a system in place to readily inform each and every employee on preventative tips and regulations, and strive to accomplish what your business wants most: everyday safety. From OSHA compliance to inspections, there’s a whole laundry list of tips on workplace safety that businesses can take with them. Some are simple, while others are a bit more complex in nature, but at the end of the day, they all can contribute to a safer haven for your staff.

***1. Proper Uniforms***

This is a critical base for businesses such as construction, home improvement, the aforementioned packing and shipping corporations on down to firefighters and other areas that require overly-protective headgear and uniforms. Construction workers must be wearing hard hats at all times in specified zones of the job site. Firefighters must have the latest fire-retardant outfits to go along with sturdy helmets. Chemists must wear safety goggles while they are inside a laboratory.

Putting up signs to reinforce the matter and educating the supervisors to stay on top of uniform regulations should be active from the moment the first employee clocks in to the last.

***2. Designate Proper Emergency Exits***

There’s a reason we did three or four fire drill exercises as a kid each year in school. As annoying and (forgive the pun) alarming as they could be, it helped everyone in the building familiarize themselves with the exits. This same exercise should apply for every business. Not that every employee go in a single-file order and move at the sound of an alarm, just that they are aware and have some document that outlines emergency procedures.

This document should map out every exit doorway, ensure you have emergency exit signs posted in their assigned posts, detail up-to-date smoke detectors, signify water spouts to quench possible fires and assure you and your staff that each building code is covered front-to-back.

***3. Open Discussions***

Setting aside time at the end of the day once a month to discuss safety rules and general working environment is a great way for managers and supervisors to assess the overall quality of current measures taken. Getting feedback from employees is helpful because it opens the manager’s eyes to potential hazards that went unnoticed, how well certain areas are doing and little touch-ups here and there that go a long way towards keeping employees safe and happy in the office.

While this may not be a safety regulation, per say, it’s an outside factor that many businesses would do well to follow.

***4. Promote Health Codes***

You know those signs you see when entering a restaurant bathroom next to the sink that inform you that all employees must wash their hands before exiting? Having little indicators like those in the wash room, in the kitchen and general areas of heavy foot traffic is important on many fronts. The most important being health code standards, educating cleanliness, and encouraging employees to take every step necessary to make the room healthy for the next individual.

***5. Proofing the Building***

This falls in the category of getting the building inspected from time to time on down to subtle improvements around the building, stairways and exterior pathways. Little safety measures like adding ribbed, rubber padding along the ends of stairway steps, de-icing the walkways leading up to the office, mats to stamp out slippery footing and other helpful precautions can give your employees as much peace of mind to know their well-being is being accounted for as much as possible.

***In summary, here's how you can create a safe working environment in 5 steps:***

* Ensure that you are dressed appropriately for your working conditions and that all safety equipment is up to date.
* Communicate the emergency plan and make sure exits routes are properly designated.
* Discuss safety rules and general working practices. Getting regular feedback will ensure a safe and healthy work environment.
* Promote health codes and standards by educating your employees on the importance of health safety and cleanliness.
* Inspect your working area and building. Ensure that walking paths are clear, stairs, and railing are secure and slip-proof.

These tips can help businesses from all over achieve a healthy balance between workplace security and overall productivity.

Topic 5. Digital basics

DIGITAL REVOLUSION, DATA AND INFORMATION

At present we live in the information age. It is a period of history when information is easy to access and affects many aspects of everyday life. The importance of information is not new. It has always been a powerful tool. The information age is unique because of its underlying technology based on digital electronics. The digital revolution offers advantages, but requires adaptations. Digital innovations require societies to make adjustments to traditions, lifestyles and legislation. Digitization is the process of converting text, numbers, sounds, photos and video into data that can be processed by digital devices. Data processing is based on an input-processing-output cycle which is often referred to as the IPOS cycle. The digital era has evolved through four phases, beginning with big, expensive computers and progressing to modern digital world in which small inexpensive digital devices are everywhere.

In the first phase computers were huge, complex and expensive devices. They existed in limited numbers, primarily housed in big corporations and government agencies. Computers and data processing became crucial tools for effective business operations. The second stage was presented by personal computing which is characterized by small, standalone computers powered by local software. Local software refers to any software that is installed on a computer’s hard disk. The third phase of the digital revolution materialized as computers became networked and when the Internet was opened to public use. A computer network is a group of computers linked together to share data and resources. The Internet is a global computer network. The Web is a collection of linked documents, graphics, and sounds that can be accessed over the Internet. A key aspect of the Web is that it adds content and substance to the Internet. From 1996–2010 computing was characterized by the Web, e-mail, multiplayer games, music downloads and enormous software applications. Then Facebook, Twitter and Google Apps have sent computing in new directions.

Cloud computing characterized the fourth phase of the digital revolution. Cloud computing provides access to information, applications, communications and storage over the Internet. Before cloud computing most computers ran software based locally. With cloud computing all that changes. You can store your data in the cloud, making it available no matter what computer you use. Using a cell phone service provider your mobile device accesses the Internet. The touchscreen on your mobile gives you access to apps that play music, show movies, report news. You use Google or Wikipedia to access information and when you need to produce a document, you head over to Google to access its cloud-based word processor. You spend lots of time maintaining your profiles on social networking services and interacting with friends through cloud-based social media.

Computers do so many things and come in such a variety of shapes and sizes that it might seem difficult do distil their common characteristics into an all-purpose definition. A computer is a multipurpose device that accepts input, processes data, stores data, and produces output, all according a series of stored instructions.

Computer input is whatever is typed, submitted or transmitted to a computer system. An input device gathers data and transforms it into electronic signals for the computer to store and manipulate. Output is the result produced be a computer. Some examples of computer output include reports, documents, music, graphs and pictures. Output devices display, print, or transmit the results of processing. Computers manipulate data in many ways, and this manipulation is called processing. In a computer most processing takes place in a component called the central processing unit or CPU. The CPU of most modern computers is a microprocessor, which is an electronic component that can be programmed to perform tasks based on data it receives. Memory is an area of a computer that temporarily holds data waiting to be processed, stored, or output. Storage is the area where data can be left on a permanent basis when it is not immediately needed for processing.

Data is typically stored in files. A computer file is a named collection of data that exists on a storage medium. The series of instructions that tells a computer how to carry out processing tasks is referred to as a computer program or simply a program. These programs form the software that sets up a computer to do a specific task.

Computers and other digital devices work with such things as texts, numbers, music, images, speech, and video. The amazing aspect of digital technology is that it distils all these different elements down to simple pulses of electricity and stores them as 0s and 1s. Data refers to the symbols that represent people, events, things, and ideas. In everyday conversation people use the terms data and information interchangeably. Nevertheless, some technology professionals make a distinction between the two terms. They define data as is any raw facts or observations that describe a particular phenomenon that represents people, events, things and ideas. Data becomes information when it is presented in a format that people can understand and use. Data is used by machines, such as computers, information is used by humans. Information is simply data that has a particular meaning within a specific context. Information may be data that has been processed in some way. When we speak of data processing, the input is data, the output is useful information. So, data processing is a series of actions or operations that convert data into useful information.

DATA REPRESENTATION

Data representation refers to the form in which data is stored, processed, and transmitted. For example, devices such as smartphones, tablets, and computers store numbers, text, music, photos, and videos in formats that can be handled by electronic circuitry. Those formats are data representations. Data can be represented using digital or analog methods. The term to digitize means to convert raw, analog data into digital format represented by 0s and 1s. A photograph or drawing can be digitized by treating it as a series of coloured dots. Each dot is assigned a binary number according to its colour. A digital image is simply a list of colour numbers for all the dots it contains. In a similar way, music can be digitized by assigning binary codes to notes.

Digital data is text, numbers, graphics, sound, and video that have been converted into discrete digits such as 0s and 1s. In contrast, analog data is represented using an infinite scale of values. Most computers use the simplest type of digital technology – their circuits have only two possible states. For convenience, let’s say that one of those states is «on» and the other state is «off». When discussing these states, we usually indicate the «on» state with 1 and the «off» state with 0. These 1s and 0s are referred to as binary digits. It is from this term that we get the word «bit» – binary digit. Computers use sequences of bits to digitally represent numbers, letters, punctuation marks, music, picture, and videos.

Numeric data consists of numbers that might be used in arithmetic operations. Computers represent numeric data using the binary number system, also called «base 2». The binary number system has only two digits: «0» and «1». No numeral like «2» exists in this system, so the number «two» is represented in binary as «10». The important point to understand is that the binary number system allows computers to represent virtually any number simply by using 0s and 1s, which conveniently translate into electrical «on» and «off» signals.

Character data is composed of letters, symbols, and numerals that are not used in arithmetic operations. A digital computer uses a series of bits to represent letters, characters, and numerals. Computers work with digital data under the control of a computer program. Computer programmers create programs that control digital devices. These programs are usually in a written in a high-level programming language, such as C, C++, Python or Java. An important characteristic of most programming languages is that they can be written with simple tools, such as a word processor and they can be understood by programmers. The human-readable version of a program created in a high-level language by a programmer is called source code. Computers employ several types of codes to represent character data, including ASCII, EBCDIC and Unicode. ASCII requires only seven bits for each character. ASCII requires codes for 128 characters.

DATA PROCESSING

The procedure for translating source code into 0s and 1s can be accomplished by a compiler or an interpreter. A compiler converts all the statements in a program in a single batch and the resulting collections of instructions, called object code, is placed in a new file. Most of the program files distributed as software contain object code that is ready for the processor to execute. As an alternative to a compiler, an interpreter converts and executes one statement at a time while the program is running. After a statement is executed the interpreter converts and executes the next statement. A microprocessor is hard-wired to perform a limited set of activities, such as addition, subtraction, counting and comparisons. This collection of preprogramed activities is called an instruction set. Instruction sets are not designed to carry out any specific task, such as word processing or playing music. Instead, an instruction set is designed to be general purpose so that programmers can use it in creative ways for the wide variety of tasks performed by all kinds of digital devices. The list of codes for a microprocessor’s instruction set, called machine language, can be directly executed by the processor’s circuitry. A set of machine language instructions for a program is called machine code. To avoid confusion, most computer files contain a file header with information about the code used to represent the file data. A file header can be read by the computer, but never appears on the screen. By reading the header information, a computer can tell how a file’s contents were coded.

A single high-level instruction very often converts info multiple machine language instructions. A programmer creates human-readable source code using a programming language. A compiler or an interpreter converts source code into machine code. Machine code instructions are a series of 0s and 1s that correspond to a processor’s instruction set. A microprocessor contains miles of microscopic circuitry and millions of miniature components divided into different kinds of operational units, such as the ALU and the control unit. The ALU (arithmetic logic unit) is the part of the microprocessor that performs arithmetic operations, such as addition and subtraction. It also performs logical operations, such as comparing two numbers to see if they are the game. The ALU uses registers to hold data that is being processed. The microprocessor’s control unit fetches each instruction. Data is loaded into the ALU’s registers. Finally, the control unit gives the ALU the green light to begin processing. The instructions that a computer is supposed to process for a particular program are held in memory. When the program begins the memory address of the first instruction is placed in a part of the microprocessor’s control unit called an instruction pointer. The control unit can then fetch the instruction by copying data from that address into its instruction register. From there, the control unit can in processing. The ALU is responsible for performing arithmetic and logical operations. It uses registers to hold data ready to be processed. When it gets the go- ahead signal from the control unit, the ALU processes the data and places the result in an accumulator. When the computer completes an instruction, the control increments the instruction pointer to the memory address of the next instruction, and the instruction cycle begins again.

THE ISSUE OF FAIR USE

Fair use is a loophole in the copyright law that allows someone other than the copyright holder to copy and distribute copyrighted material under certain conditions without first obtaining permission. It has been said that fair use is the safety valve of copyright because without it, copyright’s constitutional purpose to promote learning, advance knowledge, and promote the progress of science would be useless. The law specifically allows fair use for such purposes as criticism, comment, news reporting, teaching, and scholarship or research.

That being said, trying to decipher those purposes and conditions is a daunting and confusing task. Fair use is the most important concept relating to intellectual property that educators and librarians are likely to face. Fair use is a significant issue for educators in that it is used daily in instruction but it is not clearly defined.

Fair use evolved as courts tried to balance the rights of copyright holders and society’s interest in making copies of a work, primarily for teaching and news reporting. If not for fair use, every time a librarian or teacher wanted to use copyrighted material for educational purposes, permission would have to be obtained from the copyright holder.

Obviously, this was not practical. Without fair use, the restrictions on copyright would severely limit the educational uses of all the material created by others. The goal of fair use is to avoid the rigid application of the copyright statute when it would stifle the very creativity the law was meant to foster.

Fair use is controversial in that it is a contradiction of the basic concept of copyright’s five rights. Fair use provides the privilege of using an author’s work without permission or payment.

Four factors help guide those who wish to utilize its fair use aspects.

1. The purpose and character of the use, including whether such use is of a com-metrical nature or is for non-profit educational purposes
2. The nature of the copyrighted work
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole
4. The effect of the use upon the potential market for or value of the copyrighted work

Topic 6. Hardware basics

THE AVAILABILITY OF DIGITAL DEVICES

Storage devices. A storage medium (media) is the disk, tape, CD, DVD, paper, or other substance that contains data. A storage device is the mechanical apparatus that records and retrieves data from a storage medium.

A computer works with data that has been coded into bits that can be represented by 1s and 0s. These 1s and 0s are transformed into changes in the surface of a storage medium. How this transformation happens depends on the storage technology. Three types of storage technologies are used for personal computer: magnetic, optical, and solid state.

Storage devices are compared using such criteria as versatility, durability, speed, and capacity.

MAGNETIC STORAGE TECHNOLOGY. Magnetic storage stores data by magnetizing microscopic particles on a disk or tape surface. Data stored magnetically can be easily changed or deleted simply by changing the magnetic orientation of the appropriate particles on the disk.

Hard disk drive is a device for storing information on the principle of magnetic recording. A hard disk is one or more platters and their associated read- write heads. Hard disk platters rotate as a unit on the spindle to position read-write heads over specific data. A read-write head mechanism in the disk drive magnetizes particles to write data, and senses the particles’ polarities to read data. The density of particles on the disk surface provides hard disks with great capacities. A hard disk drive mechanism includes a circuit board called a controller that positions the disk and read-write heads to locate data.

OPTICAL STORAGE TECHOLOGY. CD and DVD technologies are classified as optical storage, which stores data as microscopic light and dark spots on the disc surface. The disk is quite durable and data less susceptible to environmental damage than data recorded on magnetic media. Optical technologies can be grouped into read-only, recordable, and rewritable.

SOLID STATE STORAGE or flash memory is a technology that stores data in erasable, rewritable circuitry, rather than on spinning disks. Solid state storage is durable, removable and provides fairy fast access to data because it includes no moving parts.

The term Universal Serial Bus is a standard type of connection for various devices. A USB flash drive is removable and rewritable. It plugs directly into a computer’s system unit using a built-in connector. It is durable and requires no card reader. Often flash drives are used to update the BIOS or UEFI (Unified Extensible Firmware Interface) motherboards. UEFI-enabled machines have faster start-up and shut-down times as compared to BIOS-based machines. A USB-storage device supports encryption, which is not unimportant for the safe storage of information. Flash drives can be used as a key for activation (USB Keys) applications.

BASIC INPUT DEVICES include: a keyboard; a mechanical or optical mouse; a scanner; a digital camera; a microphone; a trackpad (touchpad/touchscreen). Some devices require software, called a device drive to set up communication between your computer and the device. The USB port can automatically detect a newly connected device and attempt to establish the setting necessary for sending data between it and the computer.

OUTPUT DEVICES are computer hardware; they are connected via special connectors, directly to the motherboard or expansion cards. An output device can be absolutely any device that will help you get information in the form in which it will be possible to perceive it.

A computer display system includes a display device such as a monitor and graphics circuitry that generates the signals for displaying an image on the screen.

A computer monitor is usually an LCD (liquid crystal display) producing an image by manipulating light within a layer of liquid crystal cells. Image quality is a factor of screen size, dot pitch, width of viewing angle and colour depth. LCD technology is now being replaced by LED (light-emitting diode) technology which is more environmentally friendly.

Audio devices facilitate the output of sound information. A sound card is an expansion board or a built-in integrated chipset to create sound on a computer. As a rule, a sound cards or sound chip is supplied with the firmware on the disc.

A computer printer is an output device that produces computer-generated text or graphical images on paper. A computer sends data for a printout to the printer along with a set of instructions on how to print that data. The data that arrives at a printer along with a set of instructions and its printer language requires memory. Printers differ in resolution, print speed, duty cycle, duplex capability, memory and networkability.

The advantage of a network-enabled printer is that it can connect directly to a computer network; it can be placed in a location convenient for all the network users. It might be useful for printing from handheld devices that cannot be connected to a printer by cable. A plotter is a device that allows reproducing high-precision drawings, maps, schemes and other information on paper.

HARDWARE SECURITY

For trouble-free computer use, it is important to secure and regularly maintain your computer equipment. Computers are prime targets for thieves. You may keep your devices nowhere to be found by them.

Your chances of recovering a stolen computer improve if you have taken some steps in advance, such as recording the computer’s serial, number, affixing a tracking label, or installing tracking software.

Security Tracking of Office Property plates leave an indelible tattoo on your computer equipment, which contains a unique ID number registered in the international STOP database. Tracking and recovery software, such as Cyber Angel and Lo-ach for Laptops, secretly sends a message as soon as a thief uses a stolen computer to log on to the Internet. This message contains the computer’s exact location and is directed to a tracking or monitoring canter.

A power surge is a sudden increase in electrical energy affecting the current that flows to electrical outlets. You can protect your computer equipment from power surges by plugging it into a surge suppressor, instead of directly into a wall outlet. For added protection during thunderstorms, shut down your computer, turn off all your peripheral devices, and unplug the surge suppressor and all computer-related cables from wall outlets, including the cable for your modem.

To prevent hardware problems, you can undertake some preventive maintenance to extend the life of your computer equipment. Regularly clean your computer components and peripheral devices to keep them in good condition.

Your computer probably has a special safe mode designed for professional troubleshooting. When operating in this mode, your computer uses a limited version of the operating system that allows you to use your mouse, screen, and keyboard, but no other peripheral devices.

THE ISSUE OF E-WASTE

E-waste, a garbage, techno-trash – all the unwanted and outdated computers, monitors, printer·, cell phones, disk drives, disks, CDs, and DVDs. According to the Environmental Protection Agency, 3 million tons of it is discarded every year. In the United States alone, almost eight printer cartridges are discarded every second, and millions of CDs and DVDs end up in landfills every year.

Computers and other electronic gear contain toxic substances such as lead, cadmium, and mercury. When discarded equipment is burled in landfills, these substances can leach into groundwater and streams. When burned, electronic components can emit toxic dioxin.

E-waste is a global problem. As countries struggle to deal with discarded electronic components, an alarming amount of e-waste is shipped to developing countries where villagers, working for pennies day, are exposed to toxic chemicals as they attempt to reclaim resalable metals from discarded equipment. Throughout the emerging world, ugly e-waste dumps defile the landscape and have yet unknown health effects. Every country generates e-waste.

Despite laws that ban e-waste transhipping, loopholes allow discarded but working electronics to be shipped as donations. Tons of donations arrive every day in port cities, such as Hong Kong, where they follow a shadowy route to unregulated workshops and dump sites.

Some illegal e-waste originates in legitimate recycling centres, where consumers assume electronic components will be handled in environmentally friendly ways. Many recycling centres ship the e-waste to third parties. Without careful monitoring, that e-waste can be diverted to offshore locations where it piles up, waiting to be disassembled by backstreet labourers ungoverned by environmental protection regulations.

Developed countries have strict environmental regulations designed to prevent toxic substances from polluting air, land, and water. Proper disposal is expensive, however. In countries with high labour costs and stringent environmental regulations, the value of compounds retrieved from e-waste does not cover the cost of extraction.

The high cost of properly processing e-waste makes grey market options attractive. E-waste can be handled more cost-effectively in emerging countries where environmental regulations are ignored, wages are pitiful, and workers are not covered by health and safety laws.

So, who is responsible for e-waste sweatshops and pollution? Is it consumers in developed countries who deposit unwanted gear at recycling stations that don't carry out the recycling process in-house, or is it the recycling firms that ship e-waste to third parties? Is it the firms that ship e-waste to emerging countries or the governments that can't close the loopholes on e-waste transhipping?

Perhaps the responsibility lies with emerging countries that are unable to control e-waste sweatshops and ignore the resulting environmental and human casualties. Wherever the blame lies, consumers who are aware of the problem can become more responsible in the way they dispose of unwanted gear to keep it out of landfills at home and offshore.

Topic 7. Network basics

WEB BASICS

Networks can be classified according to their size and geographic scope (PAN, LAN, MAN, WAN). You can think of a network as a spider web with many interconnecting points, are referred to as node. A network node usually contains a computer, networked peripheral, or network device. To connect to a LAN, a computer requires network circuitry, sometimes referred to as a network interface card (NIC). Network circuitry is built into the main system board of most personal computers. If not, a NIC can be added to a slot in the system board or a USB port.

A networked peripheral is any device that contains network circuitry to directly connect to a network. A storage device that directly connects to a network is called network attached storage (NAS). A network device is any electronic device that broadcasts network data, boosts signals, or routes data to its destination. The most important network device is a router, which acts as a central distribution point for getting data to its destination.

Data in a network with wired connections travels from one device to another over cables. Wired connections are fast, secure and simple to configure. This type of connection is more secure than wireless one because a computer can only join a network if it is physically connected by a cable. An example of wired network technology is Ethernet.

A network without wires transports data through the air, eliminating the need for cables. Networks of all sizes, from PANs to LANs and WANs, can use wireless technologies, such as radio signals, microwaves, and infrared light. Most wireless connections transport data as RF signals (radio frequency signals). They are sent and received by a transceiver (a combination of a transmitter and a receiver) that is equipped with an antenna.

Microwaves can be aimed in a single direction and have more carrying capacity than radio waves. Microwave installations usually provide data transport for large corporate networks.

THE INTERNET TODAY

Today, the most popular wireless LAN technology is WI-FI. Additional wireless technology is Bluetooth. Bluetooth is a short-range wireless network technology that is designed to make connections between two devices. A communications channel or link, is a physical path or a frequency for signal transmissions.

Most people are familiar with television remote controls that use infrared light beams. Infrared can also carry data signals, but only for short distances and with a clear line of sight, which is used in the newest wireless technology LI-FI.

Bandwidth is the transmission capacity of a communications channel. High-bandwidth communications systems, such as a cable TV and DSL, are referred to as broadband, whereas systems with less capacity, such as dial-up Internet access, are referred to as narrowband.

A communication protocol refers to a set of rules for efficiently transmitting data from one network node to another. Protocols set standards for encoding and decoding data, guiding data to its destination.

A packet is a parcel of data that is sent across a computer network. Each packet contains the address of a sender, the destination address, a sequence number, and some data. Some communications networks, such as the telephone system, use a technology called circuit switching, which essentially establishes a dedicated, private link between one telephone and another for the duration of a call. Unfortunately, circuit switching is rather inefficient.

A more efficient alternative to circuit switching is packet switching technology, which divides a message into several packets that can be routed independently to their destination. Every packet includes the address of its destination device. Packets from many different messages can share a single communications channel. When data reaches its destination, it is checked for errors one last time and then the packets are reassembled into their original configurations.

SECURITY CONSERNS

Networks with wired or wireless connections are vulnerable to a variety of threats, including viruses, theft, and equipment failure. Many threats can be handled using techniques for standalone computers. Network equipment should be connected to power strips to prevent damage from power spikes. Data should be backed up in a case of a hard drive failure and computers should be protected by antivirus software. Wireless signals are broadcasted through the air, and like the signals from a radio station, they can be picked up by any device equipped with a receiver tuned to the right frequency. Wired connections funnel data through a cable, not through the air. Wired signals can be intercepted only by physically tapping into the cable or router.

If your network is not secured, hackers can easily connect to it, monitor transmitted data, access connected devices, spread viruses, and your network as a launching pad for spam.

Encryption transforms a message in such a way that its contents are hidden from unauthorized readers. Encryption is designed to keep messages secret.

Symmetric key encryption uses the key to encrypt a message as well as decrypt it. Symmetric keys are not practical for e-mail and other situations in which the person receiving encrypted data does not have the key beforehand.

Public key encryption eliminates the key-distribution problem by using one key to encrypt a message, but another key to decrypt the message. Public key encryption is a crucial technology for e-commerce and e-mail. When you use a secure connection to transmit a credit card number, the server sends a public key to your browser. Your browser uses this public key to encrypt the credit card number. After it is encrypted, no one- not even you – can use the public key to decrypt the message. The encrypted message is sent to a Web server, where the private key is used to decrypt it.

An intrusion is any access to data or programs by hackers, criminals, or other unauthorized persons. As the result of an intrusion, data can be stolen or altered, system configurations can be changed to allow even more intrusions, and software can be surreptitiously installed and operated under the remote control of a hacker.

A communications port is the doorway that allows a computer to exchange data with other devices. It is a portal through which data flows. A port probe (or port scan) is the use of automated software to locate computers that have open ports and are vulnerable to unauthorized access. One of the easiest steps to enhance your security is to turn it off when you are not using it. When your computer is turned off, its ports are inactive and they are not vulnerable to intrusions.

A firewall is software or hardware designed to filter out suspicious packets attempting to enter or leave a computer. Firewall software helps keep your computer secure in several ways. It ensures that incoming information was actually requested and is not an unauthorized intrusion. It blocks activity from suspicious IP addresses and – best of all – it reports intrusion attempts so that you can discover whether hackers are trying to break into your computer.

One of the most effective steps you can take to secure your computer from intrusions is to install a router. It screens IP addresses to keep locally addressed packets within the LAN so that they are delivered without traveling a circuitous route over the Internet and back. Your router has its own IP address. The key point about your IP address is that it is routable. A routable IP address is one that can be accessed by packets on the Internet. When you connect your PC to a router and request an IP address, your router answers your request, not the ISP. Most routers are configured to assign private IP addresses.

A private IP address is non-routable IP address that can be used within a LAN, but not for Internet data transport. Network address translation (NAT) is the process your router uses to keep track of packets and their corresponding private or public IP addresses. Sales representatives and telecommuters often access corporate networks from home by using a secured connection called a virtual private network.

TRACKING TECHNOLOGY

The internet backbone is a network of high-capacity routers and fibre-optic links that provides the main routes for data traffic across the internet. Backbone links and routers are maintained by network service providers (NSPs). NSP equipment and links are tied together by network access points (NAPs). An internet service provider (ISP) is a company that offers Internet access to individuals, businesses, and smaller ISPs. To communicate with an ISP, your computer uses some type of communications device, such as modem. A modem contains circuitry that converts the data-carrying signals from your computer to signals that can travel over various communications channels.

The elapsed time for data to make a round trip from point A to point B and back to point A is referred to as latency. The utility called Ping (Packet Internet Grouper) sends a signal to a specific Internet address and waits for a reply. When a reply arrives, Ping reports that computer is online and displays the elapsed time for the round-trip message.

Another utility called Traceroute records a path of packet to its round-trip speed. You can use Traceroute to analyse the latency of your data as it hops from one router to the next. The connection speeds advertised by ISPs refer to the amount of data that travels between a computer of subscriber and ISP within a given time period. Your connection speed depends on whether you connect to your ISP using a telephone, cable television, satellite, or wireless link. Actual speed can differ from maximum speed because links are susceptible to interference that can hinder signals. Upstream speed can also differ from downstream speed. Upstream speed is the rate of data that is uploaded from one computer to the Internet. Downstream speed is the rate of data downloaded to your computer. When upstream speeds differ from downstream speeds, you have an asymmetric Internet connection. When upstream and downstream are the same, you have a symmetric Internet connection.

Cable Internet service is a means of distributing always-on broadband Internet access over the same infrastructure that offers cable television service. Cable signals are not particularly vulnerable to environmental interference but data transport speeds are affected by subscriber use. The cable you share with your neighbours has a certain amount of bandwidth. The more and more neighbours use the service, it might seem to get slower and slower. Most people are familiar with services that provide also offer Internet access.

Topic 8. Software basics

TYPES OF SOFTWARE

The term software means all non-hardware components of a computer that determines the tasks a digital device can help you accomplish. The two main categories are system software and application software. Operating systems, device drivers, utilities, and programming languages are classified as system software. Application software is designed to help people accomplish real-world tasks, whereas system software is designed for computer centric tasks.

Music software offers many ways to work with music, sound effects, and narration from your desktop, laptop, or handheld computer. It includes downloading, playing and recording music files, creating playlists, transferring music to handheld devices, editing, cropping and mixing digital recordings, streaming, and identifying songs.

A mapping application displays satellite, aerial, or street maps used to locate places and get directions between two addresses. Location-based software is able to access your current location and use it to show you the closest shops, restaurants, ATMs, and theatres.

Business software is a broad term that includes vertical and horizontal market software. Vertical market software is designed to automate specialized tasks in a specific market or business. Horizontal market software is generic software that just about any kind of business can use.

A type of system software called utility software is designed to help you monitor and configure settings for your digital gear, its operating system, or application software.

A device driver is software that helps a peripheral device establish communication with a computer. This type of system software is used by printers, monitors, sound cards, network cards, storage devices, modems, mice, and scanners.

Office suites are popular with individual computer owners and in business environments. They are sometimes referred to as productivity software because they offer features that really help get work done. An office suite is a collection of programs that typically include word processing, spreadsheet, presentation, and database modules.

Word processing packages give you the ability to create, spell-check, edit, and format a document on the screen before you commit it to paper. It includes a thesaurus, a grammar checker, a spelling checker, a page layout (the physical position of each element on a page), paragraph styles (the alignment of text and the space between each line of text) and different fonts (sets of letters that share a unified design).

Spreadsheet software provides tools to create electronic spreadsheets. You can make calculations, based on simple equations that you create or more complex, built-in formulas. It also includes special data-handling features that allow you to sort data, search for data that meets specific criteria, and print reports.

Database software helps you enter, find, organize, update, and report information stored in a database. It stores data as a series of records, which are composed of fields that hold data. A record holds data for a single entity – a person, place, thing, or event. A field holds one item of data relevant to a record. Many databases contain hundreds or thousands of records. If you want to find a particular record or a group of records you can enter a query that describes the information you want to find.

A query language provides a set of commands for locating and manipulating data. A natural language query is a question stated in a language such as English, rather than an esoteric query language. A keyword search, popular with search engines such as Google, is simply a collection of words relevant to your search. A query by example (QBE) simply requires you to fill out a form with the type of data you want to locate.

SECURITY THREATS

The terms malicious software and malware refer to any computer program designed to surreptitiously enter secretly a computer, gain unauthorized access to data, or disrupt normal processing operations. Malware includes viruses, worms, Trojans, bots, and spyware. Malware is created and unleashed by individuals referred to as hackers, crackers, black hats, or cybercriminals. Some malware is released as a prank. In an increasing number of cases, malware is unleashed for monetary gain.

A computer virus is a set of program instructions that attaches itself to a file, reproduces itself, and spreads to other files. A common misconception is that viruses spread themselves from one computer to another. They don’t. Viruses can replicate themselves only on the host computer. A key characteristic of viruses is their ability to lurk in a computer for days or months, quietly replicating themselves. While this replication takes place, you might not even know that your computer has contracted a virus; therefore, it is easy to inadvertently spread infected files to other people’s computers. In addition to replicating itself, a virus usually delivers a payload which can corrupt files, destroy data, or otherwise disrupt computer operations. A trigger event, such as a specific date, can unleash some viruses. Viruses that deliver their payloads on a specific date are sometimes referred to as time bombs.

Some malware does a good job of cloaking itself, so victims are unaware of its presence. Cloaking techniques are great defence mechanisms because when victims aren’t aware of malware, they won’t take steps to eradicate it. Some hackers cloak their work using rootkits. The term rootkit refers to software tools used to conceal malware and backdoors that have been installed on a victim’s computer. Rootkits are usually distributed by Trojans.

SECURITY SOFTWARE

Security software is designed to protect computers from various forms of destructive software and unauthorized intrusions. Security software can be classified into various types: antivirus, antispyware, anti-spam, and firewalls. Each type focuses on a specific security threat.

A security suite integrates several security modules to protect against the most common types of malware, unauthorized access, and spam. A security suite has both advantages and disadvantages. First, it costs less than purchasing standalone security modules. Second, a single interface for accessing all of the security suite’s features is much less complex than having to learn how to configure and run several different products. On the other hand, most security suites cannot run concurrently with standalone security products, and overlapping security coverage from two similar products can cause glitches.

Antivirus software is a type of utility software that looks for and eradicates viruses, Trojan horses, worms, and bots. Some antivirus software also scans for spyware. Modern antivirus software attempts to identify malware by searching your computer’s files and memory for virus signatures. A virus signature is a section of program code, such as a unique series of instructions that can be used to identify a known malicious program, much as a fingerprint is used to identify an individual.

Two aspects of your antivirus software periodically need to be updated. First, the antivirus program itself might need a patch or an update to fix bugs or improve features. Second, the list of virus signatures must be updated to keep up with the latest malware developments. Virus signatures and other information that antivirus software uses to identify and eradicate malware are stored in one or more files usually referred to as virus definitions (or a virus database).

If, during the scanning process, your virus protection software identifies a virus, worm, or Trojan horse in a file, it can try to remove the infection, put the file into quarantine, or simply delete the file. A quarantined file contains code that is suspected of being part of a virus. For your protection, most antivirus software encrypts the file’s contents and isolates it in a quarantine folder, so it can’t be inadvertently opened or accessed by a hacker.

Despite occasional misses, however, antivirus software and other security software modules are constantly weeding out malware that would otherwise infect your computer. It is essential to use security software, but also important to take additional precautions, such as making regular backups of your data.

SOFTWARE PIRACY

Piracy takes many forms. End-user piracy includes friends loaning distribution discs to each other and installing software on more computers than the license allows.

Software counterfeiting is the large-scale illegal duplication of software distribution media, and sometimes even its packaging. Counterfeit software is sold in retail stores and through online auctions. Often the packaging looks so authentic that buyers have no idea that they have purchased illegal goods.

Internet piracy uses the Web as a way to illegally distribute unauthorized software. In Net jargon, the terms appz and warez (pronounced as "wares" or "war EZ') refer to pirated software. Some warez have even been modified to eliminate any forms of copy protection.

In many countries software pirates are subject to civil lawsuits for monetary damages and criminal prosecution, which can result in jail time and stiff fines. Nonetheless, software piracy continues to have an enormous impact. According to researches $130 billion of software was legitimately purchased worldwide, but software worth a whopping $53 billion was pirated.

DISADVANTAGES OF PIRACY:

* According to industry experts, software piracy has a negative effect on the economy. Software production fuels economic development in many countries. Lowering global piracy by 10 percentage points over a four-year period would add more than 500,000 jobs and $141 billion in worldwide economic growth.
* Decreases in software revenues can have a direct effect on consumers, too. When software publishers are forced to cut corners, they tend to reduce customer service and technical support.
* As an alternative to cutting support costs, some software publishers might build the cost of software piracy into the price of the software. The unfortunate result is that those who legitimately license and purchase software pay an inflated price.

ADVANTAGES OF PIRACY:

* Using a pirated software, pour people can get the access to the most required programs in their lives and, probably, make their lives a bit better.
* Also, pirated programs can be used as a trial version of the program if there is no official trial one and u can’t pay too much for unknown app.
* As an alternative to cutting support costs, some software publishers starts using a subscription system which gives people the possibility to use many different programs of these publishers and stop paying and using them if they don’t need it anymore. This way leads to lowering prices and offers to save the quality of tech-support.
* And last, but not least, sometimes counterfeit software can work even better than an official legal one (for example: several games).

Topic 9. Information systems basics

THE SDLC

Most organizations use information systems to operate more effectively, gather information, and accomplish tasks. In this section, the term information system refers to a system that uses computers and usually includes communications networks. An information system collects, stores, and processes data to provide useful, accurate, and timely information. Today most information systems rely on computers and communications networks to store, process, and transmit information with far more efficiency than would be possible using manual systems. Every organization has its mission and all activities that take place in an organization, including those that involve computers, should contribute to this mission. One of the major functions of any information system is to help people make decisions in response to problems.

An information system progresses through several phases as it is developed, used, and finally retired. These phases encompass a system development life cycle, usually referred to as the SDLC known as System Development Life Cycle, which provides a general outline of how an information system evolves and delineates the phases of system development. Systems analysis and design is a discipline that focuses on developing information systems according to the phases of an SDLC.

The Planning phase for an information system project includes the following activities: assemble the project team, justify the project, choose the development methodology, develop a project schedule, produce a project development plan

The goal of these activities is to create a Project Development Plan. The Project Development Plan is usually reviewed and approved by management. This planning document includes:

* A short description of the project, including its scope;
* A justification for the project, which includes an estimate of the project costs and potential financial benefits;
* A list of project team participants;
* A schedule for the project, including an outline of its phases.

Depending on the scope of the problem and the expertise of the professional staff, an information systems project can be managed by an in-house information technology department or outsourced to a development firm. A system development project team is assigned to analyse and develop an information system. Other members of an organization might also be asked to participate in various phases of the project.

Justifying a project often involves identifying problems and opportunities within an organization’s current information system. Project team members can identify problems and opportunities using a variety of techniques, such as interviews and data analysis. As part of the planning phase, the project team selects one or more methodologies that provide structure for the development effort. A system development methodology guides developer through the phases of system development and specifies what takes place in each phase; it encompasses the activities, procedures, methods, best practices, deliverables, and automated tools that system developers follow to complete the SDLC. The next activity is project scheduling. It begins in the planning phase, but stretches throughout the entire project. Project managers organize the work into tasks and milestones, which can be scheduled and assigned. As tasks are completed, the schedule is updated and adjusted. Project management software is assigned to help in planning and scheduling. It helps managers track and visualize the complex interactions between tasks. Popular project management offerings include open source software such as Open Workbench, and commercial software such as Microsoft Project. Industry standard tools for scheduling and project management include: PERT (Program Evaluation and Review Technique) is a method for analysing the time needed to complete each project task and identifying the minimum time needed to complete the total project. A WBS (work breakdown structure) breaks a complex task into a series of subtasks. A Gantt chart uses bars to show the timing of development tasks as they occur over time. Each bar on the chart represents a task; the length of a bar indicates the task’s expected duration.

ANALYSIS PHASE

The Analysis phase begins after the project team selects a development methodology, draws up the Project Plan, and receives permission to proceed from management. The goal of the analysis phase is to produce a list of requirements for a new or revised information system. Activities for analysis phase are: study the current system, determine the system requirements, and write requirements report. The project team determines requirements by interviewing users and studying successful information systems that solve similar problems. Another way to determine requirements is to construct a prototype. A systems analyst shows the prototype to users, who evaluate which features of the prototype are important for the new information system. Most new information systems are designed to replace a system or process that is already in place. It is important to study the current system to understand its strengths and weaknesses before designing a new system. After the project team studies the current system and then determines what the new system should do, system requirements are incorporated into a document called a System Requirements Report that describes the objectives for an information system. System requirements are the criteria for successfully solving problems identified in an information system. A new or updated information system should meet requirements defined by the project team. A CASE tool (computer-aided software engineering tool) is a software application designed for documenting system requirements, diagramming current and proposed information systems, scheduling development tasks, and developing computer programs.

SYSTEM DESIGN PHASE

If in the Analysis phase, the project team determines what the new information system must do, in the Design phase the project team must figure out how the new system will fulfil the requirements specified in the System Requirements Report. The project team chooses a solution, selects hardware and software, and designs detailed application specifications. There might be more than one way to solve the problems and meet the requirements identified in the analysis phase of the SDLC. Some potential solutions might be better than others, more effective, less costly, or less complex. The basis for choosing hardware and software includes general criteria, such as cost and delivery time. The project team should also consider the vendor’s reliability, expertise, and financial stability. A request for proposal (RFP) is a document that describes the information system problem and the requirements for the solution. An RFP essentially asks a vendor to recommend hardware and software for the solution, and to describe the vendor’s qualifications for implementing the solution. A request for quotation (RFQ) is a request for a formal price quotation on a list of hardware and software. A project team issues an RFQ to vendors when it knows the make and model of the equipment and the titles of the software packages needed but wants to compare prices from different vendors. Technical criteria for hardware might include processing speed, reliability, upgradability, maintenance costs, and warranty. Technical criteria for software might include reliability, compatibility, and the availability of patches to fix program errors. The project team has to consider the overall architecture based on level of automation, processing methodology, and network technology. Software alternatives might also be considered. Exactly what happens next in the system design phase depends on the type of solution selected. If a turnkey solution is selected, the next step might be to get approval to move into the implementation phase of the SDLC. In contrast, if the project team selects a solution that requires custom programming, the team’s systems analysts will create a set of application specifications that describe the way the information system’s software should interact with users, store data, process data, and format reports. But the last step in this stage is to write application specifications. There is a key element in developing an effective information system and play a critical role in ensuring that the development process proceeds efficiently.

IMPLEMENTATION PHASE

During the Implementation phase of the SDLC, the project team supervises the tasks necessary to construct the new information system. The tasks that take place during the implementation phase can include: purchase and install hardware and/ or software, create applications, test applications, finalize documentation, train users, convert data, convert to new system.

As the implementation phase begins, programming languages, development tools, and application software needed for the new information system are purchased, installed, and tested to ensure that they work correctly. Software testing can reveal problems that result from incompatibilities with existing hardware and software. These problems must be corrected before continuing with system development. Testing might also reveal bugs (errors) in the software, which must be corrected by the software developer. In addition to new software, the specifications for most new information systems require new hardware, which can either replace old equipment or supplement existing equipment. When the software for an information system is created by using a programming language or an application development tool, programmers must create and test all the new software modules. When an information system is constructed using application software, the software sometimes must be customized. Software customization is the process of modifying a commercial application to reflect an organization’s needs. Customization might include modifying the user interface, enabling various security settings, selecting the menus that appear on the screen, and designing forms or reports. A rigorous testing process is the only way to make sure a new information system works. Different types of testing during the implementation phase help identify and fix problems before the information system is incorporated into day-to-day business activities. One of the most important tasks during the implementation phase is to make sure the information system is completely documented so that it can be used effectively and modified easily. The documentation for an information system can be broadly categorized as system documentation or user documentation. System documentation describes a system’s features, hardware architecture, and programming. User documentation describes how to interact with the system to accomplish specific tasks. It might also include tutorials that demonstrate how to get started and how to accomplish specific tasks. In preparation for using a new information system, users generally need training on software use and data entry. During training sessions, users learn how to interact with the interface, use the new system to perform day-to- day tasks, and find additional information in user manuals, procedure handbooks, or video tutorials. Training sessions for a new information system can be conducted by members of the project team or outsourced to professional trainers. The old data must also be loaded into the new system – a process called data conversion. System conversion refers to the process of deactivating an old information system and activating a new one. It is also referred to as a «cutover» or «to go live». When converting data from an existing computer system to a new system, a programmer can write conversion software to read the old data and convert it into a format that is usable by the new system. Without such software, users would be forced to manually re-enter data from the old system into the new system.

MAINTENANCE PHASE

The Maintenance phase is the last and the longest SDLC phase and it lasts until the system is retired. It involves day-to-day operation of the system, making modifications to improve performance, and correcting problems. Three key concepts ensure good quality of maintenance service: reliability, availability, and serviceability. The term quality of service (QOS) refers to the level of performance a computer system provides. Typical maintenance phase activities ensure that the system functions as well as possible. During the maintenance phase, an information system is likely to undergo many changes to meet an organization’s needs. Changes can include: operating system, application software and security upgrades, user interface revisions to make the system easier to use, application software revisions to fix bugs and add features, hardware replacements necessary to retire defective equipment or enhance performance, hardware, software, or network adjustments to maintain and enhance quality of service. Although the analysis, design, and implementation phases of the SDLC are costly, for many organizations, the maintenance phase is the most expensive because it is the longest. When an information system first goes alive, maintenance costs are high while programmers work out bugs and users clamour for suggest. After most of the bugs are fixed and users become familiar with the information system, maintenance costs decrease. As an information system near the end of its useful life span, repair costs rise, and changing business practices begin to require modifications that time-consuming and expensive to implement.

INFORMATION SYSTEM DATA SECURITY

Threats against information systems are increasing. As with personal computers, common threats to corporate information systems include natural disasters, power outages, equipment failures, human errors, software failures, security breaches, acts of war, and malware. Threats to a corporate information system can affect thousands of people. Natural disasters can completely shut down a computer system, cut off service to customers, and potentially destroy the system completely. Power outages can be caused by natural disasters, overloaded power grids, planned brownouts, and rolling blackouts. Equipment failures can occur in any hardware component of a computer system. The risk of failures increases as a hardware component ages, but they can occur in brand-new hardware. Human errors are mistakes made by computer operators, for example, entering inaccurate data and failing to follow required procedures. Software failures can be caused by bugs or flawed software design. Flaws in critical software that controls air traffic or nuclear power plants can be deadly. Other bugs may cause security leaks that allow unauthorized access to corporate servers. Security breaches include stolen data, physical intrusions, and deliberate sabotage. Cyberterrorism can cause damage to critical national infrastructures such as power grids and telecommunications systems. Malware can damage just about any computer system. You might have experienced the nuisance of rooting out a virus from your personal computer.

With the escalation of online crime, corporate identity theft has become a major security threat. When a company’s brand is used without authorization, the company has become a victim of identity theft. Corporate identity attacks can undermine customer confidence, overwhelm customer service, generate bad publicity and result in lost revenues. The Internet makes it easy to steal corporate identities and use them for phishing scams and fake Web sites. It is not difficult for hackers to copy logos and other graphic elements from Web pages of legitimate sites and compile them into an official-looking e-mail message. Creating a fake Web site is also easy. Hackers can obtain a URL that's similar to one used by a legitimate company by using a different country code or using .biz instead of .com. By copying and pasting a few graphics, the site looks legitimate, too. Preventing corporate identity theft is not really feasible. With current HTTP and HTML technologies, corporations have no way to lock down their branding elements, so hackers can easily misappropriate them. Consumers will remain at risk until there is universal implementation of technology that verifies a Web site's legitimacy. Companies can take steps to protect their customers and deal quickly with identity theft incidents, but no computer system can be completely risk-free. Several proactive measures can protect information systems from threats. These measures can be grouped into four deterrents, preventive countermeasures, corrective procedures and detection activities. Deterrents reduce the likelihood of deliberate attack. Both physical deterrents, such as limiting access to critical servers, and common deterrents, such as multi-level authentication, password protection, and biometric identification fall under this category. Preventive countermeasures shield vulnerabilities to render an attack unsuccessful or reduce its impact. Firewalls that prevent unauthorized access to a system and encryption that makes stolen data indecipherable are examples of preventive countermeasures. Corrective procedures reduce the effect of an attack. Data backups, disaster recovery plans, and the availability of redundant hardware devices all are examples of corrective procedures. Detection activities recognize attacks and trigger preventive countermeasures or corrective procedures. For example, antivirus software detects viruses entering a system and can be configured to perform corrective procedures such as removing the virus and quarantining infected files.

To help minimize risks the hardware and software for most corporate information systems are housed in data centres. A data centre is a specialized facility designed to hold and protect computer systems and data. It includes special security features and is designed to proactively reduce the risk of data loss that might occur as a result of a disaster. Physical security is critical to data centres. Most data centres limit physical access using password protection and fingerprint identification systems. Motion detectors, automated alarm systems and many other Metrics prevent unauthorized movement through the building. For maximum protection, some data centres are housed in former military bunkers, abandoned mines, or limestone caves to provide protection against many natural disasters and a supply of uninterrupted power from high-capacity, battery-operated uninterruptible power supplies and backup power generators to keep computers functioning during power outages. But disaster recovery plans are also critical to data security. It is a step-by-step plan that describes the methods used to secure data against disaster and sets guidelines for how an organization will recover lost data if and when a disaster occurs. It must deal not only with calamities but also must take into account day-to-day events that could potentially cause data loss.

Topic 10. Digital security

BASIC SECURITY

Security software is designed to protect computers from various forms of destructive software and unauthorized intrusions. Security software can be classified into various types: antivirus, antispyware, anti-spam, and firewalls. Each type focuses on a specific security threat.

Some techniques for safe computing include installing and activating security software on any digital device that is at risk, keeping software patches and operating system service packs up to date, not opening suspicious e-mail attachments, obtaining software only from reliable resources and always scanning it for malware, avoiding unsavoury Web sites and not clicking pop-up ads.

A security suite integrates several security modules to protect against the most common types of malware, unauthorized access, and spam. Security suites might include additional features such as Wi-Fi detection that warns of possible intrusions into your wireless network, and parental controls for monitoring and controlling children’s Internet usage. A security suite has both advantages and disadvantages. First, it costs less than purchasing standalone security modules. Second, a single interface for accessing all of the security suite’s features is much less complex than having to learn how to configure and run several different products. On the other hand, most security suites cannot run concurrently with standalone security products, and overlapping security coverage from two similar products can cause glitches.

Antivirus software is a type of utility software that looks for and eradicates viruses, Trojan horses, worms, and bots. Some antivirus software also scans for spyware, although several security software publishers offer spyware detection as a separate module. Antivirus software is available for all types of computers and data storage devices, including handhelds, USB flash drives, servers, PCs, and Macs.

Modern antivirus software attempts to identify malware by searching your computer’s files and memory for virus signatures. A virus signature is a section of program code, such as a unique series of instructions that can be used to identify a known malicious program, much as a fingerprint is used to identify an individual. Antivirus software scans for virus signatures in programs, data files, incoming and outgoing e-mail and attachments.

Two aspects of your antivirus software periodically need to be updated. First, the antivirus program itself might need a patch or an update to fix bugs or improve features. Second, the list of virus signatures must be updated to keep up with the latest malware developments. Virus signatures and other information that antivirus software uses to identify and eradicate malware are stored in one or more files usually referred to as virus definitions (or a virus database). If, during the scanning process, your virus protection software identifies a virus, worm, or Trojan horse in a file, it can try to remove the infection, put the file into quarantine, or simply delete the file. A quarantined file contains code that is suspected of being part of a virus. For your protection, most antivirus software encrypts the file’s contents and isolates it in a quarantine folder, so it can’t be inadvertently opened or accessed by a hacker.

Despite occasional misses, however, antivirus software and other security software modules are constantly weeding out malware that would otherwise infect your computer. It is essential to use security software, but also important to take additional precautions, such as making regular backups of your data.

MALWARE AND FRAUDS

The terms malicious software and malware refer to any computer program designed to surreptitiously enter secretly a computer, gain unauthorized access to data, or disrupt normal processing operations. Malware includes viruses, worms, Trojans, bots, and spyware. Malware is created and unleashed by individuals referred to as hackers, crackers, black hats, or cybercriminals. Some malware is released as a prank. In an increasing number of cases, malware is unleashed for monetary gain.

A computer virus is a set of program instructions that attaches itself to a file, reproduces itself, and spreads to other files. A common misconception is that viruses spread themselves from one computer to another. They don’t. Viruses can replicate themselves only on the host computer. A key characteristic of viruses is their ability to lurk in a computer for days or months, quietly replicating themselves. While this replication takes place, you might not even know that your computer has contracted a virus; therefore, it is easy to inadvertently spread infected files to other people’s computers. In addition to replicating itself, a virus usually delivers a payload which can corrupt files, destroy data, or otherwise disrupt computer operations. A trigger event, such as a specific date, can unleash some viruses. Viruses that deliver their payloads on a specific date are sometimes referred to as time bombs.

Some malware does a good job of cloaking itself, so victims are unaware of its presence. Cloaking techniques are great defence mechanisms because when victims aren’t aware of malware, they won’t take steps to eradicate it. Some hackers cloak their work using rootkits. The term rootkit refers to software tools used to conceal malware and backdoors that have been installed on a victim’s computer. Rootkits are usually distributed by Trojans.

Topic 11. Computer programming

PROGRAMMING PARADIGMS

Computer programs are developed by computer programmers or software engineers. Computer programming encompasses a broad set of activities that include planning, coding, testing, and documenting. Most programmers participate in all of these phases of program development, but focus on the coding process. Software engineers tend to focus on designing and testing activities.

The programming process begins with a problem statement that helps you clearly define the purpose of a computer program. In the context of programming, a problem statement defines certain elements that must be manipulated to achieve a result or goal. A good problem statement for a computer program has three characteristics:

* It specifies any assumptions that define the scope of the problem.
* It clearly specifies the known information.
* It specifies when the problem has been solved.

In a problem statement, an assumption is something you accept as true in order to proceed with program planning. The known information in a problem statement is the information that you supply to the computer to help it solve a problem. After identifying the known information, a programmer must specify how to determine when the problem has been solved. Usually this step means specifying the output you expect.

A problem statement provides a minimal amount of planning, which is sufficient for only the simplest programs. A typical commercial application requires far more extensive planning, which includes detailed program outlines, job assignments, and schedules. Methodologies can be classified as predictive or agile.

A predictive methodology requires extensive planning and documentation up front. It allows little room for adaptation and change. Predictive methodologies are preferred for large software development projects. In contrast to predictive methodologies, an agile methodology focuses on flexible development and specifications that evolve as a project progress. Programmers produce a subset of the entire project, show it to users, and then plan the next phase of development.

Programmers also approach problems in different ways. Whereas one programmer might focus on the steps required to complete a specific computation, another programmer might focus on the data that forms the basis for the computation. The phrase programming paradigm refers to a way of conceptualizing and structuring the tasks a computer performs. Today’s most popular programming paradigms are:

|  |  |  |
| --- | --- | --- |
| Paradigm | Languages | Description |
| Event- driven | Visual Basic, C# | Focuses on selecting user interface elements and defining event-handling routines that are triggered by  various mouse or keyboard activities |
| Procedural | BASIC, Ada,  Pascal, Fortran, COBOL | Emphasizes linear steps that provide the computer  with instructions on how to solve a problem or carry out a task |
| Object-  oriented | Smalltalk, C++,  Java, Scratch | Formulate programs as a series of objects and  methods that interact to perform a specific task |
| Declarative | Prolog | Focuses on the use of facts and rules to describe a  problem |

When planning is complete, programmers can begin coding, testing, and documenting. The process of coding a computer program depends on the programming language you use and the programming tools you select. Programming languages can be divided into two major categories: low-level languages (machine languages and assembly languages) and high-level languages (based on human languages).

Programmers can use a text editor, program editor, or VDE to code computer programs. A text editor is any word processor that can be used for basic text editing tasks, such as writing e-mail, creating documents, or coding computer programs. A program editor is a type of text editor specially designed for entering code for computer programs. A VDE (visual development environment) provides programmers with tools to build substantial sections of a program by pointing and clicking rather than typing lines of code. A typical VDE is based on a form design grid that a programmer manipulates to design the user interface for a program.

When a program doesn’t work correctly, it is usually the result of a syntax, logic, or runtime error. A syntax error occurs when an instruction does not follow the syntax rules, or grammar, of the programming language. Syntax errors are easy to make, but they are usually also easy to detect and correct. A runtime error occurs when a program runs. Some runtime errors result from instructions that the computer can’t execute. A logic error is a type of runtime error in the logic or design of a program, such as using the wrong formula. Logic errors can be caused by an inadequate definition of the problem or an incorrect formula for a calculation, and are usually more difficult to identify than syntax errors.

Programmers can locate errors in a program by reading through lines of code, much like a proof-reader. They can also use a tool called a debugger to step through a program and monitor the status of variables, input, and output.

Anyone who uses computers is familiar with program documentation in the form of user manuals and help files. Programmers also insert documentation called remarks into the program code. Remarks are identified by language-specific symbols, such as // in Java, or keywords, such as Rem in BASIC. Remarks are useful for programmers who want to understand how a program works before modifying it.

***OOP BASICS:***

The traditional approach to programming uses a procedural paradigm to conceptualize the solution to a problem as a sequence of steps and it is very efficient for number-crunching tasks. The declarative paradigm describes aspects of a problem that lead to a solution and help to solve problems for non-numeric data, including words and concepts. The object-oriented paradigm is based on the idea that the solution for a problem can be visualized in terms of objects that interact with each other. It is efficient for problems that involve real-world objects.

Objects and classes. In the context of OO paradigm, an object is a unit of data that represents an abstract or a real-world entity, such as a person, place, or thing. For example, an object can represent a $10.99 small pepperoni pizza. Another one can represent a pizza delivery guy named Jack Flash. Yet another object can be a customer living at 22 Pointe Rd.

The real world contains lots of pizzas, customers, and delivery guys. These objects can be defined in a general way by using classes. Whereas an object is a single instance of an entity, a class is a template for a group of objects with similar characteristics. For example, a Pizza class defines a group of gooey Italian snacks that are made in a variety of sizes, crafted into rectangular or round shapes, and sold for various prices. A class can produce any number of unique objects.

When taking the object-oriented approach to a problem, one of the first steps is to identify the objects that pertain to a solution. As you might expect, the solution to the pizza problem requires some pizza objects. Certain characteristics of pizzas provide information necessary to solve the problem. This information – the price, size, and shape of a pizza – provides the structure for the Pizza class. A class is defined by attributes and methods. A class attribute defines the characteristics of a set of objects.

Each class attribute typically has a name, scope and data type. One class attribute of the Pizza class might be named «pizzaPrice». Its scope can be defined as public or private. A public attribute is available for use by any routine in the program. A private attribute can be accessed only from the routine in which it is defined. The pizzaPrice attribute’s data type can be defined as «double», which means that it can be any decimal number. OO programmers often use UML (Unified Modelling Language) diagrams to plan the classes for a program. Although a programmer completes the overall program plan before coding, jump ahead to take a quick look at the Java code for the attributes in the Pizza class. The first line of code defines the name of the class. Each subsequent line defines the scope, data type, and name of an attribute. The curly brackets simply define the start and end of the class.

Inheritance. The object-oriented paradigm endows classes with quite a bit of flexibility. For the pizza program, objects and classes make it easy to compare round pizzas to rectangular pizzas rather than just to square pizzas.

Suppose you want to compare a 10-inch round pizza to a rectangular pizza that has a length of 11 inches and a width of 8 inches. The Pizza class holds only one measurement for each ***pizza: pizzaSize***. This single attribute won't work for rectangular pizzas, which might have a different length and width. Should you modify the class definition to add attributes for ***pizzaLength*** and ***pizzaWidth***? No, because these attributes are necessary only for rectangular pizzas, not for round pizzas. An OO feature called «inheritance» provides flexibility to deal with objects’ unique characteristics.

In object-oriented jargon, inheritance refers to passing certain characteristics from one class to other classes. For example, to solve the pizza problem, a programmer might decide to add a ***RoundPizza*** class and a ***RectanglePizza*** class. These two new classes can inherit attributes from the Pizza class, such as pizzaShape and pizzaPrice. You can then add specialized characteristics to the new classes. The ***RectanglePizza*** class can have attributes for length and width, and the ***RoundPizza*** class can have an attribute for diameter.

The process of producing new classes with inherited attributes creates a superclass and subclasses. A superclass, such as Pizza, is any class from which attributes can be inherited. A subclass (or «derived class»), such as RoundPizza or RectanglePizza, is any class that inherits attributes from a superclass. The set of super-classes and subclasses that are related to each other is referred to as a class hierarchy. Java uses the extends command to link a subclass to a superclass. The statement class RectanglePizza extends Pizza means «create a class called RectanglePizza that’s derived from the superclass called Pizza».

Methods and messages. An OO program can use objects in a variety of ways. A basic way to use objects is to manipulate them with methods. A method is a segment of code that defines an action. The names of methods usually end in a set of parentheses, such as ***compare()*** or ***getArea()***.

A method can perform a variety of tasks, such as collecting input, performing calculations, making comparisons, executing decisions, and producing output. For example, the pizza program can use a method named ***compare()*** to compare the square-inch prices of two pizzas and display a message indicating the best pizza.

A method begins with a line that names the method and can include a description of its scope and data type. The scope – public or private – specifies which parts of the program can access the method. The data type specifies the kind of data, if any, that the method produces. The initial line of code is followed by one or more lines that specify the calculation, comparison, or routine that the method performs.

A method is activated by a message, which is included as a line of program code, sometimes referred to as a «call». In the object-oriented world, objects often interact to solve a problem by sending and receiving messages. For example, a pizza object might receive a message asking for the pizza’s area or price per square inch.

Polymorphism, sometimes called «overloading», is the ability to redefine a method in a subclass. It allows programmers to create a single, generic name for a procedure that behaves in unique ways for different classes. Polymorphism provides OO programs with easy extensibility and can help simplify program code.

AI (artificial intelligence)

The term “artificial intelligence” dates back to 1956 and belongs to a Stanford researcher John McCarthy, who coined the term and defined the key mission of AI as a sub-field of computer science.

Basically, artificial intelligence (AI) is the ability of a machine or a computer program to think and learn. The concept of AI is based on the idea of building machines capable of thinking, acting, and learning like humans.

A more nuanced definition is that artificial intelligence is an interdisciplinary concept that studies the possibility of creating machines capable of interacting with their environment and acting upon the received data in the manner considered intelligent. While some people falsely consider AI a technology, the more accurate approach would be seeing it as a broad concept in which machines are able to deal with tasks in a way we would call intelligent or smart.

There are certain things a machine/computer program must be capable of to be considered AI.

First, it should be able to mimic human thought process and behaviour. Second, it should act in a human-like way – intelligent, rational, and ethical.

AI is not the same as machine learning. Although the two terms are often used interchangeably, they are different. Artificial intelligence is a broader concept, while machine learning is the most common application of AI. We should understand machine learning as a current application of AI that is focused on development of computer programs that can access data and learn from it automatically, without human assistance or intervention. The entire machine learning concept is based on the assumption that we should give machines access to information and let them learn from it themselves.

Artificial intelligence, in its turn, is a bunch of technologies that include machine learning and some other technologies like natural language processing, inference algorithms, neural networks, etc.

Many people associate AI with the distant future. They incorrectly believe that despite all the buzz around artificial intelligence, the technology is not likely to become a part of their lives anytime soon. Little do they know how many aspects of their lives are already affected by AI.

There are intelligent gadgets able to recognize our speech (read: “understand what we want or need”), analyse the information they have access to, and provide an answer or solution. What is remarkable (and a little scary) about such assistants is that they continuously learn about their users until the point at which they are able to accurately anticipate users’ needs.

Spotify, Pandora, and Apple Music are some other touching points between AI and you. These services are capable of recommending music based on your interests. These apps monitor the choices you make, insert them into a learning algorithm, and suggest music you are most likely to enjoy. This particular use of AI is probably one of the simplest among all, but it does a good job helping us discover new songs and artists.

AI is making headway in areas you might least expect it. The current state of artificial intelligence already allows for some basic robot writing. It might be not yet ready to compose in-depth articles or creative stories, but does a pretty good job writing short and simple articles like sport recaps and financial summaries.

Other examples of artificial intelligence in use today include smart home devices like Google’s NEST, self-driving cars like those produced by Tesla, and online games like Alien: Isolation.

Some people claim that AI is still in its infancy. Others assure us that we are only a few years away from AI gaining control over humanity. The truth, however, lies somewhere in between. According to the most trustworthy forecasts out there, AI will outsmart humans at virtually everything in the following 45 years.

Obviously, this won’t happen overnight. Industries will be falling under AI’s spell one-by-one. Experts predict that within the next decade AI will outperform humans in relatively simple tasks such as translating languages, writing school essays, and driving trucks. More complicated tasks like writing a bestselling book or working as a surgeon, however, will take machines much more time to learn. AI is expected to master these two skills by 2049 and 2053 accordingly.

SECURE PROGRAMMING

Hackers, crackers, cybercriminals, or black hats – no matter what you call them; their goal is to gain unauthorized access to information. The first line of defence in cyber security is computer programmers who create the applications, operating systems, and utilities that you use every day. Viruses, worms, bots, malicious Web scripts, and other exploits creep into computer systems through security holes, but why do these holes exist? Some of the most common software security defects include buffer overflows and verbose error messages.

A buffer overflow is a condition in which data in memory exceeds its expected boundaries and flows into memory areas intended for use by other data. Programmers can prevent buffer overflows by controlling pointers, checking input for suspicious characters, and placing strict boundaries on the values that can be stored in variables. A technique called address space randomization arranges key data areas in locations that are difficult for hackers to predict and target.

Good programmers try to anticipate how a program might fail and include code to handle the failure. Often, the result is an error message displayed to the user. When software is in developmental and testing phases, error messages can help programmers locate the source of errors. If those verbose error messages remain when the software ships, they can present attackers with information about the directory location of programs or files, the structure of a database, or the layout of the program in memory. Some of the most common examples of verbose error messages appear during unsuccessful attempts to log in or access files.

Software security begins when program specifications are formulated. Techniques such as formal methods, threat modelling, attack trees, and defensive programming help programmers remain aware of security throughout the software development life cycle.

Formal methods help programmers apply logical and mathematical models to software design, coding, testing, and verification. Formal methods, however, add to the cost and time of software development, so they tend to be used only for life-critical systems, such as air traffic control and nuclear reactor control systems.

Threat modelling is a technique that can be used to identify potential vulnerabilities by listing the key assets of an application, categorizing the threats to each asset, and developing threat mitigation strategies that can be implemented during coding. Threats can be categorized using a model like **STRIDE**:

**S**poofing: Pretending to be someone else

**T**ampering: Changing, adding, or deleting data

**R**epudiation: Covering tracks to make attacks difficult to trace

**I**nformation disclosure: Gaining unauthorized access to information

**D**enial of service: Making a system unavailable to legitimate users

**E**levation of privilege: Modifying user rights to gain access to data.

Some threats are more likely to occur than others, and some threats have the potential to cause more damage than others. Software designers can rank threats using the **DREAD** categories:

**D**amage: How much damage can a particular attack cause?

**R**eproduce: Is this attack easy to reproduce?

**E**xploit: How much skill is needed to launch the attack?

**A**ffected: How many users would be affected by an attack?

**D**iscovered: How likely is it that this attack would be discovered?

Defensive programming is an approach to software development in which programmers anticipate what might go wrong as their programs run, and take steps to smoothly handle those situations. Techniques associated with defensive programming include source code walkthroughs that can identify security holes; simplification of complex sections of code; filtering input. Signed code is a software program that identifies its source and carries a digital certificate. It ensures that the software will not run if even a single byte of the source code is changed by a virus or any other factor.

When software bugs are discovered, the programmer’s remaining line of defence is to produce a bug fix, or patch.

Computer users have no control over software at the code level, but there are a few steps they can take to avoid security problems:

* Select applications from software publishers with a good security track record.
* Read reviews of products before you download them and avoid software that doesn’t receive good reviews.
* Watch for patches and apply them.
* Consider using open source software, which has been extensively reviewed by the programming community.
* And yes, keep your firewall and antivirus software deployed and up to date.

Topic 12. Database Basics

BIG DATA

A database is a collection of information. Today, most databases are stored as computer files. Databases can incorporate several lists. For example, the database for an e-commerce site, such as Amazon.com, includes inventory lists and customer lists.

The tasks associated with creating, maintaining, and accessing the information in databases are referred to as data management, file management, or database management. Databases can be used in a variety of ways, from a simple tool for collecting and tracking data, to a comprehensive source for making decisions and predicting future trends.

Collect and store data. A database is a collection of data, but that collection grows as additional data is obtained. Data can be collected and entered manually or electronically. Information can also be removed from a database when it is no longer needed.

Update data. One of the primary database management activities is keeping data up to date by entering current addresses, inventory quantities, and so on. As with collecting data, updates can be made manually or electronically.

Organize and output data. The data in a typical database is stored in no particular order. New data is appended to the end of the file. To make data into a more suitable report, it can be organized in different ways. It can be alphabetized, placed in numeric order, grouped and subtotalled. Database output is easy to organize and reorganize without actually rearranging the physical data on the disk.

Distribute data. Databases, combined with mail merge and other computerized technologies, offer efficient ways to distribute information customers, employees, government agencies, and other companies.

Find data. Databases make it easy to locate information. A pharmacist can check a pharmaceutical database for drug interaction before filling a prescription. A computer technician can check a manufacture’s database to find the part number for replacing your computer’s fried hard drive.

Analyse data. Databases include certain facts as raw data, such as names, addresses, bank balances, prices, and inventory quantities. Analysing this data can produce information that is not readily apparent from simply looking at raw data.

What is data mining? Data mining refers to computer algorithms that analyse information to discover previously unknown and potentially useful information, including relationships and patterns. The data accessed by data mining and analysis techniques is often stored in a data warehouse, which is a storage for data from more than one database. Data from operational databases is transferred to a data warehouse where it can be combined with data from other databases to enhance the data set.

Predictive analytics refers to a branch of data mining that analyses current and historical data to predict future trends. It makes use of statistical algorithms, neural networks and optimization research to discover patterns in data. For example, researchers might use it to predict customer behaviour, unmask terrorists, forecast storm paths, etc. Like data mining, predictive analytics processes data autonomously, rather than under the direction of an operator who specifies what to look for.

OLAP (online analytical processing) is a data analysis technique that allows decision makers to quickly get answers to complex queries that encompass multiple factors, such as locations, revenue, time periods, and employee status. Unlike data mining and predictive analytics, OLAP is an interactive process that allows decision makers to devise unique queries, enter them, and get an immediate response.

Big data refers to huge collections of data that are difficult to process, analyse, and manage using conventional database tools. An example is the one million transactions generated by Walmart sales registers every hour, which are stored in databases measured in petabytes, not gigabytes or terabytes.

The simplest model for storing data is a flat file that consists of a single, two- dimensional table of data elements. Each row in the table is a record, and each column of the table is a field. Computer databases display records as rows in a table or as forms.

A field contains the smallest unit of meaningful information, so you might call it the basic building block for a structured file or database. Each field has a unique field name that describes its contents. For example, in an iTunes playlist, the field called Name holds the name of a song, the Time field holds the song length, the Artist field holds the name of the performer, the Album field holds the name of the album and the Genre field holds the type of the song.

In the world of databases, a record refers to a collection of data fields. Each record stores data about one entity – a person, place, thing, or event. For example, a data record stored in an iTunes playlist contains fields of data pertaining to a digital music track.

Flat files are the foundation for simple databases, such as an e-mail address book, an iTunes playlist, or the addresses for a mail merge. Spreadsheets are also modelled on flat files. With a flat file, you can search for, update, group and organize. Each record in a flat file, however, is an independent entity and no relationships can be established between records.

The term DBMS (database management system) refers to software that is designed to manage data stored in a database. Each DBMS specializes in one database model, but some DBMS software offers versatility by dealing with a variety of models and data.

The Web allows access to many databases. When you shop at one online store, for example, the photos, descriptions, and prices you see are pulled from the merchant’s database and displayed as Web pages. More direct database access is offered by online public access catalogues. A database also provides the foundation for online access to course registration systems, real estate listings, movie reviews, flight schedules, and other information.

The Web provides both opportunities and challenges for accessing the information in a database. Obviously, with its global reach, the Web provides an opportunity for many people to gain access to data from multiple locations.

A technique called static Web publishing is a simple way to display the data in a database by converting a database report into an HTML document, which can be displayed as a web page by a browser. Static publishing provides extremely limited access to a database because it creates a Web page that displays a snapshot of your data at the time the report was generated. The advantages include security and simplicity. Your data remains secure because you have not provided direct access to your database, so unauthorized users cannot change your data.

In several situations, such as making e-commerce purchase or registering for a social networking site, it is important for people to use a browser to add or update records in a database.

So, many techniques exist for storing, accessing and displaying the data from databases. Individuals can use simple tools to create personal databases, such as address books. Corporate database managers, however, need to be familiar with more complex tools used to distribute data over networks and the Web. Sometimes more than one database management tool has the potential to work for a specific application.

DATABASE SECURITY

Databases are vulnerable to physical theft, hacking, and unauthorized access. A disk or tape containing a backup or an archive could be stolen. A laptop computer containing a database used by a field representative or teleworker can go missing. Hackers can gain unauthorized access to a database over the Internet or an unsecured wireless connection.

The qualities that make databases efficient also make them vulnerable. Data stored in digital format is easy to copy, back up, store, and transmit. Although it would be impractical to steal millions of paper records from filing cabinets, to steal a digital database, a criminal simply has to pocket a small backup drive or make a copy of the original database.

When a database is illicitly copied, it is stolen but not missing, as it would be if a crook made off with the folders in a filing cabinet. The theft might not be discovered for days or weeks, if ever, and affected individuals are never warned that their identities are at risk.

Privacy. You expect personal information to remain confidential. However, when your data is in a computer database, there is a risk that it can be viewed by unauthorized individuals or distributed without your permission. A preferred customer card at your favourite supermarket could be used to collect data about the groceries you purchase.

Accuracy. After accepting the fact that personal data is stored in countless databases, it would be comforting to know that the data is accurate. However, data entry errors, update errors, and hacking all add to doubt about the veracity of database data.

Security. Criminals have become sophisticated in the use of bots, key-loggers, and redirection to access data stored on personal computers and in corporate databases. The data stored in a single database is often sufficient to provide a criminal with enough information to access your bank account or use your credit card. New trends in data aggregation and analysis make it possible to assemble a detailed picture of an individual’s life with enough critical ID numbers and PINs to steal an entire identity and then run up debt, acquire a criminal record, and put a real person’s life in shambles.

Today’s computers are under assault from hackers and natural disasters. Although no computer system can be 100 % secure, system administrators can take steps to secure computer systems and the databases they contain. Security measures include encryption, access controls, data security policies, and intrusion monitoring.

Database data that’s transmitted over the Web can be encrypted using encryption technologies such as SSL. When that data arrives at the database, it is unencrypted and usually stored in plaintext. Encrypted databases are less efficient than unencrypted databases because all or part of the database has to be decrypted for the query to locate information.

Most operational databases are not encrypted while being used, but the data they contain can be encrypted before it is archived. Thieves who gain access to a database archive cannot make sense of the data if it is encrypted.

An access control limits access to systems, such as computer databases. Access controls can block unauthorized users and limit activities of authorized users. IT professionals sometimes classify access controls as identification and authentication, authorization, and accountability.

Identification and authentication determine who can access a database and the information it contains. Authorization defines what an authenticated user can do. Accountability tracks what a user did.

Basic security restricts physical access and network access to the computer that hosts the database. Physical access can be limited to authorized personnel by housing the computer in a locked data centre. Online access can be limited by firewalls and passwords. System administrators should be sure to change all default administrator passwords before opening the database to internal and external users. Security experts also recommend separating the server that hosts the database from the server that hosts publicly accessible services, such as Web pages.

A good set of policies decreases the risk of unauthorized access within the workplace, minimizes the chance of confidential data escaping from the workplace, and helps improve data entry accuracy.

Policies for retiring old equipment are also essential, and not just for computers. Modern office copier machines contain a hard disk, which stores images of every page that is copied. Removing and destroying storage devices from all discarded devices is a requirement for data security.

A database audit is a procedure that monitors and records user activity within a database. In some instances, auditing can identify intruders before they can compromise a system. If an intruder breaches database security, an audit can help to identify the damage and correct it.

Tracking who makes changes in a database helps an organization maintain accountability, trace the source of errors, and make corrections. If a database has been compromised by a hacker, an audit report can be used to check recent changes to the database to make sure they are legitimate.

If abnormal usage patterns become evident, database auditing tools can be configured to check specific types of database activity. For example, if a system administrator suspects that data is being surreptitiously deleted or changed, an audit can be set up to record any successful or unsuccessful deletions from tables in the database.

In the meantime, what to do? You can’t protect your personal data once you’ve released it, so the key to minimizing your risk is to be vigilant about the information you divulge. So, you should: know when data is being collected; find out how data is being used; find out what data is retained; supply only the data that is required; protect your passwords; not to trade your privacy; use antivirus software; not to reply to spam.