E-JAGRATHA
INTERNET EMPOWERMENT PROGRAM

TATA CONSULTANCY SERVICES LTD.

Contents

TCS Session

1. Welcome

A session with mainly an overview and an interactive session to understand how the audience are using computers and internet and how much they know about it.

2. E – World

2.1. Introduction

2.2. E-Governance

2.2.1.Government certificates
2.2.2.Railway/KSRTC Ticket Booking
2.2.3.Adhaar
2.2.4.Voters ID
2.2.5.Passport
2.2.6.Online Applications

2.3. Facilities available at Akshaya Centers

2.4. Education Support Sites

2.5. E-commerce

2.5.1.Common e-commerce sites and uses
2.5.2.Dos and Don'ts in E-commerce

2.6. Online banking

2.7. DigiLocker

3. How to use Internet Safely

3.1. Search Sites

3.1.1.Common search sites
3.1.2.   Easy searching tips
3.1.3.   Safe search

3.2. Simple online security tips

3.3. Wiki

3.4. YouTube

3.5. Blocking a website in local network/machine

3.6. E-mail account setup

3.7. Selection of Passwords

3.8. Secure downloads and copyrights

3.8.1.Impact of unsecure download
3.8.2.Copyright

4. Gaming & Social Media

    4.1. Gaming

        4.1.1.Advantages of gaming

        4.1.2.Disadvantages of gaming

    4.2. Social networking sites

        4.2.1.   Common networking sites

        4.2.2.   Secure usage of social networking Apps

5. Mobile- Safe Practices

    5.1. Healthy usage

        5.1.1.Posture

        5.1.2.Duration

        5.1.3.Earphones

    5.2. Apps and uses

        5.2.1.Overview of general Apps

6. How Internet impacts your Body and Mind

    6.1. Psychological Impact of long time usage

        6.1.1.Internet Addiction

            6.1.1.1.   Cyber relationship addiction

            6.1.1.2.   Excess Gaming Addiction

            6.1.1.3.   Cybersex Addiction

        6.1.2.Depression

    6.2. Physical Impact of long time usage

        6.2.1.Joint Pains

        6.2.2.Posture Issues

7. Cyber Threats and Laws

    7.1. Password threats and misuses

        7.1.1.Password leaks

        7.1.2.Misuses of password sharing

    7.2. Hacking

        7.2.1.What is hacking

        7.2.2.How to keep your account safe

    7.3. Malwares, Spyware, Phishing, Spamming

        7.3.1.Common hoax mails

1 E – World

Slide 1

First we will see how internet is affecting our day to day life.

We are moving towards the concept of a totally digitized society. Science and technology are evolving rapidly and bringing unexpected and exciting changes in and around us. Pervasive computing - the spread of digital information throughout the society - is also bringing rapid changes across the globe and people are getting used to accessing sensitive information stored in a digitized manner anytime and anywhere with necessary security certifications.

The explosion of these technologies and methodologies has created an abundance of new, state-of-the-art literature related to all the aspects of this expanding discipline, allowing researchers, citizens, and government officials to learn about the latest discoveries of information technology.

Slide 2

1.1.1 How the Internet Has Changed Everyday Life

Today internet has become an encyclopedia which can provide us information on, literally, anything.

The Internet has turned our existence upside down. It has revolutionized communications, to the extent that it is now our preferred medium of everyday communication.   There are different types of communication modes in internet, like email, instant messaging etc.

Along with that it has touched and affected all areas in our life, like agriculture, medical and healthcare, education etc

-------------------------------------- SUPPORTING DATA --

1.1.2 Internet and Communication

1.1.2.1 Types of Internet Communication

E-mail - Short for electronic mail, e-mail is the transmission of messages over communications networks.

Instant Messaging-An IM communications service enables you to create a kind of private chat room with another individual in order to communicate in real-time over the Internet.

Videoconferencing is a conference between two or more participants at different sites by using computer networks to transmit audio and video data. Each participant has a video camera, microphone and speakers connected on his or her computer.

World Wide Web - The World Wide Web is a service that the Internet provides, in which Web servers send information as formatted "pages" of text, images and other media.

VoIP and skype calls - The Voice over Internet Protocol uses the Internet to make phone calls. To make a VOIP call, you need a computer, smartphone or special digital handset that converts voice audio into digital data signals. Services such as Microsoft's Skype and Apple's FaceTime take the VOIP concept a step further by adding simultaneous live video

Streaming video- A wide range of content providers, including Hulu, Netflix and Amazon, make video content available through the Internet. In some instances, you can download movies to your hard drive, making them part of your permanent collection.

Social media -Social media have changed our personal space, altering the way we interact with our loved ones, our friends. They have forced us to rethink even basic daily processes like studying and shopping.

--- SUPPORTING DATA ---

1.1.3   Internet of Things Examples – [Slide 3]

 A development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data. For e.g. heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

--------------------------------- SUPPORTING DATA --

E Learning or Online Learning

- In an on-line multimedia learning environment:
    - teaching & learning is 'one-to-one' (individual)
    - more interactivity (in normal classroom, it varies with the class size)
    - learner-centered
    - Learner monitoring & grading system

Benefits

- Convenient, self-service (mix and match),on-demand (anytime, anywhere)
- private learning, self-paced, Flexibility: (modular package)
- Cost-effective, Virtual learning environment, Share lessons among schools
- Reduce material cost, Reduce travel/accommodation

Using Multimedia - visual data has a greater impact on learning and memorizing than plain text. Therefore, images, graphics, animation, pictures, slides, documentaries, etc., have a greater appeal than a plain textbook. Using multimedia and Internet provides an opportunity for children to gain knowledge about a particular subject in depth.

Easy Contact - Students can contact other students or their teachers via the e-mail if they have queries about any information. Sharing of information, discussions on a particular subject, etc., can be easily carried out using the Internet.

School/College Projects Using the Internet can be very useful for completing projects in schools and colleges.

Encyclopedia- Sometimes, an encyclopedia may not always be available to students and they may have difficulty in gaining access to the books in the library. In that case, the encyclopedia of various subjects available on the Internet can be helpful.

Easy Education System- You can now view your prospective educational institute, look up courses, enroll for online courses, take classes, research, see your results, and even look for job prospects on the Internet. Therefore, the scope of Internet in education is very wide and equal to all.

1.1.4 The Internet and Consumer Trends

1.1.4.1 Internet Banking

Internet Banking refers to the banking services provided by the banks over the internet. Some of these services include paying of bills, funds transfer, viewing account statement, etc. Banks also deliver their latest products and services over the internet.

Online bill paying services Offer a range of benefits, but the most important is that it saves one of your most valuable assets time. Online bill paying services were created to save individuals and businesses time and resources in the bill paying process.

Online booking

If you have a credit card handy and access to the Internet, you can finalize your travel plans within minutes. Online reservations to save both time and money, one advantage of booking a hotel, flight or car rental online is the convenience.

Online Shopping

Online shopping has become a popular shopping method ever since the internet has declared a takeover. Save Time, Comparison of Prices ,24/7 Availability, Easy to Search products You Want to Buy ,Save Fuel ,Hate Waiting in Lines

Advertising on the Internet

Internet advertising is ideal for businesses with a national or international target market and large-scale distribution capabilities. Cost-efficient, more reach to people

1.1.5 The Future of Social Communications, Innovation, Mobile Technologies, and Total Connectivity in Our Lives

The **mobile Web** refers to the use of browser-based Internet services from handheld mobile devices, such as smart phones or feature phones, through a mobile or other wireless network.

-------------------------------- SUPPORTING DATA --

Slide 4

The major areas that we will be discussing in this class are

- E-Governance
- E-Commerce
- E-Banking

Slide 5

E-Governance

Electronic governance or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework. Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are government, citizens and businesses/interest groups. In e-governance there are no distinct boundaries.

Generally four basic models are available – government-to-citizen (customer), government-to-employees, government-to-government and government-to-business.

Slide **6**

E-Governance Services include

- Getting Government Certificates
- Aadhaar Card Registration and Download
- Voter ID card Registration
- Passport Registration
- Akshaya Centers

Government certificates

Now we will talk about some of the major government sites in India.

Slide 7 - 27

First is Birth/Death/Marriage Registrations and Certificate Download -– For that we need to access http://cr.lsgkerala.gov.in/

In the site, Click on the Certificate Search

In the form coming up, we need to select the District, Local Body type, Local Body and Submit. Then select the year of Birth/Death/Marriage Registrations

Enter the mandatory details and submit for getting the certificates

Show Sample Certificate downloaded: Birth Certificate

Show Sample Certificate downloaded: Marriage certificate

1.1.6 Aadhaar

Do all of you have Aadhaar card? Do you know we can apply for Aadhaar card online? For that we need to register at - https://uidai.gov.in/beta/

We have to select the "Enrolment Request (Online)" option in the home page

The "Terms and Condition" for Aadhaar registration will be displayed; after reading the details enter the verification image & state and click on Verify and Proceed Option.

Enter the correct details in the Aadhaar form and Submit for further processing by the authorities
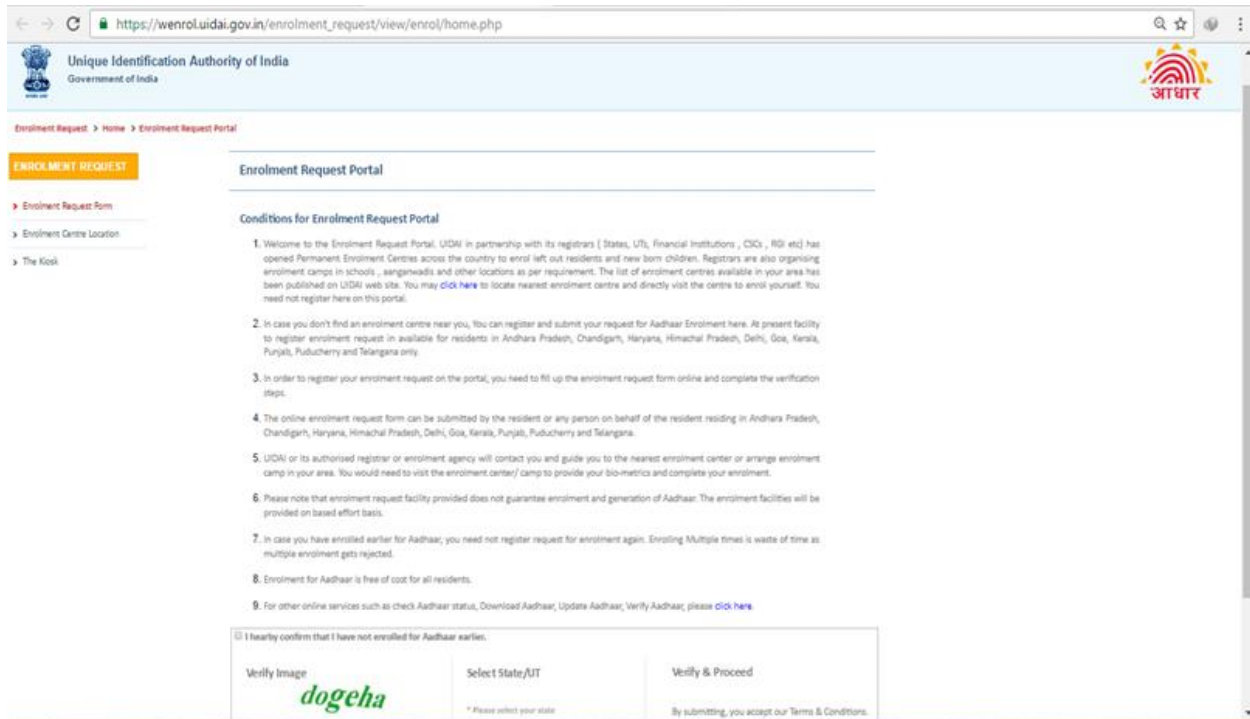
Show Sample Aadhaar downloaded (in slide)

1.1.7 Voters ID

You all know that when you turn 18, you can cast your vote. For that first you need to get a voter's ID. For the ease of the process, government has made it possible to apply for voter's id online. For that we need to go to http://www.nvsp.in/

If you are registering for the first time, for a new user click on "Apply online for registration of new voter"

For overseas voter select option "Apply online for registration of overseas voter"
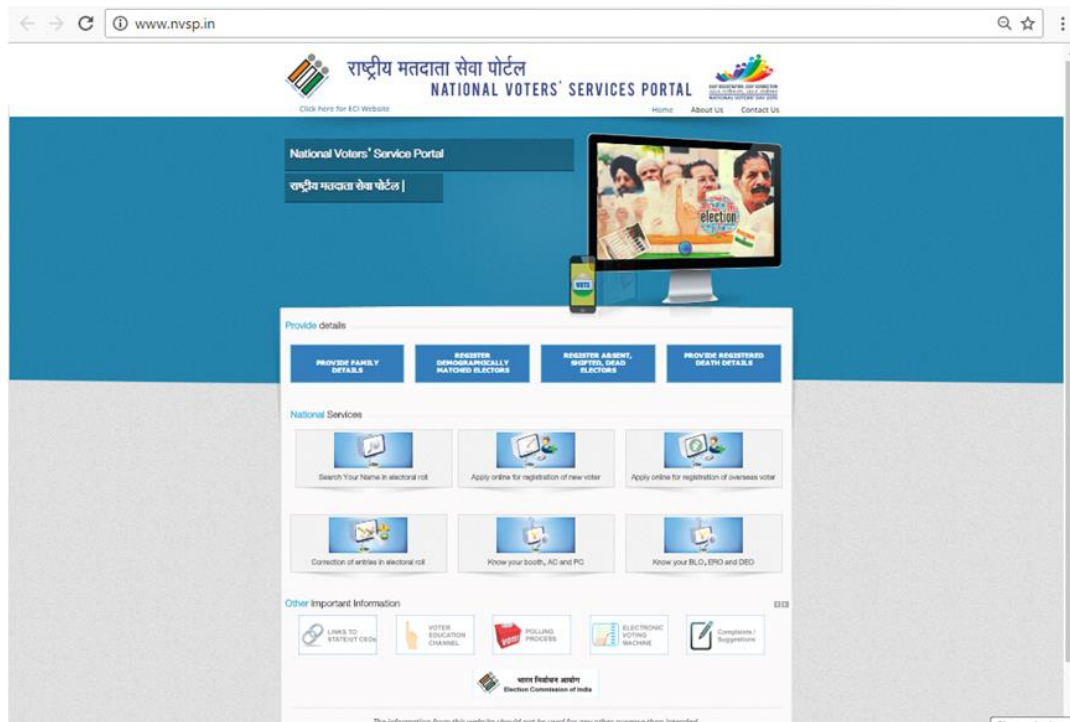
When the required option is selected the below displayed screen containing the registration form is displayed. After providing the details submit the online application for further processing by the authorities.

1.1.8　Passport

As you all know for travelling abroad we need passport. Online registration for passport can be made at this site-

http://www.passportindia.gov.in/AppOnlineProject/welcomeLink
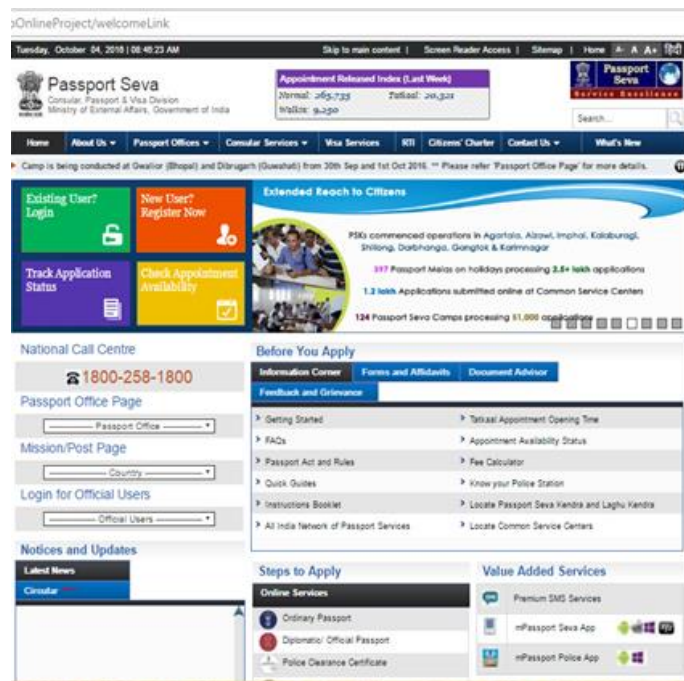
For Online registration of an ordinary passport follow the below steps:

Online Form Submission

Step 1	Register through the Passport Seva Online Portal. (Click on *"Register Now"* ![icon] link on the Home Page).
Step 2	Login to the Passport Seva Online Portal with the registered Login Id.
Step 3	Click *"Apply for Fresh Passport/Re-issue of Passport"* link. If you ever held a passport in the past, no matter how much long back or at what age, you should choose the Re-Issue category only.
Step 4	Fill in the required details in the form and submit.
Step 5	Click the *"Pay and Schedule Appointment"* link on the "View Saved/Submitted Applications" screen to schedule an appointment. **Online Payment** has been made mandatory for booking appointments at all Passport Seva Kendras/Passport Offices. Online Payment can be made using any one of the following modes: ○ Credit/Debit Card (MasterCard and Visa) ○ Internet Banking (State Bank of India (SBI) and Associate Banks Only) ○ SBI Bank Challan
Step 6	Click the *"Print Application Receipt"* link to print the application receipt containing Application Reference Number (ARN)/Appointment Number.
Step 7	Visit the Passport Seva Kendra (PSK)/Regional Passport Office (RPO) where appointment has been booked, along with original documents.

1.1.9 Other online applications

Some of the other online Applications available are

- IRCTC Railway/KURTC Bus Ticket Booking
- Electricity Bill Payment
- Kerala Authority Water Bill Payment
- Booking Bharat/ Indane Gas
- BSNL Landline/Mobile Bill payment and recharge
- MG University Course Registration
- Cee Kerala/Kerala Results
- Online PSC Registration
- Kerala E-District/HSCAP/DCE Scholarship

1.1.10 Booking railway tickets

https://www.irctc.co.in

How often do you travel in train and how do you/or your parents book tickets? If you have Internet Connection you can book tickets sitting at your home from this site. The other requirements include Debit Card, Credit Card or an Internet Banking Account

New users can Sign Up using the sign up link and enter the required details. Then login using the User Id and Password to book tickets.

1.1.11 Booking bus tickets

kurtconline.com/

Have you ever heard of booking KSRTC bus tickets? We can book KSRTC bus using this site. New users can Register using the Register link and enter the required details. Then they can login using the User Id and Password to book tickets.

Requirements: Debit Card/Credit Card/Internet Banking Account

1.1.12 Electricity Bill Payment

http://kseb.in

You don't require to travel to the Electricity Office and wait in queue anymore to pay your electricity bills. You can just visit this website for

- Application for new electricity connection
- Online bill generation/payment

Requirements for Bill Payment: Debit Card/Credit Card/Internet Banking Account
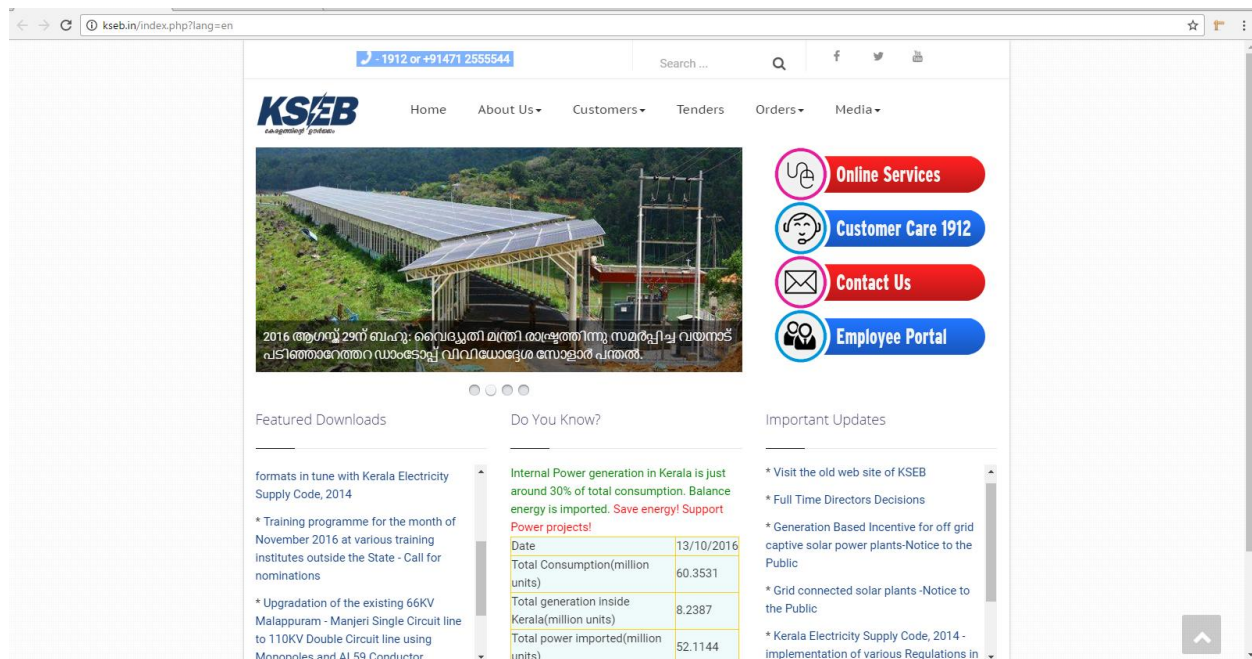
1.1.13 Kerala Water Authority Bill Payment

http://epay.kwa.kerala.gov.in/

How many of you have Kerala Water Authority Connection at home? How many of you are planning to apply for new Water Connection?

Through this website we can

- Request for new water connection
- Make payment for existing connection

Requirements for Bill Payment: Debit Card/Credit Card/Internet Banking Account
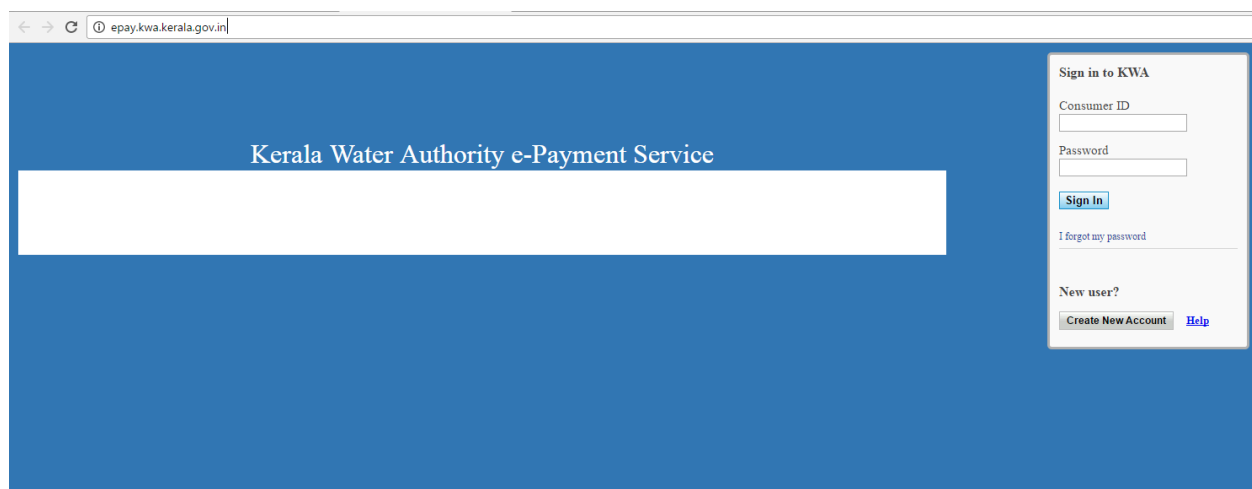
1.1.14 Booking Gas

Today we have gas connections in almost all houses. How many of you use Bharat Gas at home?

And how many of you use Indane at home?

1.1.14.1 Bharat Gas

www.ebharatgas.com

This website provides the facility for booking Bharatgas 'On Line' along with information about the product, its uses, safety and conservation tips. The website also provides a feedback system enabling the consumers to directly speak to the Organization

1.1.14.2 Indane Gas

www.indane.co.in

This website offers you the flexibility and convenience of booking your refill cylinder at any time, from anywhere, when you are on the move, on a holiday or at home. Facilities include Order refill, new connection, and double bottle connection, change your distributor, rate your distributor, and surrender your connection, preferred time delivery.

1.1.15 BSNL

http:// portal.bsnl.in

How many of you have mobiles at home? How are the recharges done in your home?

You need not visit the recharge shops anymore when this can be done at home. And the best point about this is the recharge can be done at any time 12 PM or 12 AM

This website allows you to book a New Service/Broadband Connection, Pay Your Landline/Mobile bills, Change Broadband Password, Register a Complaint, Recharge your mobile and View the Bills.

Online sites for recharge and bill payments are available for other providers like Airtel, DoCoMo Vodafone etc.

1.1.16 MG University

www.mgu.ac.in

How many of you have sisters/brothers studying at MG University? How do they check their results?

This website contains the results published on various courses, the course details, university authorities contact details, and provision to register for new admission/re-admission or examination.

1.1.17 Cee Kerala

http://cee-kerala.org

How many of you have plans to become Engineers and Doctors?

This is the official site of Commissioner for Entrance Examinations, which conduct about 13 entrance examinations and publish Results and corresponding allotments on basis of the ranks.

1.1.18 Kerala results

http:// keralaresults.nic.in

Kerala State Board/University results are published in this website. You would have or you would be visiting this site in future for seeing your examination results

1.1.19 Online PSC Registration

http://www.keralapsc.gov.in

The Public Service examination applications for various positions, results, and latest updates are available in this website.

1.1.20 Kerala E-District

http://edistrict.kerala.gov.in

This site brings several government services to the citizen under one umbrella which include : Possession , income, caste, nativity, one and the same, location, community, residence, relationship, family membership, non-remarriage, possession and non-attachment, domicile, life, identification, valuation, legal, widow-widower, dependency, destitute, solvency, inter-caste marriage, conversion, minority certificate.
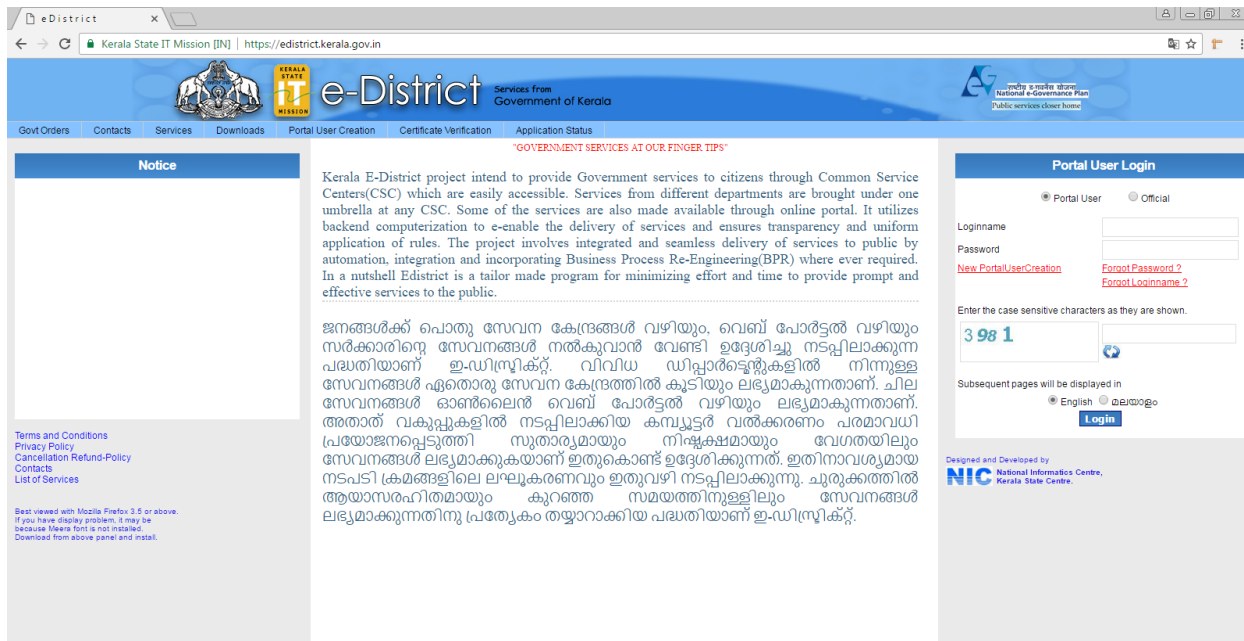
1.1.21 HSCAP

www.hscap.kerala.gov.in

Most of you might have heard about this site. Various Higher Secondary announcements, circulars are available in this website. Most importantly this site is mainly meant for Single Window System with the list of all the schools in every districts.

1.1.22 DCE Scholarship

www.dcescholarship.kerala.gov.in

Department of Collegiate Education includes online scholarship registration and other details which are available for school and college students.

1.1.23 Akshaya Centers

Have you visited any Akshaya Centers? What all services are provided by Akshaya Centers? The website http://www.akshaya.kerala.gov.in/ can take us to the Akshaya Centers and its services

Citizen Services

In 2007 Akshaya moved into phase two of the project, covering the balance six districts and also rendering new G2C and B2C Services. Akshaya has to its credit over 200 crore rupees worth transactions besides providing multitude of services through its 2000+ Akshaya centres. The second phase of e-centre is its growth as a platform for rendering all forms of services to the people. Akshaya e-centres could bring about vast improvement in the lives of citizens through e-pay, e-filing etc.

Title Filter [   ]

#	Article Title	Hits
1	Kiosk Banking	6703
2	Labour Welfare Board Data Entry	5287
3	FREES	6133
4	Unique Identification Number (UIDAI/Aadhaar)	32609
5	E-Grantz	31628
6	Collection of subscription amount of NRK Welfare Fund	2803
7	E-District	80916
8	Registration of APL/BPL families under RSBY	20215
9	e-Payment	101889
10	Online Application Of Ration Card	34539
11	e-Filing for Commercial Tax Department	20650
12	e-Ticketing	6905
13	Motor Vehicle Department services	7522
14	Aam Admi Bima Yojana (AABY) Registration	40547
15	e-Consignment	5403
16	Service and Payroll Administrative Repository of Kerala (SPARK)	54338
17	Help Desk in Collectorate	3629
18	Janamythri Police Station	4994
19	E-delivery of Admit Cards	2630
20	Nodal Centre for Malayalm Computing	2893
21	Nodal Centre for Community web portal	2855
22	Public Grievances redressal	3590
23	RELIS (Revenue Land Information System) Kerala	7021

Services that a citizen gets from an Akshaya center is shown above

Slide 28

Education Support Sites

There are many sites which offer videos and trainings on the school syllabus. They give detailed description and videos to explain the facts you are studying in school and provide online tutions and sample question papers. Merit Nation, Topper Learning etc are some examples.

Slide 29

E-commerce

Electronic commerce, commonly written as E-Commerce or e-commerce, is the trading or facilitation of trading in products or services using computer networks, such as the Internet or online social networks.

E-commerce businesses may employ some or all of the following:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in retail for launching new products and services
- Online financial exchanges for currency exchanges or trading purposes

Slide 30

1.1.24 Common e-commerce sites and uses

Some of the popular E-commercial sites are listed below

Slide 31

Uses of Ecommerce

- Exploitation of new business.
- Improvement of business transactions.
- Effective Performance
- Greater Economic Efficiency
- Incorporating Transactions
- Increasing of Revenue

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Sector – 9, Dwarka Institutional Area, New Delhi-75

TCS Internal25

E-Commerce advantages can be broadly classified in three major categories:

- Advantages to Organizations

- Advantages to Consumers

- Advantages to Society

---------------------------------Supporting Data ---

1.1.24.1 Advantages to Organizations

Using E-Commerce, organization can expand their market to national and international markets with minimum capital investment. An organization can easily locate more customers, best suppliers and suitable business partners across the globe.

- E-Commerce helps organization to reduce the cost to create process, distribute, retrieve and manage the paper based information by digitizing the information.

- E-commerce improves the brand image of the company.

- E-commerce helps organization to provide better customer services.

- E-Commerce helps to simplify the business processes and make them faster and efficient.

- E-Commerce reduces paper work a lot.

- E-Commerce increased the productivity of the organization. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-in-time manufacturing way.

1.1.24.2 Advantages to Customers

- 24x7 support. Customer can do transactions for the product or enquiry about any product/services provided by a company anytime, anywhere from any location. Here 24x7 refers to 24 hours of each seven days of a week.
- E-Commerce application provides user more options and quicker delivery of products.
- E-Commerce application provides user more options to compare and select the cheaper and better option.
- A customer can put review comments about a product and can see what others are buying or see the review comments of other customers before making a final buy.
- E-Commerce provides option of virtual auctions.
- Readily available information. A customer can see the relevant detailed information within seconds rather than waiting for days or weeks.
- E-Commerce increases competition among the organizations and as result organizations provides substantial discounts to customers.

1.1.24.3 Advantages to Society

- Customers need not to travel to shop a product thus less traffic on road and low air pollution.
- E-Commerce helps reducing cost of products so less affluent people can also afford the products.
- E-Commerce has enabled access to services and products to rural areas as well which are otherwise not available to them.
- E-Commerce helps government to deliver public services like health care, education, social services at reduced cost and in improved way.

E-Commerce disadvantages can be broadly classified in two major categories:

- Technical disadvantages
- Non-Technical disadvantages
- e-commerce disadvantages

- There can be lack of system security, reliability or standards owing to poor implementation of e-Commerce.

- Software development industry is still evolving and keeps changing rapidly.

- In many countries, network bandwidth might cause an issue as there is insufficient telecommunication bandwidth available.

- Special types of web server or other software might be required by the vendor setting the e-commerce environment apart from network servers.

- Sometimes, it becomes difficult to integrate E-Commerce software or website with the existing application or databases.

- There could be software/hardware compatibility issue as some E-Commerce software may be incompatible with some operating system or any other component.

1.1.24.5 Non-Technical Disadvantages

- Initial cost: The cost of creating / building E-Commerce application in-house may be very high. There could be delay in launching the E-Commerce application due to mistakes, lack of experience.

- User resistance: User may not trust the site being unknown faceless seller. Such mistrust makes it difficult to make user switch from physical stores to online/virtual stores.

- Security/ Privacy: Difficult to ensure security or privacy on online transactions.

- Lack of touch or feel of products during online shopping.

- E-Commerce applications are still evolving and changing rapidly.

- Internet access is still not cheaper and is inconvenient to use for many potential customers like one living in remote villages.

---Supporting Data ---

Slide 32

E –Banking

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect

to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up. The types of financial transactions which a customer may transact through online banking are determined by the financial institution, but usually includes obtaining account balances, a list of the recent transactions, electronic bill payments and funds transfers between a customer's or another's accounts. Most banks also enable a customer to download copies of bank statements, which can be printed at the customer's premises (some banks charge a fee for mailing hard copies of bank statements).

Slide 33-34

Popular Online banking sites include

- Online SBI
- Online SBT
- HDFC
- ICICI

SBI Online

https://www.onlinesbi.com/

User can click on the login button, enter the username and password and navigate to the Customer page

SBT Online

https://www.sbtonline.in/

User can click on the login button, enter the username and password and navigate to the Customer page

HDFC

https://netbanking.hdfcbank.com/

User can enter the User Id and password and navigate to the Customer page

ICICI

https://infinity.icicibank.com/corp/Login.jsp

User can enter the User Id and password and navigate to the Customer page

Digilocker

[Slide 35, 36, 37]

An Aadhaar card linked Digital Document storage service available to keep valuable e-documents at one place enabling availability of the documents electronically and online via secure link so that they would not need to present physical copies to various authorities.

- DigiLocker is one of the key initiatives under the Digital India Program.
- This was released by the Department of Electronics and Information Technology (DeitY), Government of India in February 2015.
- The storage space (maximum 10 MB at the time of launching & now upgraded to 1GB) is linked to the Unique Identification Authority of India (Aadhaar number) of the user.
- The space can be utilized for storing personal documents like University certificates, Permanent account number (PAN) cards, voter ID cards, etc., and the URIs of the e-documents issued by various issuer departments.
- There is also an associated facility for e-signing documents.
- links to access DigiLocker are http://elocker.gov.in/and http://digilocker.gov.in/

1.1.25 DigiLocker Advantages

- DigiLocker can be accessed only if you have Aadhaar Card.
- Registration is only possible through Mobile No and Email linked to Aadhaar Database. If your email and mobile no have changed then you should get it changed in Aadhaar Database before you sign up for DigiLocker.
- Currently, 10 MB space is available for cloud storage which will be upgraded to 1 GB in future.
- **Anytime Anywhere Access:** You can access your documents anytime anywhere. No need to carry your documents. Therefore, DigiLocker brings convenience factor.
- **Quick turnaround time:** Any agency can request for your documents based on Aadhar. Instead of sending the physical copy you can send digitally verified copy stored as URI (Universal Resource Indicator) in DigiLocker. The agency can directly access your document from the central repository through URI. Documents can only be requested by the agencies who will register with Digital Locker System. For e.g. today it takes around 2 weeks to get new PAN card. You applied for PAN online. Income Tax department will raise online request for documents required to issue PAN. You will eSign the documents through **DigiLocker** using Aadhaar e-KYC service. In case of eSign,

KYC of Aadhaar will suffice for eSign. E-signed documents will be received by Income Tax Department. Your PAN will be issued and appear in DigiLocker under "Digital Documents".

- **Reduce Frauds:** Today financial frauds are very common. Documents are being compromised at various touch points. Digitization will eliminate all such risks. Documents can be shared in safe and secure manner. At the same, you have to ensure that you should not share your DigiLocker or Aadhaar details with anyone.

- **eSign:** In layman terms, eSign is self-attestation or digital signature. It is the replacement of physical signature. The best part is eSign facility is Free whereas for digital signatures, you need to pay annual fees.

- **Corruption Free India:** In my opinion, Corruption is directly linked to Human Interaction. DigiLocker is the true enabler of digitization which will further reduce the human interaction to avail Govt Services. Therefore, it will help in realizing dream of Corruption Free India.

2   How to use internet safely

Slide 1

Till now we saw how internet is affecting our daily life. But to utilize internet effectively, we need to take care of many things.

From the username and password we select when we register in sites, we need to be careful. If not, its easy to become a victim of issues in cyber world.

Slide 2

One of the aspects of internet which is highly used by students are searching facility. Probably you all might have used "Google" at least once.

Its not only google, we have many search engines available today; google might be the most famous one. We can see some of the other search engines available in this slide.

Lets see what all we need to take care when we search something and how to make our searching easier and effective.

Easy Searching Tips

[Slide 3]

- When you are doing searching use the tab facility in browser. It will be easier for you to compare the search results.
- Start Simple and Take Advantage of the Search Tool - When you begin a search, use the simple mode to enter search terms.
- Use Unique Terms - When Possible to Retrieve More Specific Results Search tools use language to retrieve results
- Use Unique Terms - When Possible to Retrieve More Specific Results Search tools use language to retrieve results.
- Use More than One Search Tools - Not all search tools are alike. A search will produce radically different results depending upon the tool used.
- Use Both the Advanced and the Simple Modes of Search Tools - Learning to work with the Advanced Search allows you to work with more search options and retrieve sites that are more relevant.

- Search engines provide auto complete facility. Take advantage of this.
- Customize your searches - You can customize your search results to choose what information appears with each listing and how you want listings to be sorted and displayed. When you customize your results, your settings are saved so you don't have to reset them every time you sign into eBay. If you ever want to remove your customizations, you can restore the default (original) settings.
- Use browser history – you might have searched the same thing before
- Use not more than 5 – 7 key words – Number of key words to be given for searching should not be more than 7. It will dilute your search
- Set a time limit — then change tactics - If you are not getting the desired result after sometime, either change the keyword or change the search engine.

- Use the Directories in Search Tools or Subject Directories - To locate information on the Web, you either know Web address for a specific site, or search for a topic of interest. When searching by topic, a huge number of pages will often be retrieved and makes it difficult to identify the relevant resources. Subject directories help to alleviate the problem. **Subject Directories** are created and maintained by the directory's staff
    - allow you to browse Internet resources by different subject categories
    - enable you to search by keywords within the contents of the directories
- Keep wading to a minimum - Though the search engines return huge result, most important results will be in the first or second page, you don't have to go through everything search engine returns
- Use the MetaSearch Tools and Natural Language Tools - Metasearchers are an excellent way to explore a topic and gather keywords and other information. MetaSearch tools, such as Internet Sleuth, ProFusion, MetaCrawler, and others, search multiple tools simultaneously and are good tools to begin your research. After using a MetaSearch tool, refine the search by using the available features specific to each individual search tools.
- Use Find or Ctrl + F to find something specific in search result.

[Slide 4]

Now let's see what all we need to take care when giving the keywords.

- Use the minus operator (-) to narrow the search - If we give a second word after a (-) sign in the search, the search engine removes the result containing the second word.
- Use quotation marks for exact phrases

- Don't use punctuation
- Use a colon to search specific sites – If you want to search specific sites mention the sites after the key word separated by a colon.
- Drop the suffixes - book and books doesn't make a difference.
- Customize your searches
- Search a price range for an item (Use two periods (..) between two prices)
- Use an asterisk if you don't know the word
- Use Capitalization - When appropriate or to refine a Search Not every search tool is case sensitive.

Safe Searching

[Slide 5]

Now we will see some of the tips to make searching safer.

- **Update Web browsers regularly -**Choose "Yes" when browser programs like Firefox, Internet Explorer, or Safari prompt you to update;
- **Enable security features-**Adjust security settings for Firefox, Internet Explorer, or Safari browsers to warn you about annoying and potentially dangerous threats to your security, like popups, spyware, and malicious add-ons
- **Install protective software-**Web of Trust warns you if a Web page might pose a risk to your security and helps you verify that a page you are about to visit is legitimate. Symantec Endpoint Protection is comprehensive security software that includes additional protection against spyware
- **Guard personal information-**Look for signs of an encrypted Web page when providing sensitive personal information (credit card or banking information, SSNs, etc.) online;
- **Be wary of Internet downloads-**Streaming media Web sites might seem harmless, but watching or listening to streaming media may mean downloading a special media player that could contain malware
- **Key in Search terms correctly-** You don't want to end up with search results which you didn't intended.
- **Confirm the authenticity of sites –** Before you click on any search result, confirm the site is genuine
- **Double check a sites reputation** - Check the site's reputation, you don't want to end up in a site with illegal content

- **Use filters –** Use filters to remove unwanted data

- Use parental controls that restrict internet access

- Use browsers safest search settings

- Block words you don't want to search

- Always have parents/teachers presence when online

- Know legal versus illegal content

2.1   Kid friendly search engines

Slide - 6

Today, other than the well-known search engines available, there are some search engines, suitable for kids, which provide only information suitable for kids.

In this slide you can see the comparison of search results returned by well-known search engines and a kid friendly search engine. Here Green indicates information suitable for children and Red is information not appropriate for children. You can see that compared to other engines, it's the kid friendly site which returns suitable data.

Other than kidrex there are some more kid friendly search engines available like, Kiddle and Safe Search Kids.

Google Transparency Report

 [Slide 7]

Google's Safe Browsing technology allows users can search to see whether a website is currently dangerous to visit. When Google detect unsafe sites, they show warnings on Google Search and in web browsers.

Here you can see the response for irctc in google transparency.

Be SMART when you are online

 [Slide: 8]

The things to take care when you are online can be summarized in a single word "SMART". We will see what each letter in this indicates.

SAFE: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

MEETING: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's permission and even then only when they can be present.

ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems, they may contain viruses or nasty messages!

RELIABLE: Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows.

TELL: Tell your parent or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

In today's session you will hear these things multiple times. This is to make you understand that how important these are while using internet.

Be Online Be Safe

[Slide: 9]

- Don't sign up for sites that have an age restriction, if you are not old enough

- Don't add people as online friends unless you know them in real life

- Don't give out your personal information

- Do not give out any of your passwords to friends or anyone you meet online.

- Never to agree to meet someone that you have met online

- Be careful about discussing your personal problems with your online friends.

- Ensure privacy settings on activated on all of social media websites you use

- Choose sensible names for usernames, email addresses etc.

- Do not respond to messages you receive that are mean or speaking meanly about others.

- Always be kind to others online.

- Know what cyber bullying is and tell someone if you think it's happening to you. Cyber bullying is when someone picks on you, annoys, embarrasses, or threatens you over and over again using technology, such as the internet or a phone.

- Protect your digital footprint - don't share anything which you don't want your parents, friends or teachers to see.

[Slide 10]

- Agree to computer rules set up by your parents, teachers or guardians.

- Talk to your parents about what you're doing online and let them know when you're going on the internet.

- Check with your parents first before downloading or installing any software on your computer.

- Talk to your parents first about pictures you want to post online

- Treat others online the way you'd like to be treated.

- Remember that you cannot believe everything you read on the internet and you can't trust everything online

- Remember that the rules for online safety also apply to texting on your phone

- Always ask an adult if you're unsure of anything when you are online.

[Slide 11]

In this you can see how the parent of this young girl is ensuring that she is doing online shopping only from secure sites. "https" in the mail address indicates that the site is secure.

The other picture shows, some implications of using internet without thought. Some of them lost their job because of some stupid posts in social media and one lost the job because of posting an embarrassing video in YouTube. So be careful of the data you upload.

-----------------------------------SUPPORTING DATA---

Online security tips that should be followed:

● Always ask an adult if you're unsure of anything when you are online.

- Remember YAPPY (the personal information you should not share online) – Your full name, address, phone number, passwords, your plans.

- Don't add people as online friends unless you know them in real life or have parent permission. Never arrange to meet an online friend without talking to a parent.

- Remember that you cannot believe everything you read on the internet and you can't trust everything online friends tell you.

- Choose sensible names for usernames, email addresses etc.

- Talk to your parents about what you're doing online and let them know when you're going on the internet.

- Know what cyber bullying is and tell someone if you think it's happening to you. Cyber bullying is when someone picks on you, annoys, embarrasses, or threatens you over and over again using technology, such as the internet or a phone.

- Protect your digital footprint: don't put anything online that you wouldn't want all your friends, family, teachers and future employers to see.

- Treat others online the way you'd like to be treated.

------------------------------------SUPPORTING DATA--

Now we will see some of the sites useful and how safe we need to be while using them.

Wiki

[Slide: 12]

Wikipedia is written collaboratively by largely anonymous volunteers who write without pay. Anyone with Internet access can write and make changes to Wikipedia articles, except in limited cases where editing is restricted to prevent disruption or vandalism.

The Malayalam Wikipedia (Malayalam: മലയാളം വിക്കിപീഡിയ) is the Malayalam language edition of Wikipedia and was launched on December 21, 2002. The project is the leading Wikipedia among other South East Asian language Wikipedias in various quality matrices. It has grown to be a wiki containing more than 30,000 articles as of April 2013.

2.1.1   Advantages

What are the advantages of Wiki? How different it is from a printed encyclopedia?

- anyone can edit
- easy to use and learn
- Wikis are instantaneous so there is no need to wait for a publisher to create a new edition or update information
- people located in different parts of the world can work on the same document
- the wiki software keeps track of every edit made and it's a simple process to revert back to a previous version of an article
- widens access to the power of web publishing to non-technical users
- the wiki has no predetermined structure - consequently it is a flexible tool which can be used for a wide range of applications
- there are a wide range of open source software wiki's to choose from so licensing costs shouldn't be a barrier to installing an institutional wiki

YouTube

[Slide 13]

YouTube is an online public communications site. The site allows for registered users to upload and have available for the public their videos for viewing. Anyone who goes to the site can view the videos that are posted on this site. The videos are anything from beginner videos to more professional videos. Originally created in 2005, YouTube is now one of the most popular sites on the Web, with visitors watching around 6 billion hours of video every month.

Teens are an important part of the YouTube community. Here are some useful tools and friendly tips for staying safe on YouTube.

- **Know what type of content to film:** When filming videos of your friends, classmates, or other minors, remember that they should never be sexually suggestive, violent, or dangerous.
- **Remember "The Grandma Rule":** Is what you're filming or posting something you'd want your grandmother, boss, future employer, parents, or future in-laws to see? If not, it's probably not a great idea to post it.

- **Use YouTube's privacy features:** YouTube has features to help you limit who can see the videos you post. Protect your privacy by setting personal videos to 'private' or 'unlisted.'
- YouTube has a feature call Safety Mode.
- **Turn on Safety mode.** It's kind of hidden, but YouTube has a Safety mode that will block most (but not all) objectionable content. You'll have to scroll all the way down to the bottom of the home page to find it, however.
- **Choose carefully.** Just be sure to watch the videos all the way through before you add them to a list,
- **Eschew the Tube.** If policing YouTube content is too much of a hassle, you can block it using a Web filter and redirect your kids to family-friendly video sites.
- **Upload with extreme caution.** Monitoring what your kids see on YouTube isn't nearly as important as keeping an eye on what they *show*.
- **Post in private.** When you click the **Upload** button, you're given the option of making videos public (the default setting), private, or unlisted. Make them private, at least at first. You can still invite friends and family to see them by adding the appropriate Google Circles to the **Share to** box or plugging in email addresses.
- **Kill comments.** You can turn comments off. You'll have to start by clicking the **Upload** button and posting a video. Select the **Advanced settings** tab on the Upload screen. You have two options: Kill comments entirely, or block them until you've had a chance to approve them.
- **Accentuate the positive.** YouTube can be a great resource for education as well as entertainment. You have to help kids discover the good stuff and guide them toward it.

Downloading Tips

[Slide 14]

Be careful what you download, and ask questions about the site you are downloading from.

We live in a digital age in which we can download just about anything we want to watch, listen to or use… and have access to it almost immediately.

While there are hundreds of legitimate sites from which digital content can be downloaded, there are thousands more that offer bogus, and harmful content, filled with malware designed to steal your financial and other personal information.

What all you need to take care while downloading something from internet?

- First and foremost, disable the automatic download. Always read and give permission to download.

- Stick to Software from Trusted Sources

- If Possible, Download directly from the Software's Official Site

- Use Your Antivirus Software to Check Potential Downloads

- Check File Specs for Authenticity

- Don't download pirate apps.

2.1.2   Secure downloads

[Slide 15]

So, if you must download the latest movie or song, think twice about where you are downloading it from.

- Is the site well-known?

- Have any of your friends used the site without incident or unexpected surprises?

- Is it actually the site you think it is rather than a clone?

- Check your browser if the URL beginning with https:// for some certainty and don't ever visit a download link sent you via email

- Many downloading sites are embedded with malwares and adware. Always hover your mouse over the download button or link to see the exact link and only use the links which are related to the site you are using.

- Any carefree clicks can help a hacker to install a malware into your system. Always be careful.

2.2   Blocking a Website in a local network/machine

[Slide 16]

Many a times there is a necessity to block sites in a network or a particular machine. How to do that? This will help you to block some unwanted sites in your home and school.

2.2.1   Using OpenDNS to Block Site Categories or Domains

OpenDNS is a company that provides free DNS servers rather than using your internet service provider (ISP).One feature is the ability to block domains or group of domains. The service is free. If you need to restrict access, OpenDNS has over 50 category filters covering the usual suspects.

2.2.2 Using your Router Software to Block Sites

Another way to block websites is with your router. A router is hardware that directs traffic between your network and the internet. Most popular routers offer some sort of "parental control" or "internet access policy". In this case, I'm allowing one PC to use the internet all the time except for the eBay domain that I've blocked.

2.2.3 Using the Windows Hosts File

The idea is that you redirect your web browser to go to another IP address, such as your local machine, rather than the intended site. In most cases, the fix requires you add a line to the Hosts file using a text editor.

E-mail account setup

[Slide 17, 18]

Email is useful for communication, marketing, and promotion, mobility, filtering and follow-up. Correspondence with friends and internal business communication are both daily uses for email.

To create a Gmail, follow the steps as below:

- Step 1: Open the Gmail web site - Go to http://gmail.google.com
- Step 2: Enter all the required information in the "Create an Account" online form
- Step 3: Choose a login name or username for your email address
- Step 4: Choosing a password for your email
- Step 5: Protecting your Gmail account with a security question
- Step 6: Word Verification: You need to enter the characters that you see in the picture above the field in your form.

----------------------------SUPPORTING DATA ---

Step 1: Open the Gmail web site: To create your Gmail account you only need a web browser and an internet connection. Go to http://gmail.google.com. You should now get to a page that looks something like the one below.
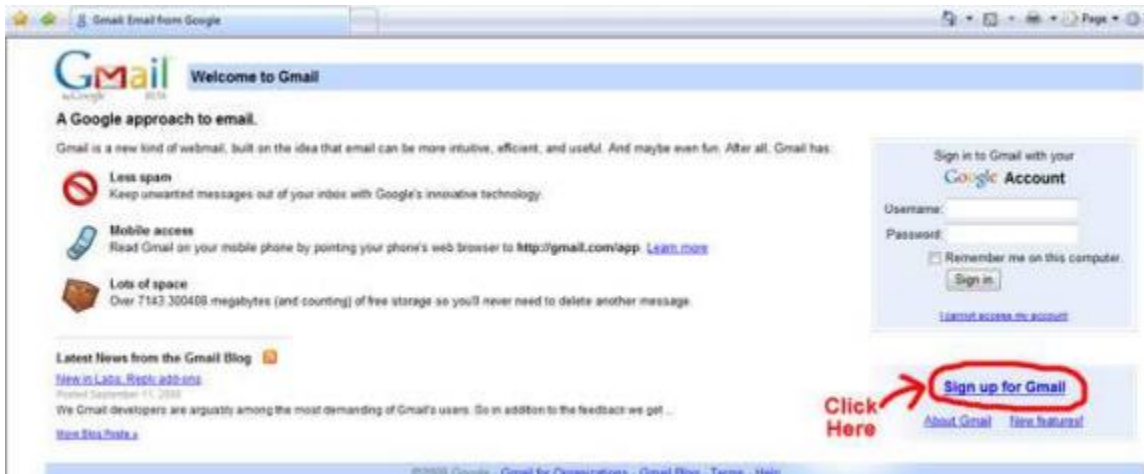
Step 2: Enter all the required information in the "Create an Account" online form.
You now need to start filling the form. Once you have entered your first and last names, it is time to choose a login name. This is important as your login name will decide the email address you will get, and in case of a Gmail account, would be your-chosen-loginname@gmail.com. So be sure to pick a login name, also called the username, with care.

Step 3: How to choose a login name or username for your email address

The availability of a login or user name can be verified by entering it first in the text field and hitting the check availability button.
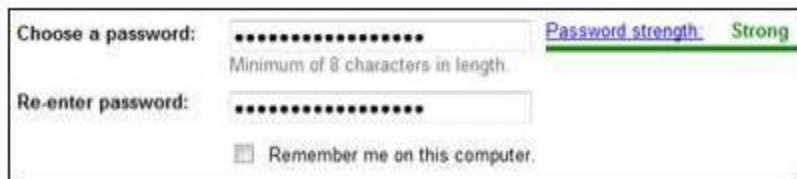
Step 4: Choosing a password for your email

Securing your Gmail email account with a *strong* password is a must. A combination of uppercase and lowercase letters with some digits thrown in would be a strong enough password. On the right of the text fields in which you enter your password a sort of meter would indicate the strength of the password. You need to enter the password twice and you can leave the "*Remember me on this computer*" box unchecked.

Step 5: Protecting your Gmail account with a security question

Step 6: Word Verification: You need to enter the characters that you see in the picture above the field in your form.

Why is this required? So that Gmail knows the inputs are from a human being and not some automated program.

**CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

------------------------------SUPPORTING DATA --

Selection of Passwords

[Slide 19]

Strong passwords are extremely important to prevent unauthorized access to your electronic accounts and devices.

A strong password:

- At least 8 characters long

- Unique; different from other passwords

- Mix of alphabetical and numeric characters

- Symbols if the system allows

- Mixture of upper and lowercase

- Complex but easy to remember

- Difficult for others to guess

- Change regularly

In this slide you can see how we can arrive with a strong password from a passphrase or sentence which is easy for you to remember.

- 15 Ferrari red -> 1+ferr+red+ari+5 -> 1feredari5 - It's not difficult to remember the phrase 15 Ferrari red. But the password arrived from that *1feredari5* is a difficult password to guess.

[Slide 20]

Take care of these items when you are choosing a password.

Don'ts:

- Doesn't include terms that are significant to you like pet's name, username, real name, date, phone number that are easy to guess or use complete words that make it easier for hackers who use dictionary attack programs.

- Also avoid common word misspellings and words in which letters have been replaced by numbers or symbols because some dictionary attack programs also check for these.

E.g.: $ instead of S, @ instead of a, 1 instead of i

- Keep your passwords secure. Don't leave notes with your passwords to various sites on your computer or desk. People who walk by can easily steal this information and use it to compromise your account.

- **DON'T** write your password down

- **DON'T** share your password with anyone

- **DON'T** include all or part of your username, first name, or last name

- **DON'T** include terms that are significant to you like pet's name

- **DON'T** include phone number, birthday, number plates

- **DON'T** use alphabet or number sequence

- **DON'T** use a word contained in English or foreign language dictionaries

- **DON'T** use a word spelled backwards

- **DON'T** use a password of all digits, or all the same letter

- **DON'T** Re-use any of your last 10 passwords

There are multiple ways hackers try to get the password and some of them are

- Social Engineering
- Spyware
- Key logger
- Remote Admin Tool
- Trojans
- Cracking
- Guessing

And believe it or not, rather than any other technology, guessing and social engineering are still the best ways to get the password.

Also many sites provide secret questions to retrieve your password in case if you forget them. Many of the times what happens is that you select some question randomly and won't be able to recollect the answer given at a later point of time. To be safe on this aspect, always select questions for which you have

a definite answer. If you select the question "What is your favorite color" there might be a chance that you provide a wrong answer. But to a question like "the city where you were born" you will always have a single answer.

Copyrights

(Slide 21)

You all must have heard about copy rights. Many things we have around us are copy righted, books, songs and even movies. Similarly many a time's digital content in internet is also copyrighted.

If you are not already aware, Copyright is a legal right created by the law of a country that grants the creator of an original work exclusive rights for its use and distribution.

In our country, Sharing **copyrighted material** to open public without due permission from the owner(s) is a punishable offence under the **Copyright** Act.

In many other countries, downloading and watching copyrighted material over internet is a punishable offence.

3   Gaming

Now let us talk about a topic where most of you will be interested, gaming. All of you must be playing computer games, isn't it? And you enjoy playing them, don't you? Are you aware that gaming helps to sharpen your spatial and fine motor skills? Like that playing computer games in good moderation has many advantages. Let's go through them once.

3.1   Positives of Gaming

(Slide 2, 3)

3.1.1   Problem Solving Capability

When a child plays a game, he trains his brain to come up with creative ways to solve puzzles and other problems in short bursts

Hand-eye coordination, fine motor   and spatial skills

While Playing First person shooting games player must then coordinate the brain's interpretation and reaction with the movement in his hands and fingertips.

Studies with adults shows that experience with video games results to better surgical skills and also fighter pilots of today are more skilful than the older generation.

Planning, resource management and logistics

Players Need to utilise the limited resources they have and have to win the enemies who have huge resources than them .So , to make this happen , Players have to think smarter and make important On-game decisions in order to win

(Slide 4)

Though there are some advantages of gaming, the continuous and non-controlled gaming makes us loose our sleep, physical stamina and make us indifferent from the society.

People who play games tend to have a bigger and more active striatum – a part of the brain that links simple stimulus-response-reward sequences together – and a smaller and less active hippocampus, which forms episodic, relationship-based memories. And that has implications for overall brain health, since a shrunken hippocampus is associated with risk of neurological disorders such as Alzheimer's and schizophrenia.

3.2 Side effects of excessive gaming

Slide-5

Let's talk about main effects of excessive gaming in detail

Preoccupation

A video game addiction can be harmful if your child is unable or unwilling to participate in any interests or extracurricular activities other than gaming.

Health Problems

Children who spend more than two hours a day in front of a television or video games in lieu of participating in physical activity may suffer from childhood obesity.

Moreover gaming addiction can lead to medical issues such as backaches, headaches, eyestrain and carpal tunnel syndrome--pain and numbness that child may feel in his wrists, hands, shoulders and elbows.

Suffering Relationships

Relationships with friends and family members may suffer if your child is spending more time gaming than he is talking to or going out with loved ones.

Increased Aggression

Video games that feature violent actions and scenarios may lead addicted players to be desensitized to the violence. Studies show, players who become engrossed in first-person shooter-style video games, for example, may adopt a detached view of society or develop aggressive thoughts and tendencies.

Poor Performance

Long hours playing video games can negatively affect a child's performance in school if he's preoccupied with video games. Children may have trouble falling asleep, have problems paying attention and have lower test scores than other children who don't spend as much time in front of a television or video game console.

So limit your play time so that you can enjoy the gaming without it affecting you adversely.

3.3 Different Source of games

Slide – 6

Now what are different sources of games?

Boxed games – Games that come on a disc or cartridge that are purchased from a store or online, and played on a game device like a console, handheld or PC.

Digital download – These are downloaded directly to the console, PC or handheld device. Most consoles (Xbox 360, PlayStation 3 and Wii) have their own online marketplaces where games can be downloaded.

Mobile storefronts – Smartphones and tablets let users download apps from online marketplaces linked to a credit card, e-wallet or your mobile phone account

Subscription – Online games or arcades where the player signs up for an account that lets them play a game (or many games) for a certain amount of time for a fee.

Free-to-play" and "freemium" – These games are typically supported by ads instead of purchase or subscription fees; "freemium" games let you play a limited portion for free but require that you pay to access new content or features.

Social networking games – Played from within a social network like Facebook, these games encourage users to share content and updates with others in their social network.

3.4 Gaming Tips for Kids, Tweens and Teens

Slide 7,8 – How can we keep ourselves safe while playing?

Keep a clean machine: All Internet-enabled devices need to be kept up to date to protect them from malware and other threats. Security protections are built in and updated on a regular basis.

Make your password a sentence: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music.").

Speak up: If another player is making you feel uncomfortable, tell a trusted adult.

Report cyberbullies: Learn how to block and/or report another player if they are making you uncomfortable.

Protect your personal information: Never reveal your real name, location, gender, age, or any other personal information. Keep your user name vague and use an avatar rather than an actual picture of yourself.

Protect your identity: Do not use voice chat when playing an online game, unless there is a feature that allows you to disguise your voice. Do not use a web-cam while playing an online game. Do not present yourself as dating material.

Time limit: Put a time limit on yourself for game playing.

When in doubt, throw it out: Do not accept downloads from strangers. This includes cheat programs that may claim to help you perform better in the game, but really could be carrying malware.

Think before you act: Do not meet a stranger from your gaming world in person. People are not always who they say they are.

Be a good digital citizen: Know the risks and practice good judgment.

Block the Player: If a situation makes you uncomfortable, you can always block the person playing with you. If you are getting multiple accounts writing inappropriate content, talk to your parents immediately about the problem before the situation gets worse.

Check the rating: Checking for a game's Entertainment Rating Software Board's rating - on game packages, online or in some mobile app storefronts – is a great place to start in terms of gauging its age-appropriateness.

Keep the computer out in the open: If your computer is in a central location, the chances are more that you're stick to the timing and sites permissible for you.

4   Social Media

Slide – 9, 10

Now another interested topic for you. Social media. You all know Facebook and WhatsApp. Do you use them? What other social media you use?

You know what is social media definition?

"Social media is the use of electronic and internet tools for the purpose of **sharing** and **discussing** information with other human beings"

Slide – 11

There are many ways in which social media helps you. Do you know that?

1. Worldwide connectivity – It helps to keep you connected with your friends however far they are and thus keeps your friendship stronger over the time.
2. Commonality of Interest - When you opt to participate in a social network community, you can pick and choose individuals whose likes and dislikes are similar to yours and build your network around those commonalities
3. Real-Time Information Sharing - Many social networking sites incorporate an instant messaging feature, which lets people exchange information in real-time via a chat.
4. Expand your business – Now you can see many people are opting to do online business through social network sites.

Slide 12

Please keep these points in your mind when you are on social media.

- It's not show and tell - Don't try to have posts on everything you buy and do.
- E-mail blasts – don't send out information if not needed.
- It's not your diary – Don't disclose everything you feel and do in social media.
- Finally understand that whatever you see in social media need not be real. Be careful.

Slide 13

There are various classification of social networks

Social News Site and book marking Sites - these help the user to go through user posted stories and rate them. Examples are Digg and Reddit

Blog and Microblogs – Here the users can broadcast large or small (microblogs) amount of information. Examples are Twitter and Tumblr.

Social networking - helps people to build social networks or social relations with other people who share similar personal or career interest's activities, backgrounds or real-life connections

Media Sharing sites – In these platforms the users can share video or photo contents.

Virtual world – In virtual world the user accesses a computer-simulated world which presents perceptual stimuli to the user, who in turn can manipulate elements of the modeled world and thus experience a degree of presence

Slide 14

When you are using social media, always ensure that

You are not sharing:

- × Contact Information

- × Pictures you don't want everyone to see

- × Information about your school or work

- × Your Travel Plan

- × New Purchases

- × Friends In 'Unglam' Shots

- × Chain Status updates

And don't

- × Assume any communication is private

- × Add friends you don't really know

- × Disable privacy on your accounts

- × Comment on every post
- × tag people in irrelevant posts
- × send random application/game invites

Disadvantages of Social Networking

(Slide – 15)

1. Lacks Emotional Connection

The quality of a conversation using social media is awful because you cannot sense the emotion or enthusiasm from the other person. It makes you wonder if they actually mean what they say."

2. Gives People a License to be Hurtful

As the users are not talking face to face, one can take it for granted and feel that they can get away after being hurtful to others.

3. Decreases Face-to-Face Communication Skills

"Computer reliance could hurt a person's ability to have a face to face conversation by making it awkward and unusual to hear something and respond with a thoughtful message through the spoken word.

4. Creates a Skewed Self-Image

"We tell ourselves lies about ourselves and develop something we are not. We post pictures of us looking perfect and share the good news. We never post pictures of ourselves when our dog dies, when someone we love leaves, and when we lose a job. We never share the bad news that always clouds our lives. We all develop this perfect image of ourselves."

5.   Reduces Family Closeness

"Texting, Facebook, Twitter, and Gmail alienate us from our families more than we actually think it does….

6.   Conveys Inauthentic Expression of Feelings

7.   Diminishes Understanding and Thoughtfulness

8.   Causes Face-to-Face Interactions to Feel Disconnected

9.   Facilitates Laziness

10.   Causes Distractions

11. Reduction in physical Activities

4.1   Social Media Sites and security settings

Slide 16

Now let's talk about two most commonly used social networking applications, Facebook and WhatsApp.

There are many functionality available in apps like Facebook, WhatsApp etc to ensure to keep your privacy safe and secure. Some of them are:

- Who can look you up using the phone number you provided?
- Who can send you friend requests?
- Control what's public on your Time line.
- Tagging can be restricted.
- Who can view the posted photos and videos?

But many a times users especially teenagers are so busy that they don't take a moment to care about this and post many unwanted details in Facebook which leads to many dangers. They post their personal information, whereabouts and even phone numbers which is a complete No No.

Slide 17

When using WhatsApp, there are many loop holes.

- Opens the Door to Strangers – Once someone gets your contact number, it's easy to reach you
- Raises Probability of Sexting
- Increases the Vulnerability to Cyberbullying
- Easy to share location details

We need to take care of the following things when using WhatsApp.

- ✓ Do not share your personal information or valuable information. It may be saved in the server and can be hacked.
- ✓ Do not respond to unknown users; block them
- ✓ Make sure that you are not clicking on unknown links or images. These can hack your data on your phone
- ✓ Don't join every group that you are invited or added to

- ✓ Share settings: Share settings should be set to "my contacts."
- ✓ Be careful when you are added to groups. Ensure that everyone in the group is known to you.
- ✓ Be extra careful while sharing information in groups.

Even after repeated reminders children post their personal details and make them visible for public. The kids should understand that all the social networking sites are always combed by people looking for preys. As mentioned never make your personal data public. And always make sure that you are not talking to any strangers in social media. It's the easiest way someone can trick you into dangers. Be careful, use the social media wisely.

Reference

- Hand Eye Coordination

-Davinci machine

- Parental safety: https://www.youtube.com/watch?v=LAxKmGwIYig

- TED Talks: Your brain on video games: https://www.youtube.com/watch?v=FktsFcooIG8

- Can Video Games Make You Smarter? : https://www.youtube.com/watch?v=OOsqkQytHOs

- http://www.authorstream.com/Presentation/bgibbons-1480356-negative-positive-impacts-video-games/

- **https://youtu.be/9p_upvWRUcQ**

- **https://youtu.be/TWhFHppxSYU**

5   Mobile - Safe Practices

<u>Slide 1</u>

Today there are not many people who don't use mobile phones. They provide an efficient and easy way to communicate with friends, family, and co-workers. But excessive use of mobile phones can take a toll on your health. Are you aware how mobile phones are impacting you? There are many physical, psychological and social impact of mobile usage. Let's go through some of them.

Slide 2

Impacting your social life

All in the family are so focused on their mobile devices that they don't have time to consider each other. We can see lot many families in restaurants, but all of them will be busy checking their mobiles rather than spending time with each other**.**

Increases Stress Levels

The high frequency of cell phone use can have negative effects on our stress levels. The constant ringing, vibrating alerts, and reminders can put a cell phone user on edge**.**

Increases Risk of Chronic Pain

Cell phones require constant use of your hands, especially when sending text messages and e-mails. Responding to messages at rapid speed can cause pain and inflammation of your joints. Back pain is also common with increased cell phone use, especially if you hold the phone between your neck and shoulders as you multitask.

Increases risk of eye vision problems

Staring at your mobile device can cause problems in your vision later in life. Screens on mobile devices tend to be smaller than computer screens, which means you are more likely to squint and strain your eyes while reading messages.

Radiation

Studies are still in progress to determine the impact of cell phone radiation on humans, but initial analysis points out that it can increase the risk of brain tumor by 40%.

Selfie accidents

Nowadays we get to hear many incidents where people are getting killed or seriously injured while trying to take selfie in dangerous situations.

Slide 3

Slump/Text Neck

This is again a major outcome of continuous mobile usage.

You may look at the photo and think nothing of it, because this is what we typically see when we are out and about, and it is even the stance we are accustomed to taking when using our own smart phones and devices.

When we hold our head in a healthy, neutral position, the forces to the cervical spine are about 4.5 – 5.5 kg.

Repetitive increases in stress of this nature may lead to all sorts of neck problems, including early wear and tear, degeneration, and possibly the need for surgery

With the help of a plumb line and angle lines, we can see this man's head is tilted at approximately 45 degrees. That means this guy has gone from putting the normal 4.5-5.5kg of weight on his neck to a massive 20 kg)!

 Every day, people like you and I spend an average of two to four hours with our heads tilted over reading and texting on our smart phones and devices. Cumulatively this amounts 700 to 1,400 hours per year of excess stress placed on the cervical spine. To make matters even worse, high school students are spending an extra 5,000 hours bent over reading, texting, and typing on their devices. If you want to save your neck, please consider using proper postures while using mobile phones.

Slide 4

We all know that we cannot avoid cell phones. So how to use them safely. Let's see some tips for using your mobile phone safely

Although cellphones are considered to be low-powered radiofrequency transmitters, your handset transmits power when it is on, and therefore it is important to increase your distance from the handset to reduce radiofrequency exposure.

- Limit the use of mobile phones to essential calls and always keep calls short
- Don't carry your mobile in your pocket or on your belt while it is switched on. Your lower body tissues absorb radiation more quickly than your head.
- Don't immediately put the phone to your ear once you've made the call, wait a few seconds for the connection to be made and while the other phone is ringing.
- Purchase a phone with a low specific absorption rate (SAR).
- Use Text Messaging instead of talking wherever possible.
- Use a land line phone whenever possible (but not a cordless).
- Try not to make calls when there is a weak signal, the radiations from the phone will be on the higher side.
- Please don't sleep with your cellphone near you, especially near your head.
- And don't use cell phone while driving.

It is recommended to use ear phones while talking over phone to reduce health issues. Using headphone or earphone can reduce the radiation to the body, reduce risk of high stress, and reduce risk of ear related issues

Slide 5

Always use proper posture when using the cell phone. The screen should be always at the eye level and you should not be slumping your body while using it. And try doing some basic exercises to improve your posture.

Some examples are:

Stretch your neck in all directions for a couple of minutes every hour.

Strengthen your core muscles to bring down the neck pains.

It's recommended to keep your cell phone usage shorter as much as possible and keeping a distance of 20 cm from the body significantly reduces the radiation. So it's always better to keep the phone away from you as much as possible.

Slide 6

We mentioned that it's better to use earphones while using cellphone. But earphones also have their own set of risks. Continuous usage, especially on higher volume, can cause irreversible damages to ear. It can

lead to ear infections, hearing problems/complete hearing loss and pain. Using earphones in roads are also very dangerous because the user losses the awareness about the surrounding.

Slide 7

When you are using earphones, please consider these points:

- Avoid using tiny headphones/earphones that directly go into the ear canals. Better those big headphones, the old ones which stay outside your ears
- Avoid sharing your earphones/headphones with others. It can lead to infections
- Make sure you change the sponge cover/ rubber cover of your headphones/earphones once a month. If your earphones/headphones doesn't have sponge covers, make sure you sanitize them.
- Do not use earphones/headphones when you are travelling by car, train, metro or even walking.
- No loud music ever when you use earphones/headphones

Slide 8

Mobile apps and uses

Mobile apps were originally offered for general productivity and information retrieval, including

- Email
- Calendar
- Contacts
- Stock market.
- Weather information

However, public demand and the availability of developer tools drove rapid expansion into other categories, such as those handled by desktop application software packages. Now the cellphone are full with user applications supporting every aspect of human life.

Some of the commonly used apps are:-

- Email(Gmail, Yahoo, Outlook) – used for sending and receiving mails
- Messaging and Social Media Apps (Facebook, WhatsApp, Instagram) – Mostly used for communication via internet in real time.
- Gaming Apps (Temple run, Subway surf, Car racing)

- Musical/Entertainment Apps (Play Music, Video players, VLC, MX player)
- Internet browsing(Chrome, QC browser)

Slide 9

When downloading applications for your cellphone you need to make sure that you are downloading it from trusted sources. For each OS available in cellphones, there is a store from where you can download the applications. But at most care need to be taken to verify the authenticity of the application as many OS stores, especially android allows public to upload applications without much security compliance.

Slide 10/11

Other than health hazards and issues, we need to take care of many other aspects when we are using the cell phone that too in a public place. Many a times we can see people talking over phone loudly not even thinking that people around them can hear their conversation.

Some of the pointers for using the cell phone are:

Use a normal tone of voice while speaking on your cell.

Just because you can't hear someone clearly doesn't mean that he can't hear you, so keep your voice down.

Don't Commit Phubbing

The act of snubbing someone in a social setting by looking at your phone instead of paying attention".

Don't Answer Your Phone in the Movie Theatre

If you've forgotten to turn your mobile phone off, and it rings during the movie, don't answer it in the theatre while you're scurrying to move outside

Don't use your speaker phone in public

Not a good idea unless you want everyone around you to hear your conversation

When you are in public places, keep your distance

If you cannot avoid the use, try to stay about 10 feet or more from other people while chatting on your phone.

Don't look things up on your phone while you are talking with someone on that same phone

You can't give the other person your full attention if you are surfing on the web at the same time.

When you're on the job/study, keep your phone put away.

Use it only when you're allowed to do so.

Don't use your phone when having a meal with someone

This is true both at home and in a restaurant. Enjoy your meal and your company.

Avoid texting or talking on your phone when you are having a face-to-face conversation with other people

The people in your immediate vicinity are more important than people on the other end of your cell phone unless its an emergency

6   How Internet impacts you

Today, you saw that internet provides vast opportunity for us. But at the same time, internet, especially continuous or unsafe use of internet pose many threats to us.

Continuous use of internet or even computer impacts you mentally and physically. In this session we will see how internet is affecting your life adversely.

- Slide 1/2

Even with so much technology around, nowadays we hear many times from youngsters that they are bored. Have you ever wondered why? The simple answer is that they spend so much time on the virtual world that they are expecting the same brightness and speed in our real lives which is not possible and when they are not able to find it, they get bored and try to go back to the virtual world.

6.1   Psychological Impact of long time usage

Are you getting addicted to Internet??

Around the world 80% of the youth spend more time on internet. There are more physical and mental risk as this generation is introduced into internet at a very young age. Youth now is suffering from risks due to excess internet use

Excess of internet is not good for you

→   When you are more happy with online friends than actual friends

→   When you can't stop yourself from gaming or surfing or chatting

→   When you avoid family, friends and basic daily needs for internet

→   This condition is known as internet addiction

Slide 3

How can we identify when someone is addicted to internet. The symptoms you need to look for is:

1) Always think of online activity (previous chat/gaming sessions) even in dreams

2) Use internet for more time than the time you expected to use

3) Moody/restless/depressed when internet is cut down

4) Lying to family members for internet use

5) Ignoring your friends and family for internet

6) Ready to forego sleep for internet

Video helps https://www.youtube.com/watch?v=2WrmQ2SHaxM

Slide 4

We can classify internet addiction into separate baskets based on where the user is spending more effort.

Social Media Addiction (Cyber relationship addiction) - Spends more time with online friends

Excess Gaming Addiction – compulsive use of computer games, which interferes with a person's everyday life.

Cybersex addiction   - compulsive use of adult websites for cybersex and cyberporn.

Net compulsions   - Obsessive online gambling, shopping or day-trading

Information Overload – too much information makes processing the information and decision making difficult.

6.1.1   Social Media Addiction (Cyber relationship addiction)

Slide 5

Let's talk about Social Media Addiction (Cyber relationship addiction

Social media addiction is categorized as a psychological disorder in US. India is not very far behind in this. Here you want to spend all the time you have with online friends, than family members/Friends through chat rooms or social media sites

This results in

a) Less time with family and actual friends

b) Weakening of bonds b/w kid and family

c) Lesser social interaction resulting in weaker social skills

e) Anxiety over acceptance in your virtual world.

d) Project yourself as different person in online world than how you are in real world. This results in "loss of self" or "reduced self-awareness"

e) Getting cheated by fake profiles. Not everybody you meet online are real.

f) Make you uninterested about your studies.

https://www.youtube.com/watch?v=Vsq95M_kzWY

Slide 6

Describe the comic.

The child addicted of social media is concerned about losing her twitter account and is not concerned about her performance in the exam. The child who is not addicted, tries hard and is able to perform well in the exam, whereas the addicted child is not able to answer anything during exam.

How can we save ourselves and our friends and family from this??

6.1.1.1   Understand That You're Being Played

Heavy social-media habit isn't entirely your fault. All social media sites are been designed to make you repeatedly use them and check back in

6.1.1.2   Check with Purpose

Most of us wander onto social media aimlessly—usually when we're bored. To cut back, set a higher bar for logging on. Ask yourself, "D*o I have a specific, positive reason for this"?*

6.1.1.3   Be a Tough Editor

Before you post a status update or a photo, question your motive: Are you just trying to prove that you're having a good time? Posting a photo has the effect: You stop thinking about your experience and start contemplating other people's responses to it.

Respond Off-Line

When Facebook reminds you that it's your friend's birthday, wish him or her directly rather than posting on the wall. It will be more meaningful to the recipient.

Alter Your Settings

Disable all alerts and delete addicting apps

6.2   Excess Gaming Addiction

Slide – 7

All of you must be playing computer games. Those who are addicted often have a hard time taking breaks from playing. What starts with a time pass activity turns into a full time activity.

The gaming addiction follows different stages to the state of addiction. The activity first starts as a time pass and then the user realizes that it's a great stress buster and time pass. Soon the user is trying to improve his/her score again and again and finally reaches ultimate addiction stage where he/she doesn't want to do anything else.

Excessive gaming may have some or all of the symptoms of drug addiction or other proposed psychological addictions. Some players become more concerned with their interactions in the game than in their broader lives. Players may play many hours per day, neglect personal hygiene, gain or lose significant weight due to playing, disrupt sleep patterns to play resulting in sleep deprivation, play at work, avoid phone calls from friends, or lie about how much time they spend playing video games. In one extreme instance, it was reported that a seventeen-year-old boy would play for periods of up to 15 hours, skipping meals and only stopping when he blacked out.

6.2.1   Outcome of excessive playing

Slide - 8

- Excess playing time: This can affect people in education and performance in the workplace.

- Social isolation: A gamer who spends so much time alone with no human contact can become withdrawn and this will have a negative effect on their social skills.

- Cost: Gaming is a multi-billion dollar industry and the costs to the average gamer is rising all of the time. The costs also include electricity, internet costs and additional hardware costs required for gamin such as controllers.

- Separation from reality: Some gamers become so engrossed in games that they actually believe they are part of the virtual world in which the game takes place. Examples are people who have committed murders in the form of actions seen in games that they had become addicted to.

- Education: brain training, strategy and thinking skills are the benefits of gaming to help education. However gaming can also have a negative effect on the development of both children and young adults in society. Gamers have neglected their studies due to their immersion in games. The time spend playing games has effected the amount of time spent doing homework or in some cases actual attendances at school or college.

- Some video games teach kids the wrong values. Violent behavior, vengeance and aggression are rewarded. Negotiating and other nonviolent solutions are often not options. Women are often portrayed as weaker characters that are helpless or sexually provocative.

- Games can hurt and help children's attention issues — improving the ability to concentrate in short bursts but damaging long-term concentration.

- Video games may also have bad effects on some children's health, including obesity, video-induced seizures, and postural, muscular and skeletal disorders, such as tendonitis, nerve compression, carpal tunnel syndrome.

Some pointers for teachers and parents

- Monitor video game play the same way you need to monitor television and other media.
- Be a loving, attentive parent who disciplines your child well.
- Although playing video games can be a learning experience, give your kid a variety of entertaining things to learn from, so your kid will not be addicted to just one thing.   Be sure to make them read books, play sports, interact with other kids, and watch good TV. Everything should be taken in moderation.
- Consider limiting child's video game playing to an hour a day
- Monitor the effect of video games on your child. Observe his behavior. If it appears that he is becoming more aggressive with his siblings or friends during the period that he is playing violent games, stop him from playing the games
- Limit your child's video game playing when you see him spending less time doing homework and that he is getting lower grades.
- Limit your child's video game playing when you observe him having a sedentary lifestyle, and not engaging in sports and exercise.

- Limit your child's video game playing if he displays sign of addiction

What you need to look for in choosing a game

- Decide what is acceptable in your home and if you think violent games are not acceptable, don't go for it.
- Check the Ratings of the game before you buy it
- Consult your parents before buying any game.
- Pick games that require the player to come up with strategies, and make decisions in a game environment that is more complex than punching, stealing, and killing.
- Look for games involving multiple players to encourage group play.

Video helps https://www.youtube.com/watch?v=wNgGFJgNYOQ

6.3   Cybersex Addiction

Slide – 9

It has been estimated that 1 in 5 Internet addicts are engaged in some form of online sexual activity. With the increase usage of mobiles, there is an increasing tendency of sexting among teenagers. Studies confirm that the effect of pornography and drugs are same on brain.

Slide -10

- Routinely spending significant amounts of time in chat rooms and private messaging with the sole purpose of finding cybersex
- Engaging in explicit sex chat with other people online.
- Looking at amateur or professional pornography sites.
- Taking part in online pornography, for example by posting nude photos or posing for a webcam.
- Hiding your on-line interactions from your near ones.
- Feeling guilt or shame from your on-line use.

Many a times children by mistake views these porn sites and becomes long time viewers of such sites

Anonymity of online interactions that serves to increase the likelihood of the behavior, the **Convenience** of cyberporn and sexually-oriented chat rooms making it easily available to users, and finally, the **Escape** from mental tension derived from the experience which serves to reinforce the behavior leading to compulsivity.

And what is the outcome?

- Physical and mental health problems

- Tendency to commit sex based crimes

- Risk of teenage pregnancy

- Viewing woman as sex objects

- Depression

- Waste of time

How to avoid cybersex addiction

Again, the first and foremost step is to limit the time one spent online. If you must be online, try to do only essential activities such as email for work.

Block Sex sites. If possible, have a friend or loved one set the administrative password so that you can't change the settings.

Pursuing other activities. Choose one or more enjoyable activities, such as cooking, exercising, or reading, and plan to do them during the time you would have been online

Enlisting the help of friends and family. If you feel comfortable discussing your addiction, ask the people who care about you to help you quit

6.4   Depression

Slide - 11

Do you know, Teenagers who are addicted to the Internet are more likely to develop depression or other psychiatric problems than teens who are classified as normal Internet users

Individuals who can relate themselves to the Social Media Anxiety Disorder fear that interacting with people will give rise to the feelings like evaluation, judgments, inferiority and self-consciousness. It often leads to the feelings like depression, inadequacy and embarrassment.

The biggest problem with having the Internet is, its ability to create rifts between the real and virtual world. The virtual world can often seem so alluring that once hooked, going back to real life seems daunting and leads to depression.

The fear of not having internet also causes depression in many teenagers.

The excessive use of internet increases the chance of cyber bullying and this can cause the loss of self-esteem and confidence.

6.5 Physical Impacts of long term internet use

Slide - 12

Long term internet/media usage is leading to lack of physical activity/exercises. It also results in many postural disorders and other diseases. Listed below the physical risks

1. Risk of obesity

Lack of physical activity can lead to more fat storage in body there by resulting in obesity

Slide 13

2. Posture disorders

Working at a computer can cause back, neck and shoulder pains, headache, and eyestrain and overuse injuries of the arms and hands. You can help avoid computer-related injuries with proper furniture, better posture and good working habits. Parents should put sensible time limits on their children's computer use and video-game playing. Your child should take regular breaks from using a computer and should do some physical activities each other

Slide 14

3. Joint Pains

   The continuous use of computer causes pain in many joints and the reasons for this is:

   - Localized pressure. Direct pressure on nerves or tendons can cause damage in the long run. The wrist is one location of concern. The elbow (the funny-bone or crazy-bone nerve) is another.

- Use of force. Even small exertions can cause stress if small muscles are involved. Sudden, fast motions involving a jerk or snap.

- Holding one position. Muscles that hold a body part in position for long periods are more prone to fatigue than muscles that move a body part around.

4. Other disorders

As per research, some users are tend to epileptic seizures which subjected to video games.

Important Health Warning About Playing Video Games

Photosensitive Seizures
A very small percentage of people may experience a seizure when exposed to certain visual images, including flashing lights or patterns that may appear in video games. Even people who have no history of seizures or epilepsy may have an undiagnosed condition that can cause these "photosensitive epileptic seizures" while watching video games.

5. Eating disorders due to promotion of skinny ads in sites. Kids tend to eat less due to ads for becoming lean.

Slide 15

We can see here some of the common mistakes people do when using computer.

- Not keeping the screen on the eye level
- Not sitting properly in chair
- Keeping legs fixed in one position for long
- Hunching the shoulders
- Keeping the mouse and keyboard far
- Cradling the phone to the ear

You can also see the mistakes people do while using keyboard and mouse.

Slide 16

In this, you can see the right posture for using computer. What all we should take care?
- Monitor and eyes should be on the same level
- Feet should be comfortably positioned flat on the floor

- Keyboard and mouse should be on the same height level as the wrist
- Should be sitting straight
- Instead of cradling the phone, headphones should be used.

In this slide you can also see the correct way of using keyboard and mouse.

7   Cyber Threats and Laws

Slide-1/2

As the use of computer and internet is increasing, crimes related to internet are also increasing in our society. Here we will see what those common crimes are and how we can be safe from them.

7.1   Password Threats and misuses

Slide 2

The root cause behind many of the cybercrimes is misuse of passwords. Statistics show that at least 1 in 5 people are affected by high profile data breach or password leak.

For any account/user name you will definitely have password along with it. Passwords are the key to any website/portal. There are ways that your password is misused by others. Either you provide them your password (password sharing) or they find it out (password leak).

7.1.1   Password Leaks

Slide 3

Many a times you would have heard about mass passwords leaks happening in many famous sites. Have you ever thought who is behind is and how is this done?

Slide 4

Someone finding out your password by any means is known as password leak. The password leak can be accidental or caused by external agents.

7.1.1.1   By External Agents

1) Shoulder surfing-Spying on the user of a computer or ATM to obtain the password he type on the keyboard

2) Hacking-Someone from somewhere gain unauthorized access to your username/password/account

What should be done to escape from this?

- Always use strong passwords
- Enable 2 step authentication wherever possible
- Revoke access to third party apps

7.1.1.2   By Accidental human errors

Another major reason for password leak is careless use of passwords.

1) When you expose your passwords to others. E.g.: Noting down all the passwords in paper and sticking them near your system

2) By session or history in browser e.g.: When you are browsing in a cafe and you left the cafe just by closing the browser. The next person who browsers can get your password from history or will be taken to the same session which you logged in before. If you even save your password in browser, it helps another user to logging into your account.

3) Using default password of the website

To be safe from this, we need to ensure the following:

1) Never write down passwords
2) Don't use the same password across different sites
3) Never use common words as passwords
4) Never use personal information in password
5) Always log out and delete browsing history after accessing accounts from internet café.

7.1.2   PASSWORD SHARING

Slide -5

You sharing your password with anyone else is known as password sharing.

Sometimes you share your password with your friends in order to make your work easier. But you should never share your password to anyone even to your close family members.

You are responsible for your logon/password, if you let someone else use your password; you are responsible for what they do when logged in as you. Once you have given your password away, it is out of your control.

7.1.3   CONSEQUENCES OF PASSWORD LEAKS/SHARING

Slide -6

Many of you might be wondering what bad can happen if someone gets hold of your account information.

Imaging that it's the details for an e-commerce site where you have saved your card details or bank details for easy shopping. They can easily do a big purchase using your details.

Or imagine someone sending out illegitimate mails out of your inbox to your contacts; what will be the outcome of it?

1. Theft—your account information would be stolen
2. The information can be used to defraud the government or a private user and you would stand responsible.
3. Financial Problems-You can suffer from loss of money from your account
4. Sharing Password can be considered a crime. You can get punished for it.
5. Your reputation will be damaged. You will be exposed to society as someone who violated security rules.

Slide 7

To prevent misuse of passwords, as we discussed earlier always go for strong passwords. And one safest way to create strong password is to have passphrases.

7.2 Hacking

7.2.1 Hacking history

Slide 8

Do you know, originally, "hacker" did not carry the negative connotations now associated with the term? In the late 1950s and early 1960s, most companies used mainframe computers: which had high cost and time to maintain, and programmers had to fight for access. This led looking for ways to get the most out of the machines and started created what they called "hacks" - shortcuts that would modify and improve the performance of a computer's operating system or applications and allow more tasks to be completed in a shorter time.

Slide -9

We have white hat and black hat hackers. White hat hackers are ethical hackers who use their expertise to ensure the security of an organization's information systems by testing different loop holes where as

black hat hackers use their technical expertise to breach the security in the systems for little reason beyond maliciousness or for personal gain

7.2.2   How easy is it to break into my computer?

Slide -10

Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely.

Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

7.2.3   Easy to trace a hacker

Slide -11

But don't think that it's easy to escape after hacking/cracking. Cybercrime investigation is a full-fledged method now and use digital forensics to identify the criminals behind the hack. Like any crime, if the hacker is leaving even a small footprint, the investigators will be able to reach till the root.

The computer can be a source of evidence. Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigator. There are methods to identify the IP from which the intruder has connected to the system or website and once it is identified, with the help of ISPs the location and address is obtained. In most countries Internet Service Providers are required, by law, to keep their log files for a predetermined amount of time.

Mumbai police have arrested a hacker by name Kalpesh (name change) for hacking into a financial website. Although the hacker couldn't break into the main server of the financial institution, which was well secured by the financial institution. The accused person could make some addition to the home page

of the financial website and has added a string of text to the news module of the home page of the website. Police were able to crack the case by following the trace left by the hacker on the web server of the financial institution. The financial institution has maintained a separate server for financial online transactions, for which utmost security has been taken by the financial institution. The website was hosted on a different server which comparatively had lesser security.

The hacker Kalpesh (name changed) is a 10th Pass youngster of 23 years old. He has done computer courses like CCNA, MCSE etc. But he is a computer addict. He sits before the computer for almost 16 to 20 times each day. He has mostly used the readymade hacking tools, to hack into any website. He goes to a particular website on the web, which facilitates him to see the entire directory structure of that website. Then using various techniques, such as obtaining a password file, he gets into the administrator's shoes and hacks the website.

A case has been registered against the hacker under section 67 of Information Technology Act – 2000 and under various sections of Indian Penal Code.

7.2.4   Malware, spyware, Trojan horse and virus

Slide 12/13

You all must have heard the story of Trojan horse in Greek Mythology. Greeks intruded Troy city hidden inside a huge wooden horse and destroyed the city in night thus ending a long war between them.

In the same way, crackers use different tricks to trick the user into willingly running a malicious program.

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. There are several of the most common types of malware; spyware, Trojan horses, viruses, and worms.

Slide -14

A **Trojan horse**, commonly known as a "Trojan," is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, and even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc.), use the computer in botnets, and anonymize internet activity by the attacker.

Slide -15

Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans.

Slide -16

A **virus** is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

Rootkit - A **rootkit** is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed. Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it

Worms -A computer **worm** is a standalone **malware** computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program

Crime ware - Crime ware is designed to perform identity theft through social engineering or technical stealth in order to access a computer user's financial and retail accounts for the purpose of taking funds from those accounts or completing unauthorized transactions that enrich the cyber thief. Alternatively, crime ware may steal confidential or sensitive corporate information.

Adware - Adware is a type of software that is downloaded to your computer to show you advertisements. These advertisements may take many forms, from relatively noninvasive banners within a program, to very invasive pop-up windows that come up regardless of that you are doing in the foreground. Adware

often piggybacks on other program downloads that you do want. A lot of freeware's have adware associated with them. When you download freeware you are also downloading adware that is packaged with it. Sometimes adware will monitor the sites you visit and your computer habits to create a user profile. This user profile will be used to tailor the advertisements you see to your taste or narrow search results to fit your profile

------------------------------SUPPORTING DATA--

Ritu and the disappearing bank account: Ritu was a housewife and mother of two living in Hertfordshire, UK. One day, she was surprised to find her bank account balance a little lower than expected. When she checked her recent transactions, she discovered some withdrawals that she didn't make. The first ones were small, 10 or 20 pounds at a time. Within days the withdrawals grew to hundreds of pounds at a time.

She changed all her passwords and canceled her payment cards, but the unauthorized transfers didn't stop. She didn't know what to do- who do you turn to in a situation like this?

Don't let it happen to you: Your best bet is always to contact your bank or financial institution once you spot a problem. They will be able to reverse any unauthorized transactions and will do their best to prevent future ones. You should also try to find the root of the problem: maybe your email account has been compromised or your computer is infected. Contact your email provider and run a virus scan with the most up-to-date antivirus to track down the source of the problem.

How Sandra's browser exposed her to danger: Sandra, an HR professional, has been working desk jobs for over 10 years and has never had a problem in all her time behind a computer. Last summer the IT department at her office installed a critical update to her a computer, a patch for a newly discovered vulnerability in Internet Explorer.

Wanting to be sure that her computer at home didn't have the same vulnerability, she searched online for information about it. She discovered a website that detailed the vulnerability and offered a patch for it, but knowing never to download anything from an untrusted source, she opted out of the download and went to Microsoft's official site instead.

Unbeknownst to her, the original website she visited was bait for Internet Explorer users who still had the vulnerability. When she clicked "no" to opt out of downloading the patch, the website instead installed a key logger on her computer, which records everything she types. The next time she logged into her online banking, the key logger collected the name of her bank, her user ID, her password, the last four digits of

her Social Security number and her mother's maiden name. Several weeks later, her bank account was almost empty.

Don't let it happen to you: The best way to protect your computer is by keeping your antivirus software and your internet browsers up-to-date. Make sure to install the updates from the source and be extra vigilant on sites you're not familiar with.

Koby, a middle school instructor, wanted to sell his car on an online auction site to make a bit of extra cash. Within days of putting up the listing, he found a buyer and received payment without any problems, so he took the listing down. The next time he logged into his account, he noticed the listing was still up, except with one crucial difference: the email address was incorrect.

Koby knew something was 'phishy', and he came up with a plan. He emailed the "seller" pretending to be a potential buyer and collected the information for where to send the money. He then gave this information to the FBI, who promptly tracked down the fraudsters and arrested them. They had collected Koby's login information using a phishing email and reposted his listing in order to fraudulently collect payment from a gullible buyer for a car that wasn't theirs to sell.

Don't let it happen to you: Koby was lucky he spotted the signs of a phishing scam and was able to work with authorities to stop it. If you think someone has gotten access to your private information, contact the authorities immediately and give them as much information about the phishers as you can get.

The Koobface Gang: This last story didn't happen to just one person, it happened to more than 800,000 Facebook users around the world. These people received fake Facebook messages which installed a worm that infected and took over their computers. This worm, known as the Koobface computer virus, allowed a group of five men in St. Petersburg, Russia, to collect $10,000 dollars a day from their victims before the virus was discovered and shut down.

While their tools have been dismantled, nobody in the Koobface Gang has been arrested.

Don't let it happen to you: Learn the signs of phishing messages – even messages that come from your connections on social networks could be malicious. Hackers will take over accounts and send out spam to all of a person's connections hoping to land a victim or two.

So next time you think to yourself "I'm sure nothing bad will happen" remember the stories you've just heard. Remember how important it is to keep your browser, firewall and anti-virus protection always up to date and to never leave an opening for the criminals.

----------------------------------SUPPORTING DATA--

Most importantly, never share your personal information on any public page or with any website you don't trust.

7.2.5   Malware Symptoms

Slide -17

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

- Increased CPU usage

- Slow computer or web browser speeds

- Problems connecting to networks

- Freezing or crashing

- Modified or deleted files

- Appearance of strange files, programs, or desktop icons

- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)

- Strange computer behavior

- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)

7.3   Spam

Slide -18

Any unwanted messages, with commercial or otherwise content reaching your inbox is called spam.

Email spam

Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

Increasingly, e-mail spam today is sent via "zombie networks", networks of virus- or worm-infected personal computers in homes and offices around the globe. Many modern worms install a backdoor that allows the spammer to access the computer and use it for malicious purposes. This complicates attempts to control the spread of spam, as in many cases the spam does not obviously originate from the spammer.

An industry of email address harvesting is dedicated to collecting email addresses and selling compiled databases. Some of these address-harvesting approaches rely on users not reading the fine print of agreements, resulting in their agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam

SMS spam

Instant messaging spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, as instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging systems such as Skype.

Forum spam is the creation of advertising messages on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity; if a sale goes through, the spammer behind the spambot works on commission.

Social networking spam

Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family.

7.4 Phishing

Slide -19

7.4.1   What is Phishing?

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masked as a trustworthy entity in an electronic communication, usually an email.

Slide -20

So far the hackers have used **emails** to launch this type of attack, but with the widespread use of **social media networks** and **smartphones** with internet access, the **types of attacking** are multiplying. These emails include a link that takes the user to site known to have a confidential website, but they're mere mimics with zero confidentiality. Thus, overconfident users who do not have adequate **antivirus protection**, could be involved in attacks that are aimed to steal personal data.

And because of the economic crisis which is unfortunately affecting several countries, phishing attacks attracting people with the promise of a great job or an easy way to get money.

7.4.2   Phishing Mails

Slide 21

1: The message contains a mismatched URL

One of the first things we recommend checking in a suspicious email message is the integrity of any embedded URLs (or website addresses). Often the URL in a phishing message will appear to be perfectly valid. However, if you hover your mouse over the top of the URL, you should see the actual hyperlinked address. If the hyperlinked address is different from the address that is displayed, the message is more than likely fraudulent or malicious.

2: URLs contain a misleading domain name

People who launch phishing scams often depend on their victims not knowing how the DNS naming structure for domains works. The last part of a domain name is very important. For example, the domain name info.brienposey.com would be a child domain of brienposey.com because brienposey.com appears at the end of the full domain name (on the right-hand side). Conversely, brienposey.com.maliciousdomain.com would clearly not have originated from brienposey.com because the reference to brienposey.com is on the left side of the domain name.

This trick used countless times by phishing artists as a way of trying to convince victims that a message came from a company like Microsoft or Apple. The phishing artist simply creates a child domain bearing the name Microsoft, Apple, or whatever. The resulting domain name looks something like this: Microsoft.maliciousdomainname.com.

This often works because most people trust companies like "Microsoft" and "Apple" so when long standing names like this are used people often let their guard down. The lesson here is to never let your guard down when it comes to email messages.

3: The message contains poor spelling and grammar

Whenever a large company sends out a message on behalf of the company as a whole, the message is usually reviewed for spelling, grammar, and legality, among other things. So if a message is filled with poor grammar or spelling mistakes, it probably did not come from a major corporation's legal department.

4: The message asks for personal information

No matter how official an email message might look, it's always a bad sign if the message asks for personal information. Your bank does not need you to send it your account number. It already knows what that is. Similarly, a reputable company should never send an email asking for your password, credit card number, or the answer to a security question.

5: The offer seems too good to be true

If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.

6: You didn't initiate the action

If you get a message informing you that you have won a contest you did not enter, you can bet that the message is a scam.

7: You're asked to send money to cover expenses

One telltale sign of a phishing email is that you will eventually be asked for money. You might not get hit up for cash in the initial message. But sooner or later, phishing artists will likely ask for money to cover expenses, taxes, fees, or something similar.

Although most of the phishing scams try to trick people into giving up cash or sensitive information by promising instant riches, some phishing artists use intimidation to scare victims into giving up information. If a message makes unrealistic threats, it's probably a scam.

To summarize

1. Learn to Identify Suspected Phishing Emails

> There are some qualities that identify an attack through an email:
>
> They duplicate the image of a real company.
>
> Copy the name of a company or an actual employee of the company.
>
> Include sites that are visually similar to a real business.
>
> Promote gifts, or the loss of an existing account.

2. Check the Source of Information From Incoming Mail

3. Never Go to Your Bank's Website by Clicking on Links Included in Emails

4. Enhance the Security of Your Computer

5. Enter Your Sensitive Data in Secure Websites Only

6. Periodically Check Your Accounts and change Password.

7. Have the Slightest Doubt, Do Not Risk It.

8. Enable two factor authentication for you Bank accounts, Emails etc.

7.5 Pornography

Slide -22

Pornography is one of the main challenges the internet is facing today.

Dangers of Pornography

1. Addiction and health issues

The **effects of pornography** may differ from person to person and can impact sexual function or sexual relationships

2. Child Abuse

Lot of children all around the globe are dragged into this sin due to the Pornography.

3. It causes you to lose respect for women

The continual viewing of pornography promotes the degradation of women. Porn promotes the falsehood that women are objects with which to fulfill body pleasure.

4. It involves you in the crime of abusing women and children

When you view pornography, you contribute to its success and financially pave the way for its producers to go further and further into perversions that involve teen and child abuse.

5. It ruins careers and leads to job loss

When your mind is so absorbed in pornography, you lose the ability to concentrate on your work. While most companies forbid pornography use on the job, porn's continual use away from work will gradually take over your mind, leaving little room for things that matter.

6. It causes shame and self-deprecation

You cannot feel good about yourself when you are doing something you know is wrong. You have a conscience, and you will know you are doing something wrong when you view porn. That's when self-loathing sets in and self-respect plummets.

Protecting from Pornography

1. **Set your search engine to "safe search" mode:**

 For Google users go to http://www.google.com/familysafety/; if you child uses services like YouTube, be sure you have set the "safe" mode on those platforms as well.

2. **Use the family safety tools provided by your computers/other device's operating system:** Both Windows and Mac operating systems provide family safety settings.

3. **Set up an internet censor:**

   a. Use **StayFocused**. StayFocused is a browser add-on for Chrome browsers that allows you to control what websites you can access and how much time you can spend on those sites. It's great for policing your own behavior, if you're the one struggling with porn.

   b. Alternatively use **Stop Procrastinating App** that allows you to block internet access or filter websites on all web browsers, not just Chrome. It is impossible to get around and also offers users goal setting options to help them focus psychologically on breaking their addiction.

   c. Set up **OpenDNS** to block all objectionable content across all devices in your home. You can

set up the OpenDNS software, which is available for free, to block all objectionable content in your household. This is the program frequently used by schools and it functions very well for protecting your family.

7.6   Cyber terrorism

Slide 23

Tomorrow's terrorist may be able to do more damage with a keyboard than with Bomb.

Cyber terrorism is a phrase used to describe the use of internet based attacks in terrorist activities including acts of deliberate, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Examples of cyber terrorism:

- **The Original Logic Bomb**

  During the cold war in 1982, the CIA found a way to disrupt the operation of a Siberian gas pipeline of Russia without using traditional explosive devices such as missiles or bombs. Instead, they caused the Siberian gas pipeline to explode using a portion of a code in the computer system that controls its operation in what they tagged as "logic bomb." The chaos that ensued was so monumental that the resulting fire was even seen from space.

7.6.1   Features of Cyber Terrorism

- **Difficulty Identifying Attackers:** It remains difficult to determine the identity of the initiators of most of cyber-attacks.
- **Lack of Boundaries:**   Attack can originate from anywhere in the world and from multiple location simultaneously
- **Speed of Development:** The time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits the vulnerability is getting shorter.
- **Low cost of Tools:** The technology employed in attack is simple to use, inexpensive, and widely available.

7.7   Anti-Virus

Slide - 24

Antivirus or anti-virus software, sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.

How antivirus works:-

Antivirus software maintains a database of known viruses and compare scanned files against that match the characteristics of known viruses. If a scanned file matches those characteristics of known virus, it is moved to safe location in the system so that virus cannot spread to other location or execute any process.

Basic function of Antivirus:

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.
- Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer

Top 10 free antivirus software are

1. Avast! Free Antivirus
2. Panda Cloud Antivirus
3. Microsoft Security Essentials
4. Avira antivirus Personal Edition
5. AVG Anti-Virus Free Edition
6. Comodo Antivirus
7. Immunet Protect FREE
8. PC Tools Antivirus Free
9. Malwarebytes
10. ClamWin Free Antivirus

---SUPPORTING DATA---

Limitation of Antivirus:

- **Limited detection** - There's more than one way to detect a virus, but one big disadvantage to some antivirus programs is that they may not employ all detection techniques.
- **No 100% protection** - Having an antivirus program with multi-detection methods isn't enough. To

avoid viruses, Microsoft Security recommends putting up an Internet firewall as well. A firewall is usually a program that blocks the hackers, viruses and spyware on the Internet from getting into your computer. You can also use hardware -- like a router -- to reinforce the firewall, especially if you use more than one personal computer to access the Internet, or have a small network of computers.

- **Slow down PC -** Installing and running antivirus software can use up a lot of computer memory and hard disk space, slowing down your PC.
- **Conflicts -** If we have multiple antivirus installed, these programs may conflict with each other and may not work together.

---SUPPORTING DATA--

7.8   Prevention of cyber attacks

We are ending the session again with some precautions we need to take when online.

Slide 25

We all know that the Internet is a cool place to hang with friends and check out new things. But don't forget about the Internet's risks and dangers. If you're going to use the Web, do it safely! Here are some suggestions on what you should and shouldn't be doing online to help protect you against the bad stuff.

Be careful online.

Never reveal personally identifiable information online. A lot of creeps use the Internet to take advantage of other people, especially kids and teens. Never reveal any personally-identifiable information online, whether it's on your profile page or in a blog, chatroom, instant messenger chat or email.

• Always use a screen name instead of your real name.

• Never give out your address, telephone number, hangout spots or links to other websites or pages where this information is available.

• Be careful about sending pictures to people you do not know very well.

• Never tell people personal or private information about your friends or family.

• Never assume you're completely anonymous online. Even if you don't put personal information online, there are different ways that people can still figure out who you are and where you live.

Never share your password with other people (except for your parents).

Your passwords to websites, email accounts and instant messenger services should not be shared with friends or strangers. Your friends may not be as safe as you are and may unknowingly subject you to danger. You should, however, share your passwords with your parents if they ask so they can make sure you're using the Internet safely.

Never arrange meetings with strangers.

Just because you've seen a person's picture and read his or her profile, does not mean you know them. Many people online lie about who they are and what their intentions are. Just because someone seems nice online, does not mean they really are. They could be trying to hurt you. Never arrange a meeting with a stranger you've met online. Even meeting a stranger in a crowded place could be dangerous as he could follow you home. If you wish to meet an online friend in person, talk to your parents and arrange a time and place where your friend can meet your parents first, just in case. If you are worried about your parents meeting one of your online friends, you probably shouldn't be friends with them in the first place.

Don't believe everything you read or see online.

Be wary of everything you see online unless it is from a trusted source. People lie about their age, who they are, what they look like, where they live, how they know you and what their interests are. Also, a lot of websites and emails contain information that is misleading or just plain untrue. If a person or deal sounds too good to be true, it probably is. Ask your parents to help you figure out what information is really true.

Don't download files or software without your parents' permission.

There are a lot of files on the Internet that are unsafe to download to a computer. Some files will bombard you with pop-up ads all day long. Some files will actually track everything you and your family does on your computer, including your logins, passwords and credit card information, which criminals then use to steal money from you and do other harm. There is no easy way to tell which files are bad and which are ok to download. That free desktop wallpaper you want to download might also steal your parents' credit card information. Ask your parents before you download any files or software from the Internet.

Don't respond to inappropriate messages or emails.

Some people send inappropriate messages just to see if you will respond. If you do, you are simply encouraging them to send more inappropriate material to you. Don't respond to inappropriate messages. Instead, talk to your parents about how to report them to the right place.

Don't post inappropriate content.

If you post information about tennis, you will attract people who are interested in tennis. If you post inappropriate content or pictures, you will attract people who have inappropriate interests. If you post jokes, photos or other content that contain sexual references you will probably attract people who are only interested in talking about sex. Be mindful of what you are communicating to the rest of the online world through the content you put onto the Internet.

Be leery of personal questions from strangers.

People you don't know who ask personal questions are often up to no good. Don't continue communicating with strangers who ask your personal questions. Talk to your parents about how to block them from communicating with you and report them to the right place.

Don't be bullied into fights.

People tend to say things online that they would never say in person. Some people even say rude and malicious things, sometimes just to see if you will respond. Don't respond to these people. Instead, talk to your parents about how to block them from communicating with you and report them to the right place.

Don't use adult sites.

There are some websites that kids just should not use. Don't use websites that contain adult content or that facilitate communication with older adults. No matter how much you think you know about the Internet, there are some people and places you just aren't ready to deal with. Enjoy websites that are designed for people your own age.

Understand what you put online will be there forever.

Assume that everything you put online—- every email you write, every picture you post, and every blog or journal entry you post—- will be accessible on the Internet forever. Many search engines copy Internet

pages and save them for viewing even after the pages are no longer online. Think about that before you post anything online. Do you really want pictures or blog entries to be seen 10 years from now?

Use Strong Password

For each computer and service you use (e-mail, chatting, online purchasing, for example), you should have a password.

You shouldn't write them down nor should you share them with anyone, even your best friends.

Computer intruders use trial-and-error, or brute-force techniques, to discover passwords.

Use alphanumeric characters and special characters in your password.

The length of password should be as long as possible (More than 8 characters).

Do not write it to some place where it is visible to someone else.

Don't Use Free Wi-Fi

Open Wi-Fi networks are notorious dens of opportunity for hackers. When the cost of entry is zero, a hacker can return again and again to a lucrative pool of unsuspecting users logging into secure websites, sending messages to their friends or accessing Facebook. While it's true that, in theory, hackers can do the same things on paid networks, they're less likely to because staying on them costs time and money. Instead of using free networks, use proprietary ones, or even better, use a cellular connection.

Turn off Bluetooth When You're Not Using It

Unless you use a Bluetooth headset on a regular basis, you should keep Bluetooth off on your phone when it's in normal use. As with Wi-Fi, hackers can tap into this signal to pull data from your phone or install tools that can open it up for access. Instead, turn on Bluetooth only as needed.

Don't Click on Links in Unknown Texts

It should go without saying; just as with email, text messages from unknown people, particularly messages containing links, should be regarded with skepticism. If you don't recognize the number, you can try replying to the message for further details (scam text messages often generate an error when you try to reply to them), but its likely better to just discard it. Never give your personal information to someone you don't know.

Download apps only from official app stores like Apple's App Store or Google Play. The vast majority of rogue apps are found on unofficial app stores or websites, many based in China or Russia. Staying loyal to official marketplaces dramatically decreases the amount of malware users will ever encounter.

When evaluating third party apps for purchase, do some research on the developer and their **reputation**. Read user ratings, paying special attention to reviews from disgruntled users, and seek out app recommendations from reputable sources. On the other hand, help other users by giving feedback both good and bad to apps you have experienced.

7.9 Cyber Laws

India passed the Information Technology Act 2000 in May 2000 and notified it for effective on October 17, 2000. IT Act 2000 consists of 4 schedules 94 sections segregated into 13 chapters and focuses on providing legal recognition to e-commerce and on facilitating the filing of e-records with the government.

ITA 2008 is the amendment of IT Act 2000, it has added new sections on offenses including Cyber Terrorism and Data Protection. This amendment has been passed by the Parliament on 23rd December 2008 and came into force from October 27, 2009 onwards

7.9.1 Section 65: Tampering with Computer System Document

Whoever knowingly or intentionally conceals, destroys or alters any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

For the purposes of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

7.9.2 Section 66: Hacking

Imprisonment up to 3years or fine which extend up to 5 lakhs or both.

Section 66 A:

Punishment for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet

(This section was scrapped recently by SC of India)

Section 66 B: Receiving stolen Computer or communication devices

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66 C: Identity Theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66 D: Cheating by personation by using computer resources

Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66 E: Violation of Privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Section 66 F: Acts of Cyber Terrorism

(1) Whoever,—

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(*i*) Denying or cause the denial of access to any person authorised to access computer resource; or

(*ii*) Attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(*iii*) Introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

Commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.]

Section 67 A/67 B: Pornography

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

References : https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

http://cybercellmumbai.gov.in/html/write-ups/index.html

https://blog.payza.com/online-security/personal/4-spooky-cybercrime-stories/

http://www.govmu.org/portal/sites/cert/sid2012/Psychological%20Impact%20of%20Internet%20usage%20on%20Children.pdf

https://www.betterhealth.vic.gov.au/health/healthyliving/computer-related-injuries

http://www.amsro.com.au/amsroresp/wp-content/uploads/2015/10/WEBINAR-CASE-STUDIES-IS-Presentation-.pdf

8 Career Options

Some of the fields that support IT professionals include:

- Medicine

- Computers and Information Technology

- Finance and Banking

- Educational Services

- Military Defense

- Textiles

- Food Services

- Government

- Engineering

- Telecommunications

- Manufacturing

Some of the main designations in IT world are as follows:

- Computer Programmer: The stepping stone towards a more advanced career in IT. A computer programmer writes code to create software programs, and generally interact with software developers and engineers

- Quality Assurance Engineer: A Quality Assurance Engineer would be responsible to check whether the program developed by the computer programmer is the correct one or not.

- Computer Systems Analyst: A computer systems analyst is the glue between business and IT, helping organizations better understand their computer system's needs.

- Information Security Analyst: As cyber-attacks continue to increase, the roles and responsibilities of information security analysts continues to increase as well.

ⵌ Computer Information and Research Scientist: Many of these jobs require a Ph.D., as they deal with solving highly complex problems in the fields business, medicine, science, and others.

The minimum qualification for the above mentioned designations would be either BSc, BCA or B.Tech in any of the fields.

There is another option which is now a days increasingly become popular i.e. **freelancing.**

Freelancer is a person who works as a writer, designer, performer, or the like, selling work or services by the hour, day, job, etc., rather than working on a regular salary basis for one employer.

Freelancing can be done in following fields:

Travel Writer - you don't necessarily have to have training in this area just passion and a way with words!

Be a Teacher: One can take tutorials, videos or document the course content which can be used by people across the globe.

Photographer: If you have got skills in taking photos through a good camera or a phone. There are website where you can post it and even earn!

Sell products: Create your own products (it may vary from homemade delicacies to paintings) and sell them from your own website.

Genuine Job sites

There are a number of sites which gives right information about various IT and IT related jobs. Some are listed below

ww.Naukri.com

Timejobs.com

hiree.com

monstorindia.com

Every IT Company website will have direct Career page where we can directly register.

There are more options like government sites to search for central and state government jobs.

www.indgovtjobs.in is an example for the same.

Hoax Mails on Job Offers

There are many scams which aim at people who are looking for jobs. They achieve it by sending job offer e-mails from IDs which look alike the ones from famous companies. Mostly they will be demanding you to transfer an amount for covering your initial expenses and will be random; you might not even have attended any interview with this company or sent your CV to the company.

How Do I Recognize and Defend Against Spoof Emails?

Email hoax prevention is possible through education. Web users of all levels are encouraged to stay on top of continuously changing Internet and email security issues.

If you don't believe that the email is truthful, or that the sender is legitimate, then simply don't click on the link and type your email address. If there is a file attachment, simply don't open it, lest it contain a virus payload.

If you get an e-mail like this, you need to confirm its authenticity from the company mentioned. For that contact the company directly from the details provided in the official website of the company. Never use the contact details listed in the e-mail you received. Before confirming never share your documents or money. Please note, most of the reputed companies never ask for money along with the offer letter.

8.1   Preparing Curriculum Vitae

This sample resume has been designed to focus on:

- A marketing statement that highlights your capabilities and demonstrates what you bring to the job
- Personal attributes that will help you to transition into the work environment
- Any achievements, commendations or awards you received at high school that show you are honest and reliable
- Any volunteer placements that demonstrate your willingness to contribute to the community

Other things you can put on your resume include:

- Any sporting or community club participation (if relevant to the job)

- Work placements or work experience that show you know how to work in a professional environment

- Key skills that demonstrate your employability (and examples of their use)

- Written testimonials provided by supervisors, sporting club coaches, teachers or others involved in volunteer and community clubs

- Any hobbies or interests that are relevant to the job

Jayani Lal
Email: jayanilal@xmail.com.au
Mobile: XXXX XXX XXX

VCE graduate seeking casual employment in a dynamic organisation

Personable and astute student with proven time management and collaboration skills developed from sporting and volunteer engagements. Strong interpersonal skills enhanced by taking part in theatre activities to develop confidence and communication abilities. Understanding of general employability skills and the importance of working as part of a team, learning from others and developing as a professional. VCE graduate looking for first-time employment in a position that requires a dedicated, young and enthusiastic employee.

KEY SKILLS

Customer Service (phone and face-to-face)	Transaction processing	Store-based security
Problem solving	Sales refunds	Stock receipting
Cash management	Dispute resolution	End-of-day processing
Sales reconciliations	Data processing	Sales negotiations
	Inventory control	Product selection

Software Skills: Microsoft Word, Microsoft Excel, Microsoft Outlook, Firefox, Internet Explorer

EDUCATION

All Saints Anglican College
VCE
2013
ATAR: 88.7

Achievements

- **2013:** Class captain (in partnership with one other class representative)
- **2012:** Represented school at National Youth Day events
- **2012:** Recognition award for contribution to the local community and volunteering

PERSONAL ATTRIBUTES

- ✓ **Effective Communication Skills:** Articulate communicator with appreciation for the different communication styles required when working with other team members or with customers.

- ✓ **Honest and Reliable:** Strong morals and ethics ensure honesty, reliability and ability to undertake tasks responsibly.

- ✓ **Flexible:** Understanding of need to remain flexible to support last-minute demands and changes. Comfortable in changing environments and situations, ensuring ability to remain flexible and adaptable at all times.

STUDENT WORK EXPERIENCE PLACEMENTS

TAYLOR SMITH PARTNERS - RECEPTIONIST (2-WEEK WORK PLACEMENT)   2013

Achievements and Contributions

- **Customer Service:** Responded to incoming calls. Screened telemarketing and direct sales calls while transferring customer enquiries to appropriate department.

- **Administration:** Typed general communication and letters to customers and businesses as directed. Ensured accurate development of communication by providing correspondence to supervisor for approval.

- **Records Processing:** Entered customer information into internal records management system. Updated existing customer records while creating new data files as directed.

VOLUNTEER PLACEMENTS

St Vincent De Paul   2010 - 2013

Provided support during various fundraising activities for local community group. Assisted at events and gatherings including providing suggestions to help meet fundraising targets. Personally attended various events, including spending time with homeless youth in Melbourne CBD.

PROFESSIONAL REFEREES

Joanne Boyle	**Allan Blue**
Manager	Maintenance Manager
St Vincent De Paul Society	Melton Community Gardens
Phone XX XXXX XXXX	Phone: XX XXXX XXX

You can upload your CV in the job sites listed above and the interested employers will be contacting you, but beware of hoax mailers.