11 Societal Impacts

Outline

11.1 Introduction

We are now living an era called the information age where we see that most our activities are technology–influenced, be it making an online payment, creating or development of own piece of art or information (such as writing articles or clicking photographs and so forth). With the reach of technology to our day to day life, there has been a paradigm shift, and it has also raised specific issues and problems related to society, ethics and law. In this chapter, we shall talk about topics about this very domain such as intellectual property rights, plagiarism, cybercrime, cyberlaw, e-waste management etc.

11.2 Digital Footprint

Digital footprints are the records and traces individuals leave behind as they use the Internet.

Your interactions on social media, your friend circle on social media sites, sites you *visit, online purchases, locations visited through Facebook check-ins* etc. all make up your **digital footprints.**

DIGITAL FOOTPRINTS

"**Digital Footprints** are the records and traces individuals' activities as they use the Internet. Digital footprints are permanently stored."

A common comparison to digital footprints is the footprints you leave behind you when walk along a beach. Every step you take leaves an impression on the sandy surface that allows another person to see the marks that your activity has made and offers the possibility for them to follow your trail. Digital footprints are also referred to as "digital tattoos".

Digital footprints get created actively and passively. An **active digital footprint** includes data that you intentionally submit online, *e.g., Sending an email, sending messages online, posting a social media post, replying to post or commenting online* etc.

A **passive digital footprint** gets created through your data trail that you unintentionally leave online. For example, when you visit a website, the web server may log your IP address, which identifies your Internet service provider and your approximate location.

Unlike a beach footprint which will eventually fade away, the Internet – and any electronic 'event' in general – doesn't work the same way. It is safe to assume that anything you do, publish or post online may be there permanently and won't be 'washed away'.

Mistakes aren't as easy as they used to be because once we post anything online, it stays forever and cannot be undone, Digital Footprints last forever, and colleges and jobs will look back at them to see if you are what you portray and how you conduct yourself actually.

11.2.1 Managing Digital Footprint

In this age, your digital reputation is equally important, which is controlled by your digital footprint.

To manage your digital footprint, you can follow the guidelines given below :

1. **Know what your digital footprint is.** Look at all the social networking sites and forums that you belong to, and search your name to know what information about you is available.

2. **E-behave responsibly.** You should be smart and sensible enough to know which sites you are visiting, which emails you are sending, or what links you open. Also, make sure to never share your location when online. It is best to wait until you are home to share pictures of an event or activity on social media.

3. **Keep your digital footprint clean.** Carefully go through your social media handles, past browsing history on YouTube and other public sites and do the following :
   (*a*) remove any photos, content, and links that may be inappropriate
   (*b*) remove any details about you that reveal too much information like your phone number, school, college name, address etc.

4. **Control the visibility of your information.** Every web browser, social networking site offers options in their settings to control the visibility and access of your information.

Rather than making every browsing activity and post of yours ***Public***, you should be selective about who you authorize to access your information. It should be limited to only your known circle or the people you can trust upon (*private*), *e.g., Friends, or Friends of Friends, or your contacts* etc.

Thus, you should use the privacy features of your browser and of the various websites you frequent to reduce the visibility of your information.

5. **Allow Comments Moderation.** Since many comments on public websites can be publicly seen, monitor and moderate comments associated with you to maintain a positive digital footprint.

   Consider using the "**block comments**" feature or setting your social networking profile to "private" so that only designated individuals can view your information.

6. **Think before you post.** All the above mentioned steps are to control what has been done earlier. But if you are cautious and think before you post anything online, your digital footprint will be clean.

DIGITAL FOOTPRINT	
Be Careful About	**Be Smart About**
❖ What you share online ❖ Where you share ❖ With whom you share	❖ Sites you visit ❖ Emails you open ❖ Links you click

11.3 Net and Communications Etiquettes

The word **netiquette,** derives from the combination of words — **'net'** (internet) and **'etiquette'**. It refers to online manners while using Internet or working online. While online, you should be courteous, truthful and respectful of others. Following lines list basics rules of netiquettes.

1. **Refrain from personal abuse**. If you disagree to something, you may express robust disagreement, but **never** call them names or threaten them with personal violence.
2. **Never spam.** That is, don't repeatedly post the same advertisement for products or services.
3. **Write clearly and concisely.** On a site that has many non-native English speakers, avoid using slang they may not understand.
4. **Always post correct content in respectful language.** Remember that your posts are public. They can be read by your friends, your siblings, your parents, or your teachers.
5. **In a discussion forum, stick to the topic.** Don't post about football in a hair-care forum or about hair care in a gardening forum!
6. **Never expect other people to do your homework for you**. Never ask for or expect that your complete homework solution will be made available to you. Also, while asking for help, include details of what attempts you've made to solve the problem. It will save time and also show people that you are making an effort to help yourself.
7. **Do not post copyrighted material to which you do not own the rights.** It is plagiarism. If you need to use the copy righted material, then follow these rules :

   (*a*) Ask permission from the copyright holder.

   (*b*) Enclose the copyrighted information that you are using and cite its source.

Failing this will put you and the site in legal trouble.

11.3.1 Email Etiquettes

It is important that whether for business or personal use that we should follow the basics of email etiquettes. Following lines enlist some important email etiquette that everyone needs to be aware of and follow.

1. **Be concise and to the point.** Do not make an e-mail longer than it needs to be. A long e-mail can be very discouraging to read.
2. **Use proper spelling, grammar & punctuation.** It is important for conveying the message properly. Improper spelling, grammar and punctuation give a bad impression.
3. **Use proper structure & layout.** Since reading from a screen is more difficult than reading from paper, the structure and lay out is very important for e-mail messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.
4. **Do not write in CAPITALS (Case Sensitivity).** IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be highly annoying and might trigger an unwanted response. Therefore, try not to send any email text in capitals.
5. **Add an e-mail disclaimer.** Disclaimers in your internal and external mails can help protect you from liability if you inadvertently forwarded a virus by e-mail.
6. **Handle abbreviations and emoticons with care.** In business e-mails, use of abbreviations (such as BTW for by the way) and emoticons (smiley faces) is generally inappropriate.
7. **Gender Sensitivity.** If you are writing to a person unknown to you, your email should be gender neutral. That is, you should carefully not write or replace the *gendered nouns* with ***gender-neutral nouns***, *e.g.*, as shown in some samples below :

Gendered noun	Gender-neutral noun
man, woman	person, individual
mankind	people, human beings, humanity
man-made	machine-made, synthetic
the common man	the average (or ordinary) person
chairman	chair, chairperson, coordinator
mailman	mail carrier, letter carrier, postal worker
policeman	police officer
steward, stewardess	flight attendant
congressman	congress person, legislator, representative
Dear Sir:	Dear Sir or Madam:, Dear Editor:, Dear Service Representative:, To Whom it May Concern:

11.4 Ethical Issues

These days, we can easily say that our society is information society and our era is information era. As we all know that ***information*** *is the means to acquire knowledge*. In other words, we can say that *information forms the intellectual capital* for a person or body. However, there are many ethical issues involved with the usage and availability of information.

Some common ethical issues are :

(*i*) Intellectual property rights

(*ii*) Digital property rights

(*iii*) Plagiarism

11.4.1 Intellectual Property Rights

As mentioned earlier, information makes intellectual property. Any piece of information is produced or created with a lot of efforts and it consumes a lot of time. The cost factor is also involved with the creation or production of information. Though once produced, it becomes very easy to duplicate it or share it with others. But this very thing makes information difficult to safeguard unlike tangible property.

The creator/producer of the information is the real owner of the information. And the owner has every right to protect his/her intellectual property. To protect one's intellectual property rights one can get information *copyrighted* or *patented* or use *trademarks*.

NOTE

Intellectual property rights are the rights of the owner of information to decide how much information is to be exchanged, shared or distributed. Also it gives the owner a right to decide the price for doing (exchanging / sharing/distributing) so.

- **Copyright.** A copyright is a collection of rights automatically vested to someone who has created an original work. The copyright owner has the authority to keep or to transfer the rights to use/distribute, individually to one or more people, or to transfer them collectively to one or more people.
- When someone uses a copyrighted material without permission, it is called **copyright infringement**. Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder.
- **Patent.** A patent is a grant of exclusive right to the inventor by the government. Patents give the holder a right to exclude others from making, selling, using or importing a particular product or service, in exchange for full public disclosure of their invention.
- **Trademark.** A trademark is a word, phrase, symbol, sound, colour and/or design that identifies and distinguishes the products and goods of one party from those of others.

COPYRIGHT INFRINGEMENT

"**Copyright infringement** is the use or production of copyright-protected material without the permission of the copyright holder."

The ethical issue involved with it is that information must not be exchanged without the consent of its owner.

The intellectual property rights must be protected, for it :

- encourages individuals and businesses to create new software and new software applications, as well as improving existing applications,
- ensures new ideas and technologies are widely distributed,
- promotes investment in the national economy.

11.4.1A Digital Property Rights

Digital property (or **digital assets**) refers to any information about you or created by you that exists in digital form, either online or on an electronic storage device. All of your digital property comprises what is known as your ***digital estate***.

DIGITAL PROPERTY

> **Digital property** (or **digital assets**) refers to any information about you or created by you that exists in digital form, either online or on an electronic storage device.

Examples of digital property include : *any online personal accounts, such as email and communications accounts, social media accounts, shopping accounts, photo and video sharing accounts, video gaming accounts, online storage accounts, and websites and blogs that you may manage ; domain names registered in your name ; intellectual property, including copyrighted materials, trademarks, patents and any software or code (such as software tools created by you or games or apps created by you) you may have written and own etc.*

Digital property rights lie with the owner. Legally a person who has created it or the owner who has got it developed by paying legally is the legal owner of a digital property. Only the owner can use and decide who all and in what form can his/her digital asset may be used by other, whether by making payments or by buying it or by obtaining its license or usage rights etc. But this is not the case generally; there are many threats to digital properties.

Threats to Digital Properties

Let us briefly talk about common threats to digital properties :

1. **Digital software penetration tools.** Although one needs to buy usage rights or license to use a digital property, there are many software penetration tools such as *cracks* and *keygens*, tools created by hackers to penetrate your software's registration system and enable unauthorized users to freely access your software without actually paying for it.
2. **Stealing and plagiarizing codes of your digital properties.** Sometimes other developers somehow get hold of your software's source code and then create plagiarized versions of your code and use it in their own software. In other words, they steal your software's source code and use it to build their own versions of it, and then sell it under their own company name.

Digital Property Rights Protection

As there are multiple types of threats to digital properties, there are many ways you can ensure protection of your digital properties. Let us talk about these protective measures :

1. **Anti-Temper Solutions.** There are many anti-tamper solution available today which ensure that your digital property is tamper-proof. These anti-temper solutions use a host of advanced technologies to prevent hackers from hacking, reverse-engineering or manipulating your digital properties such as *utility tools, software, apps, video games* and so forth.
2. **Legal Clauses.** Add legal clause in the clauses of use of your software/digital properties. You must include a transparent clause in your software's *Terms of Service* that prohibits the scraping of your software's source code for reuse. This is a sound legal backup for you.
3. **Limit the sharing of software code.** You should share your software code only with trusted individuals who are part of development team. You should also use a Digital Rights Management (DRM) solution to protect your software from being scraped for source code using decompilers etc.

11.4.2 Plagiarism

Simply put, *Plagiarism* means *stealing*. Surprised? If you look into an English dictionary to find the meaning of word plagiarism, it will give somewhat like "the unauthorized use or close imitation of the language and thoughts of another author and the representation of them as one's own original work."

PLAGIARISM

"**Plagiarism** is stealing someone else's intellectual work and representing it as your own work without citing the source of information."

Thus, **Plagiarism** is stealing someone else's intellectual work (can be an idea, *literary work* or *academic work* etc.) and representing it as your own work without giving credit to creator or without citing the source of information.

Any of the following acts would be termed as Plagiarism :

- Using some other author's work without giving credit to the author.
- Using someone else's work in incorrect form than intended originally by the author/creator.
- Modifying/lifting someone's production such as *music-composition* etc. without attributing it to the creator of the work.
- Giving incorrect or incorrect source of information *i.e.*, wrongful citation.
- Failure in giving credit or acknowledging the contribution of others in a collaborative effort, to which you are also part of.

How not to Plagiarize ?

As most universities[1] put in their student-handbook. 'To avoid plagiarism :

You must give credit whenever you use

- another person's idea, opinion, or theory;
- quotations of another person's actual spoken or written words ; or
- Paraphrase of another person's spoken or written words.

Plagiarism is Offence

'If plagiarism involves copying not only ideas but also a substantial portion of a copyrighted work without attribution and without permission, it would amount to both copyright infringement and the violation of the 'special right' of the author to be credited.

Copyright infringement and the violation of an author's right to be credited are both civil wrongs and criminal offences. A civil suit may be instituted, and criminal charges may also be filed'[2].

Both civil suit and criminal charges are punishable offences and amount to fine and penalties.

11.5 Open Source Philosophy

Broadly the term '*open source software*' is used to refer to those categories of software / programs whose licenses do not impose much conditions. Such software, generally, give users freedom to run/use the software for any purpose, to study and modify the program, and to redistribute copies of either the original or modified program (without having to pay royalties to previous developers).

1. Found in most universities' guidelines for students/student-handbooks
2. www.mxmindia.com (interview of *Nandita Saikia*)

There are many categories of software that may be referred to as open source software. Following subsection is going to talk about the same.

11.5.1 Terminology

Before we talk about various terms and definitions pertaining to '**Open**' world, you must be clear about *two* terms which are often misunderstood or misinterpreted. These terms are :

- Free software and
- Open source software

Free Software

Free Software means the software is freely accessible and can be freely used, changed, improved, copied and distributed by all who wish to do so. And no payments are needed to be made for **free software**.

The definition of **Free Software** is published by *Richard Stallman's Free Software Foundation*. Here is the key text[3] of that definition :

> *"Free software" is a matter of liberty, not price. To understand the concept, you should think of "free" as in "free speech," not as in "free beer." Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it refers to four kinds of freedom, for the users of the software :*
>
> - *The freedom to run the program, for any purpose (**freedom 0**).*
> - *The freedom to study how the program works, and adapt it to your needs (**freedom 1**). Access to the source code is a precondition for this.*
> - *The freedom to redistribute copies so you can help your neighbour (**freedom 2**).*
> - *The freedom to improve the program, and release your improvements to the public, so that the whole community benefits (**freedom 3**). Access to the source code is a precondition for this.*
>
> *A program is free software if users have all of these freedoms.*

Open Source Software

Open Source Software, on the other hand, can be **freely used** (in terms of making modifications, constructing business models around the software and so on) but it ***does not have to be free of charge***. Here the company constructing the business models around *open source software* may receive payments concerning support, further development. What is important to know here is that in *open source software, the source code is freely available* to the customer.

11.5.2 Philosophy of Open Source

Open source software is officially defined by the **open source definition** at *http://www.opensource.org/docs/definition_plain.html*.

It states that :

> Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria :

3. **Excerpt courtesy** *Free Software Foundation*. **This keytext is available at** *www.gnu.org/philosophy/free-sw.html*.

Free Redistribution	No restriction on the re-distribution of the software whether as a whole or in part.
Source Code	The program must include source code, and must allow distribution in source code as well as compiled form.
Derived Works	The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.
Integrity of the Author's Source Code	The integrity of the author'source code must be maintained. Any additions / modifications should carry a different name or version number from the original software.
No Discrimination Against Persons or Groups	The license must not discriminate against any person or group of persons.
No Discrimination Against Fields of Endeavor	The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.
Distribution of License	The rights attached to the program must apply to all to whom the program is redistributed.
License must not be Specific to a Product	There must not be any restriction on the rights attached to the program, *i.e.*, there should not be a condition on the program's being part of a particular software distribution.
The License must not Restrict other Software	The license must not place restrictions on other software that is distributed along with the licensed software. *For example*, the license must not insist that all other programs distributed on the same medium must be open-source software.
Licence must be Technology Neutral	No provision of the license may be predicated on any individual technology or style of interface.

A software which is **free** as well as **open** belongs to category **FOSS** (*Free and Open Source Software*).

NOTE

The terms Free and Open represent a differing emphasis on importance of ***freedom*** (***free software***) or ***technical progress*** (open source software).

11.5.3 Definitions

After understanding the difference between the terms free and **open**, let us now proceed to our discussion on terminology and definitions pertaining to open source software.

OSS and FLOSS

OSS refers to *open source software*, which refers to software whose source code is available to customers and it can be modified and redistributed without any limitation. An OSS may come free of cost or with a payment of nominal charges that its developers may charge in the name of development, support of software.

FLOSS refers to *Free Libre and Open Source Software* or to *Free Livre and Open Source Software*. The term FLOSS is used to refer to a software which is both ***free software*** as well as ***open source software***. Here the words **libre** (a Spanish word) and **livre** (a Portuguese word) mean ***freedom***.

FSF

FSF is *Free Software Foundation*. FSF is a non-profit organisation created for the purpose of supporting free software movement. *Richard Stallman* founded FSF in 1985 to support GNU project and GNU licences. Now a days, it also works on legal and structural issues for the free software community.

GNU	GNU[4] refers to ***GNU's Not Unix***. GNU Project emphasizes on freedom. The GNU project was initiated by *Richard M. Stallman* with an objective to create an operating system. With time, GNU project expanded and now it is not limited to only an operating system. Now, it offers a wide range of software, including applications apart from operating system.
OSI	OSI is *Open Source Initiative*. It is an organisation dedicated to cause of promoting open source software. *Bruce Perens* and *Erics Raymond* were the founders of OSI, that was founded in February 1998. OSI specifies the criteria for open source software and properly defines the terms and specifications of *open source software*. Open source doesn't just mean access to the source code. The distribution terms of open source software must comply with the *Open Source Definition* by OSI.
Freeware	The term *freeware* is generally used for software, which is available free of cost and which allows copying and further distribution, but not modification and whose source code is not available. Freeware should not be mistaken for open software or for free software. Freeware is distributed in binary form (ready to run) without any licensing fee. In some instances the right to use the software is limited to certain types of users, for instance, for private and non-commercial purposes. One example is Microsoft Internet Explorer, which is made available as freeware.
W3C	W3C is acronym for *World Wide Web Consortium*. W3C is responsible for producing the software standards for world wide web. The W3C was created in October 1994, to lead the world wide web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. The World Wide Web Consortium (W3C) describes itself as follows : The World Wide Web Consortium exists to realize the full potential of the Web. The W3C is an industry consortium that seeks to promote standards for the evolution of the Web and interoperability between WWW products by producing specifications and reference software. Although industrial members fund W3C, it is vendor-neutral, and its products are freely available to all.
Proprietary Software	***Proprietary software*** is the software that is *neither open nor freely available*. Its use is regulated and further distribution and modification is either forbidden or requires special permission by the supplier or vendor. Source code of proprietary software is normally not available.
Shareware	***Shareware*** is software, which is made available with the right to redistribute copies, but it is stipulated that if one intends to use the software, often after a certain period of time, then a license fee should be paid. Shareware is not the same thing as *free and open source software* (FOSS) for two main reasons : (*i*) the source code is not available and, (*ii*) modifications to the software are not allowed. The objective of shareware is to make the software available to try for as many users as possible. This is done in order to increase prospective users' will to pay for the software. The software is distributed in binary form and often includes a built-in timed mechanism, which usually limits functionality after a trial period of usually one to three months.
Copylefted Software	Copylefted software is free software whose distribution terms ensure that all copies of all versions carry more or less the same distribution terms. This means, for instance, that copyleft licenses generally disallow others to add additional requirements to the software) and require making source code available. This shields the program, and its modified versions, from some of the common ways of making a program proprietary.

4. GNU is recrusive acronym for GNU's Not Unix. A recursive acronym is the one that uses its abbreviation in full form *e.g.*, VISA is also recursive acronym – VISA international service association.

11.6 Copyright and other Licenses

The Licenses are permissions given to use a product or someone's creation. *Copyright* is a related term, which you must know. *Copyright* defines the ownership rights. A **copyright** is a collection of rights that automatically vest to the creator of an original creative work such as *a literary work, a design, song, movie or software* etc. A copyright holder can give licenses to use its work in a specific way.

Let us talk about these terms in details.

Here, you should know about a related term, **Copyleft. Copyleft** is a license that gives rights opposite to copyright. The **Copyleft** offers users the right to freely distribute and modify the original work, but only under the condition that the derivative works be licensed with the same rights. Its symbol is also flipped copyright symbol.

(a) Copyright symbol

(b) Copyleft symbol

Figure 11.1

LICENSES

> Licenses are the permissions given to use a product or someone's creation by the copyright holder.

COPYRIGHT

> A copyright is a legal term to describe the rights of the creator of an original creative work such as a literary work, an artistic work, a design, song, movie or software etc.

Since Open Source software movement was started against the proprietary software licenses, let us now talk about various types of software licenses available in this domain.

11.6.1 Licenses and Domains of Open Source Technology

As per Open Source Initiative, "*Open source licenses are licenses that comply with the Open Source Definition — in brief, they allow software to be freely used, modified, and shared.*"

Open-source licenses make it easy for others to contribute to a project without having to seek special permission. It also protects you as the original creator, making sure you at least get some credit for your contributions. It also helps to prevent others from claiming your work as their own.

Broadly used open source licences are being given below for your reference.

1. GNU General Public License (GPL)

The GNU General Public Licence (GPL) is probably one of the most commonly used licenses for open-source projects. The GPL grants and guarantees a wide range of rights to developers who work on open-source projects. Basically, it allows users to legally copy, distribute and modify software. This means, with GPL, a user can :

Copy the software	Copy the software as many times as needed. There's no limit to the number of copies one can make.
Distribute the software however you want	There is no restriction of distribution methods and styles – can be in copied form or printed form or web-link form.
Charge a fee to distribute the software	After modifying the software, you can even charge for your software, explaining why you are charging them but the software should still be under GNU GPL.
Make whatever modifications to the software you want	You are free to make any kind of modifications to the GNU GPL software. The only catch is that the other project must also be released under the GPL.

2. GNU Lesser General Public License (LGPL)

There is another GNU license : the **Lesser General Public Licence (LGPL)**. It offers lesser rights to a work than the standard GPL licence. The LGPL is used to license *free software* so that it can be incorporated into both *free software* and *proprietary software*. The LGPL and GPL licenses differ with one major exception ; with LGPL the requirement that you have to release software extensions in open GPL has been removed.

Mostly, LGPL is used by libraries. LGPL is also called GNU libraries and formally called the Library GPL.

3. BSD License

BSD licenses represent a family of permissive free software licenses that have fewer restrictions on distribution compared to other free software licenses such as the *GNU General Public License*. There are *two* important versions of BSD licence :

the New BSD License/ Modified BSD License	The New BSD License ("3-clause license") allows unlimited redistribution for any purpose as long as its copyright notices and the license's disclaimers of warranty are maintained. The license also contains a clause restricting use of the names of contributors for endorsement of a derived work without specific permission.
the Simplified BSD License / FreeBSD License	The Simplified BSD license is different from New BSD License in the sense that the latter omits the non-endorsement clause.

4. MIT License

The MIT License is the shortest and probably broadest of all the popular open-source licenses. Its terms are very loose and more permissive than most other licenses.

The basic provisions of the license are :

- You can use, copy and modify the software however you want. No one can prevent you from using it on any project, from copying it however many times you want and in whatever format you like, or from changing it however you want.
- You can give the software away for free or sell it. You have no restrictions on how to distribute it.
- The only restriction is that it be accompanied by the license agreement. It basically says that anyone can do whatever they want with the licensed material, as long as it's accompanied by the license.

NOTE

The MIT License is the least restrictive open source license.

5. Apache License

The Apache License, grants a number of rights to users. These rights can be applied to both *copyrights* and *patents*. The Apache License offers :

Rights are perpetual	Once granted, you can continue to use them forever.
Rights are worldwide	If the rights are granted in one country, then they're granted in all countries.
Rights are granted for no fee or royalty.	There is up-front usage fee, no per-usage fee or any other basis either.
Rights are non-exclusive.	You are not the sole-licensee; other can also use the licensed work.
Rights are irrevocable	No one can take these rights away once they're granted.

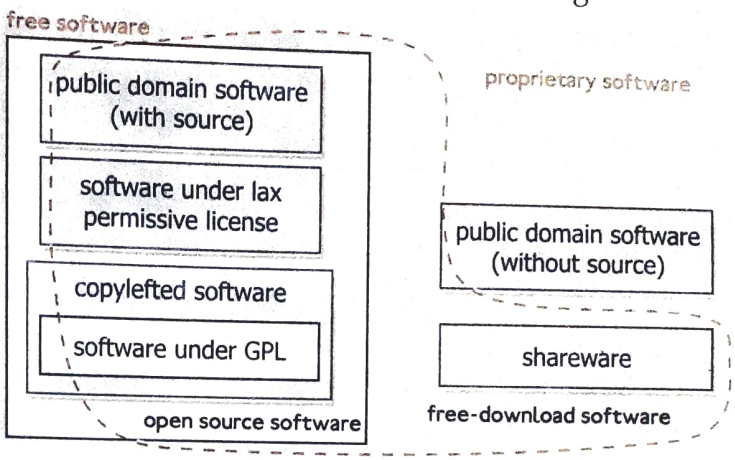
Redistributing code requires giving proper credit to contributors to the code and the same license (Apache) would remain with the software extension.

Public Domain Software vs. Proprietary Software

Public-domain software is free and can be used without restrictions. The term public-domain software is often used incorrectly to include freeware, free software that is nevertheless copyrighted. *Public domain software* is, by its very nature, outside the scope of copyright and licensing.

On the contrary, there is *Proprietary software*, which is neither free nor available for public. There is a proper license attached to it. User has to buy the licence in order to use it.

Consider the diagram (Fig. 11.2) originally made by *Chao-Kuei*[5] that describes the categories of software.



Figre 11.2 Categories and domains of software.

11.7 Cyber Crime

Cyber crime is any criminal offense that is facilitated by, or involves the use of, electronic communications or information systems, including any electronic device, computer, or the Internet. The term, **cyber crime**, is a general term that covers crimes like *phishing, credit card frauds, illegal downloading, industrial espionage, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and/or distribution of viruses, spam* and so on.

Some cyber crimes common these days are being discussed below :

> CYBER CRIME
>
> “ Any criminal offense that is facilitated by, or involves the use of, electronic communications or information systems, including any electronic device, computer, or the Internet is referred to as **Cyber Crime.** ”

Hacking

While working online, you often enter and create information related to you. You often enter information related to payments and even about your home address etc. while shopping. This information must be safe and must not fall into wrong hands. One should be careful while working online as there are many ways through which thieves can obtain your personal information.

One such way of doing it is ***hacking.*** **Hacking** a computer means, gaining unlawful entry in it. So a **hacker** is someone who gains unauthorised access to your network or computer or digital files, with an intention to steal or manipulate data or information or to install malware. Hackers exploit your computer/network security and employ techniques like, ***spoofing, phishing, social engineering*** etc. to capture user's personal or financial details.

> HACKING
>
> “ Hacking refers to gaining unauthorised access to a network or computer or digital files, with an intention to steal or manipulate data or information or to install malware. ”

Hacking can be ethical or unethical. **Ethical Hacking** is done on behalf of a company, which wants to find out the loopholes in the system in context to security. **Unethical Hacking**, on the other hand, is done in order to harm or cause loss to an individual or a company.

Spoofing

It refers to as a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a trusted source known to the receiver.

In spoofing attack, a hacker or malicious individual impersonates another user or device on a network, duping users or systems into believing they are legitimate or authentic.

Phishing

Phishing is the practice of attempting to acquire sensitive information from individuals over the internet, by means of deception. Information typically targeted by phishing schemes includes passwords, user-names, bank account information, and social security numbers. The term 'phishing' is a play on 'fishing' — hackers use various forms of 'bait' in order to catch a victim.

PHISHING

"**Phishing** is the practice of attempting to acquire sensitive information from individuals over the internet, by means of deception."

It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card information, account data etc. In Phishing, an imposter uses an authentic looking email or web-site to trick recipients into giving out sensitive personal information. For instance, you may receive an email from your bank (which appears genuine to you) asking to update your information online by clicking at a specified link. Though it appears genuine, you may be taken to a fraudulent site where all your sensitive information is obtained and later used for cyber-crimes and frauds.

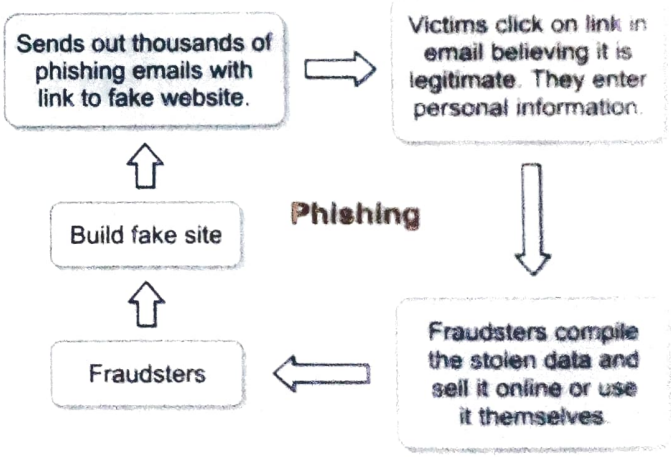


Figure 11.3 How Phishing attacks are carried out.

Social Engineering/Pretexting

They pose as a legitimate business or government officials to obtain your personal infor- mation from financial institutions, telephone companies, and other sources.

(ii) Cyber Trolls and Bullying

Cyber **troll** refers to a person who purposely posts opposing-, sarcastic-, demeaning- or insulting- comments about something or someone with an aim of targeting a person online. The provocative messages posted this way are also called **troll**. So the word *troll* can refer to a person also who is doing it and it may refers to the derogatory comments posted by a troll. Trolling is a cybercrime and is closely related to cyber bullying. In fact, it is a form of **cyber bullying**.

CYBER TROLLS

"Derogatory messages or comments posted online targeting people are called **cyber trolls**."

Cyber Bullying

Cyberbullying occurs when someone uses the Internet, a cell phone, email, instant messaging, chat rooms, or social networks, such as *Facebook*, *Twitter* etc., to harass, demean, embarrass, or intimidate someone else. It is commonly a crime committed by teens too, as their growing access to electronic communication makes it possible to make fun of or ostracize others.

The problem spreads like wildfire as the bully can hide behind the anonymity of a login identity, while encouraging other kids to join in the "fun" of harassing the victim.

Cyber bullying is a crime, garnering such criminal charges as harassment, libel, assault, and even terrorism. In addition to criminal charges, cyberbullies may be held responsible for the damage they do in a civil lawsuit, where they may be ordered to pay for it.

CYBER BULLYING

"Harassing, demeaning, embarrassing, defaming or intimidating someone using modern technologies like Internet, cell phones, instant messengers, social networks etc., is called **Cyber Bullying**."

Cyber Stalking

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

Cyber stalkers often do this to trouble their victims :

- They collect all personal information about the victim such as name, family background, telephone numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc.
- The stalker may post this information on any filthy/obscene or illegal websites posing as if the victim is posting this information.
- People of all kind from nook and corner of the World, who come across this information, start calling the victim at his/her residence and/or work place for many filthy/obscene reasons.
- Some stalkers subscribe the e-mail account of the victim to innumerable obscene or illegal sites because of which victim starts receiving such kind of unsolicited e-mails.
- Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
- Stalkers follow their victim from board to board. They "hangout" on the same social networking site as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed.
- Stalkers will almost always make contact with their victims through email having friendly or threatening content. The stalker many times uses multiple names when contacting the victim.

Scams

Any fraudulent business practice that extracts money from an unsuspecting, ignorant person is called a scam. These days, the Internet has become another primary source of scams. Scams committed over the Internet are called **online scams**.

An example on online scam is being given below :

"Mrinalini wanted to gift her friend a customized bracelet whose picture she saw of a photo sharing website that listed the design and cost of customization. Mrinalini, happily transferred an advanced payment of ₹2450 to the account mentioned on the site and was promised a date of delivery. But to her shock, the gift never arrived. Even after repeated calls, she only had a promise that it would be delivered soon and suddenly that website account was deleted from the photo sharing website and even the numbers went dead."

This is one example of the common cyber
happen to unsuspecting customers.

practice that extracts
from an unsuspecting, ign
person is called a **scam**.

Measures to avoid Online Scams

Important things to keep in mind while using the Internet to avoid scam include the following :

(*i*) Never enter personal information or any financial information (banking informatio credit/debit card information) on unsecure websites, *i.e.*, the sites that do not em HTTPS and do not have padlock sign.

(*ii*) Never reply to emails from any unknown or unreliable source.

(*iii*) Never click on any links that you have received in your email, even if you know sender. Rather open a browser window and type the url yourself than clicking on link in the email.

(*iv*) Never respond to an e-mail or advertisement claiming you have won something.

(v) Illegal Downloads

Illegal downloading refers to obtaining files for which you don't have the right to use download from the Internet. It is downloading a paid digital item, without making payment and using an illegal way to download it.

For example, if you are downloading a movie which is not available for free download, thi illegal download. Similarly, downloading a copy of the licensed software bypassing the le measures is also illegal download.

Most items that are protected under copyright law are available against a payment. Violati this is known as illegal download. For example, a movie or a photograph or a video etc. copyrighted in the favour of the creator/owner/producer.

A product is protected by copyright law cannot be downloaded, copied, reproduced or resc without their permission.

(vi) Child Pornography

Child pornography is defined as any visual or written representation (including image movies and/or texts) that depict or advocate sexual activity (including sexual molestation exploitation) of anyone under the age of 18. The law also includes some child nudity, simulate sex involving children and any material that is computer-doctored to look like child porn.

Information Technology Act, 2000 & Indian Penal Code, 1860 provides protection from chil pornography. Child is the person who is below the age of 18 years.

According to the new (amended) Information Technology Bill, Section 67 has been amended that **not only creating and transmitting obscene material in electronic form but also t browse such sites is an offence**.

11.8 Cyber Law and IT Act

Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any lega aspects or issues concerning any activity of netizens and others, in Cyber space comes within

the ambit of Cyber law. The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law.

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace.

India's IT Act and IT (Amendment) Act, 2008

In India the cyber laws are enforced through **Information Technology Act, 2000** (*IT Act 2000*) which was notified on 17 October 2000. It is based on the United Nation's Commission for International Trade related laws (UNCITRAL) model law.

IT ACT 2000's prime purpose was **to provide legal recognition to electronic commerce** and to facilitate filing of electronic records with the Government, *i.e.*, to provide the legal infrastructure for e-commerce in India.

The Act was later amended in December 2008 through the **IT (Amendment) Act, 2008**. It provided additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Data Protection. **The Information Technology Amendment Act, 2008** (IT Act 2008) came into force from October 27, 2009 onwards. Major amendments of IT ACT (2008) included :

Digital Signatures	Authentication of electronic records by digital signatures gets legal recognition.
Electronic governance	E-Documents get legal recognition. Documents required as per law by any arm of the government may be supplied in electronic form.
Offences and Penalties	The maximum penalty for any damage to computers or computer systems is a fine up to ₹1 crore.
Amendments to other laws	Other related acts such as the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891, the Reserve Bank of India Act, 1934 were to be amended to align them with the IT Act.

11.9 E-Waste Management

Electronic waste, e-Waste, e-Scrap, or **Waste Electrical and Electronic Equipment** (WEEE) describes discarded electrical or electronic devices. "Electronic waste" may also be defined as discarded computers, office electronic equipment, entertainment device electronics, mobile phones, television sets and refrigerators. This includes used electronics which are destined for reuse, resale, salvage, recycling, or disposal.

Of all the different types of waste, electronic waste has the characteristics of :

(*a*) the fastest growing segment of waste

(*b*) most valuable due to its basic composition

(*c*) very hazardous if not handled carefully

11.9.1 E-Waste Disposal Process

E-Waste is categorised by the government of India under the broad class of hazardous waste. Within e-Waste, there are several categories such as Large and small household appliances, electrical and electronic toys and sporting equipment, tools, computers and related equipment and so forth.

Composition of e-waste. Electrical and Electronic equipment contains metallic and non-metallic elements, alloys and compounds such as Copper, Aluminum, Gold, Silver, Palladium, Platinum, Nickel, Tin, Lead, Iron, Sulphur, Phosphorous, Arsenic etc.

The E-waste management involves proper recycling and recovery of the disposed material. The recycle and recovery includes the following unit operations.

1. **Dismantling.** Removal of parts containing dangerous substances (CFCs, Hg switches, PCB); removal of easily accessible parts containing valuable substances (cable containing copper, steel, iron, precious, metal containing parts).
2. **Segregation of ferrous metal, non-ferrous metal and plastic.** This separation is normally done in a shredder process.
3. **Refurbishment and reuse.** Refurbishment and reuse of e-waste has potential for those used electrical and electronic equipments which can be easily refurbished to put to its original use.
4. **Recycling/recovery of valuable materials.** Ferrous metals in electrical are furnaces, non-ferrous metals in smelting plants, precious metals in separating works.
5. **Treatment/disposal of dangerous materials and waste**. Shredder light fraction is disposed off in landfill sites or sometimes incinerated (expensive), chlorofluoro-carbons (CFCs) are treated thermally, Printed Circuit Board(PCB) is incinerated or disposed off in underground storages, Mercury(Hg) is often recycled or disposed off in underground landfill sites.

NOTE

IMPORTANT. Before discarding your laptop, desktop, or smartphone (*i.e.*, the e-waste), make sure to permanently delete all data and information from its storage. Otherwise this information may get stolen and may pose bigger threat through its misuse.

11.9.2 Benefits of e-Waste Recycling

The e-Waste disposal and proper recycling is very much necessary and important for the benefit of people, environment and the nation. The key benefits are :

1. **Allows for recovery of valuable precious metals.** Most consumer electronics contain valuable materials like copper, gold and zinc that can and should be recycled. Virgin Materials are significantly more costly than recycled materials for manufacturing.
2. **Protects public health and water quality.** E-waste contains a variety of toxic substances, which may include lead, mercury and cadmium. When e-waste is disposed into landfills, these toxins can be released into the atmosphere or leak in through the land and have negative health and environmental effects.
3. **Creates Jobs.** Recycling e-waste domestically creates jobs for professional recyclers and refurbishers and creates new markets for the valuable components that are dismantled.
4. **Toxic Waste.** Mining produces toxic waste, which are linked with crop devastation and human health crisis due to water contamination.
5. **Saves landfill space.** E-waste is a growing waste stream. Recycling these items will help conserve landfill space.

11.10 Health Concerns with Technology Usage

Although technology has improved our lives enormously yet it should be used in modera amounts. Excessive use of technology, such as *smart phones, computers, online gaming, social medi* etc. leads to many health related problems. In the following lines we are discussing major healt concerns related to excessive technology usage :

1. Impact on Hearing

Studies have proven that listening to music that loud for more than 15 minutes cause hearin damage over time. Also, it has been said that using headphones increases the bacteria levels i your ears over 700 times when used for more than an hour. This shocking statistic came from study way back in 1992 when experts measured bacteria on 20 headsets.

2. Impact on Bones and Joints

Use of technology has affected our postures. Most of the times, we sit in the same postures and make similar, repetitive movements, *e.g.*, thumb movements on mobile phones. Slouching, or using your joints and muscles in repetitive movements all cause strain on our muscles and joints. A **Repetitive Strain Injury (*RSI*)** is an injury or disorder of the muscles, nerves , tendons, ligaments and joints.

NOTE

A **Repetitive Strain Injury (*RSI*)** is an injury or disorder of the *muscles, nerves, tendons, ligaments* and *joints*.

3. Eye Problems

Constant exposure to smart phone, laptops and computer screens impacts our vision and may lead to other eye related problems. The blue light that comes from our phones and computers is very damaging on the retina, even more than UV light; this may even lead to vision loss. **Computer Vision Syndrome (CVS)** is a technology related health condition affecting eyesight.

NOTE

Computer Vision Syndrome (CVS) is a technology related health condition affecting eyesight.

4. Sleep Issues

Excessive smartphone, computer and tablet use can disrupt our sleep. Bright lights from these devices block melatonin secretion, the hormone that regulates sleep and this leads to smaller sleep cycles and disrupted sleep. Sleep is so essential for overall health that it impacts our normal *thinking and behavioural patterns, memory and attention span.*

5. Mental Health Issues

Excessive use of technology leads to isolation as people don't get time to physically socialise. It sometimes also leads to anxiety and depression as by looking at picture perfect social media profile of others, people often tend to think that their "connections" have "perfect rosy lives" while they are not.

Excessive use of technology and Internet leads to addiction. People keep obsessively looking through emails and messages. They start feeling stress if they don't get some likes or replies on their posts etc. This problem is formally termed as ***Internet addiction disorder***.

Check Point 11.1

1. What is digital footprint ?
2. What is IPR ?
3. What is plagiarism ?
4. What is FOSS ?
5. How is freeware different from free software ?
6. What are open source licences ?
7. What is hacking and spoofing ?
8. How is e-waste disposed and recycled ?

Following infobox talks about ***Internet addiction Disorder*** in details.

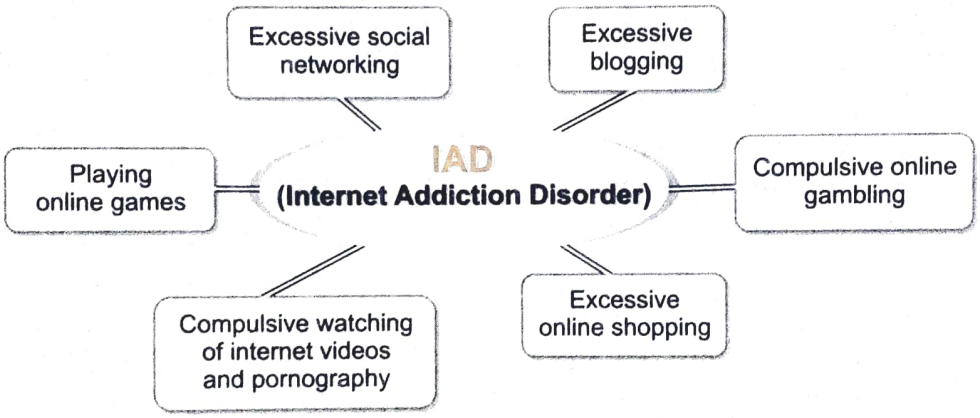
Internet Addiction

Internet addiction is a specific type of disorder, an impulse control disorder, whereby one uses Internet impulsively and compulsively. When someone uses Internet excessively on social media, blogs, online gaming, porn etc., this poses a great to the person's mental health. Such a condition is termed as **Internet addiction** by doctors.

Persons who have Internet addiction exhibit feelings of restlessness, moodiness, depression, or irritability when attempts are made by the family to cut down use of the Internet.

IAD

"When a person can't find a balance between their time online and their time offline, it considerably affects their mental health, this condition is called **Internet addiction** or **Internet Addiction Disorder** (IAD)."



Internet addiction results in many problems in the affected person, such as :

- One suffers from personal, family, academic, financial, and occupational issues, just like these happen in other types of addictions.
- Real life relationships (both personal and professional) get disrupted.
- Sufferer becomes socially awkward.
- Sufferer starts lying about the time spent on the Internet and avoids interaction with people around.
- Sufferer's changed habits and behaviour leads to loss of trust in the people or relations around him, and it leads to more loneliness.

How to Overcome Internet Addiction?

To overcome Internet addiction, one needs the help of a qualified doctor, counsellor and of course the family support. Other than doctor and counsellor's assistance, family support is crucial, for the family need to know how the sufferer may exhibit the withdrawal symptoms and how the family needs to react towards them.

When a person is trying to come out on Internet addiction, he/she may experience withdrawal symptoms like :

- **Mental and emotional symptoms.** Anger, depression, relief, mood swings, anxiety, fear, irritability, sadness, loneliness, boredom, restlessness, procrastination.
- **Physical symptoms.** An upset stomach, eating irregularities, (such as skipping meals), severe headaches, backaches, dry eyes, ignoring personal hygiene, and sleep disturbance.

Thus, for Internet addiction, a person needs timely help of qualified doctor, counsellor and family.

LET US REVISE

- *A digital footprint is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services.*
- ***Intellectual property rights** are the rights of the owner of information to decide how much information is to be exchanged, shared or distributed ; and to decide the price for doing (exchanging/sharing/distributing) so.*
- ***Plagiarism** is stealing someone else's intellectual work and representing it as your own work without giving credit.*
- ***Digital property** (or **digital assets**) refers to any information about you or created by you that exists in digital form, either online or on an electronic storage device.*
- *OSS refers to Open Source Software, which refers to software whose source code is available to customers and it can be modified and redistributed without any limitation. An OSS may come free of cost or with a payment of nominal charges that its developers may charge in the name of development, support of software.*
- *FLOSS refers to Free Libre and Open Source Software or to Free Livre and Open Source Software. The term FLOSS is used to refer to a software which is both **free software** as well as **open source software**. Here the words **libre** (a Spanish word) and **livre** (a Portuguese word) mean **freedom**.*
- *Phishing is the practice of attempting to acquire sensitive information from individuals over the internet, by means of deception.*
- *Hacking refers to gaining unauthorised access to a network or computer or digital files, with an intention to steal or manipulate data or information or to install malware.*
- *Licenses are the permissions given to use a product or someone's creation by the copyright holder.*
- *A copyright is a legal term to describe the rights of the creator of an original creative work such as a literary work, an artistic work, a design, song, movie or software etc.*

Objective Type Questions — OTQs

Multiple Choice Questions

1. A software that can be freely accessed and modified is called _____ .
   (a) Synchronous Software (b) Package Software
   (c) Open Source Software (d) Middleware
2. Data which has no restriction of usage and is freely available to everyone under Intellectual Property Rights is categorised as : [CBSE D 20C]
   (a) Open Source (b) Open Data
   (c) Open Content (d) Open Education
3. Which of the following is an advantage of 'open source' software ?
   (a) You can edit the source code to customise it.
   (b) You need to be an expert to edit code.
   (c) You have to pay.
   (d) Can sometimes be too generic for specialist purposes.
4. Which of the following is a disadvantage of 'open source' software ?
   (a) High quality software with lots of features

(*b*) Not as customizable

(*c*) May not have been tested as much as proprietary software, so might have bugs.

(*d*) You can edit the source code to customise it

5. Which of the following is an advantage of 'proprietary' software ?

(*a*) It is usually free.

(*b*) Thoroughly tested because people are paying to use it.

(*c*) Not as customizable

(*d*) Can sometimes be too generic for specialist purposes

6. Which of the following is a disadvantage of 'proprietary' software ?

(*a*) You need to be an expert to edit code.

(*b*) You have to pay for this type of software.

(*c*) It's licensed.

(*d*) It is launched after proper testing.

7. The generally recognized term for the government protection afforded to intellectual property (written and electronic) is called _____ .

(*a*) computer security law

(*b*) aggregate information

(*c*) copyright law

(*d*) data security standards

8. Which of the following would be a creative work protected by copyright ?

(*a*) A list of all Indian President names

(*b*) A portrait of your family

(*c*) A song you wrote

(*d*) The name of your pet dog

9. Which of the following is not a type of cybercrime ?

(*a*) Data theft

(*b*) Forgery

(*c*) Damage to data and systems

(*d*) Installing antivirus for protection

10. Which of the following is not done by cyber criminals ?

(*a*) Unauthorized account access

(*b*) Mass attack using Trojans as botnets

(*c*) Email spoofing and spamming

(*d*) Report vulnerability in any system

11. What is the name of the IT law that India is having in the Indian legislature ?

(*a*) India's Technology (IT) Act, 2000

(*b*) India's Digital Information Technology (DIT) Act, 2000

(*c*) India's Information Technology (IT) Act, 2000

(*d*) The Technology Act, 2008

12. What is meant by the term 'cyber-crime' ?

(*a*) Any crime that uses computers to jeopardise or attempt to jeopardise national security

(*b*) The use of computer networks to commit financial or identity fraud

(*c*) The theft of digital information

(*d*) Any crime that involves computers and networks

13. What is an example of e-waste ?
(a) a ripened banana
(b) an old computer
(c) old clothes
(d) empty soda cans

14. An organisation purchases new computers every year and dumps the old ones into the local dumping yard. Write the name of the most appropriate category of waste that the organisation is creating every year, out of the following options :
(a) Solid Waste
(b) Commercial Waste
(c) E-Waste
(d) Business Waste [CBSE D 20C]

15. A software company purchases new computers every year and discards the old ones into the local dumping yard. Write the name of the most appropriate category of waste that the organisation is creating every year, out of the following options :
(a) Business Waste
(b) Commercial Waste
(c) Solid Waste
(d) E-Waste [CBSE D 20C]

16. The rights of the owner of information to decide how much information is to be shared/exchanged/distributed, are collectively known as _____ (IPR).
(a) Intelligent Property Rights
(b) Intellectual Property Rights
(c) Interactive Property Rights
(d) Instance Property Rights

17. Stealing someone else's intellectual work and representing it as own, is called _____ .
(a) Intellectual steal
(b) Pluckism
(c) Plagiarism
(d) Pickism

18. The information/art/work that exists in digital form is called _____ .
(a) *e*-work
(b) *e*-asset
(c) digital property
(d) *e*-property

19. Every activity you perform on the Internet is saved for how long ?
(a) one month
(b) one year
(c) as per my setting
(d) forever

20. The digital trail which gets created as a person's Internet usage using computers, smartphones, gaming consoles etc. is called _____
(a) Internet data
(b) Internet trail
(c) Digital footprint
(d) *e*-footprint

21. Gaining unauthorised access to a network or computer or digital files with malicious intentions, is called _____
(a) Cracking
(b) Hacking
(c) Banging
(d) Phishing

22. Legal term to describe the rights of a creator of original creative or artistic work is called _____
(a) Copyright
(b) Copyleft
(c) GPL
(d) none of these

Fill in the Blanks

1. OSS stands for _____ .
2. Any fraudulent business practice that extracts money from an unsuspecting, ignorant person is called a _____ .

3. _____ is stealing someone else's intellectual work and representing it as your own without giving credit.
4. Any work/information that exists in digital form either on Internet or on an electronic device, is known as _____ property.
5. Discarded electrical or electronic devices are known as _____ .
6. The least restrictive open source license is _____ license.
7. The original code written by programmers for a software is known as _____ .
8. _____ means no price is to be paid for the software.
9. _____ _____ means freedom to use the software.
10. IAD means _____ _____ _____ .
11. The _____ _____ is the digital trail of your activity on the Internet.
12. The _____ are the permissions given to use a product or someone's creator by the copyright holder.
13. _____ is a license that gives rights opposite to copyright.
14. The practice of taking someone else's work or ideas and passing them off as one's own is known as _____ . [CBSE Sample Paper 2020-21]
15. A _____ _____ _____ is an injury or disorder of the muscles, nerves, tendons, ligaments and joints.
16. _____ _____ _____ is a technology related health condition affecting eyesight.

True/False Questions

1. Open Source Software can be used for commercial purposes.
2. It is okay to copy and paste information from the Internet into your report then organize it.
3. Shareware software allows you to try the software before you buy it.
4. Freeware is copyrighted software that is freely available to use.
5. Cyber-laws are incorporated for punishing all types of criminals only.
6. Deceptively attempting to acquire sensitive information of someone else using online means, is a cybercrime.
7. Freeware and free software mean the same thing.
8. Excessive use of Internet and social media is termed as a disorder.
9. Digital footprint can be deleted.
10. Digital footprint remains forever.
11. It is safe to make all one posts public on social media.
12. Hacking is performed to help find the security loopholes.
13. If you post something mean about someone, you can just delete it and your activity will be undone.
14. Hacking is a cybercrime.
15. Copyright is the right of the creator of creative/artistic work.

NOTE : Answers for OTQs are given at the end of the book.

Solved Problems

1. *What is digital footprint ?*

Solution. A digital footprint is the record or trail left by the things one does online. The social media activity, the information on personal website, the browsing activities, online subscriptions, any photo galleries and videos uploaded by a user — essentially, any activity carried out on the Internet makes the digital footprint of a user.

2. *Why is it important to have positive digital footprint ?*

Solution. It is very important to have a clean and secure digital footprint because :

- It gives us a digital persona by defining our online behaviour.
- The digital footprint is often used by universities before approving admissions to a student.
- The digital footprint is also used by future employers, and law enforcement offices, to find people with positive and clean digital footprint.
- The digital footprint should not provide personal information as it could be misinterpreted or misused for theft of identity.

3. *What are intellectual property rights ?*

Solution. **Intellectual property rights** are the rights of the owner of information to decide how much information is to be exchanged, shared or distributed. Also it gives the owner a right to decide the price for doing (exchanging/sharing/ distributing) so.

4. *Why should intellectual property rights be protected ?*

Solution. The intellectual property rights must be protected because protecting them

- encourages individuals and businesses to create new software and new software applications, as well as improving existing applications,
- ensures new ideas and technologies are widely distributed,
- promotes investment in the national economy.

5. *What do you understand by plagiarism ? Why is it a punishable offence ?*

Solution. Plagiarism is the act of using or stealing someone else's intellectual work, ideas etc. and passing it as your own work. In other words, plagiarism is a failure in giving credit to its source. Plagiarism is a fraud and violation of Intellectual property rights. Since intellectual property holds a legal entity status, violating its owner's right is a legally punishable offence.

6. *What is digital property ? Give some examples of digital properties.*

Solution. Digital property (or digital assets) refers to any information about you or created by you that exists in digital form, either online or on an electronic storage device.

Examples of digital property include : **any online personal accounts (email/social media accounts/ shopping accounts/video gaming accounts, online storage accounts) and personal websites and blogs ; domain names registered in your name; intellectual properties etc.**

7. *What is Identity theft ? Give example.*

Or

What do you mean by Identity theft ? Explain with the help of an example. [CBSE Sample Paper 2020-21]

Solution. Identity theft occurs when someone uses another person's personal identifying information and pretends to be that person in order to commit fraud or to gain other financial benefits.