

Societal Impact

Why this chapter?

Digital technologies have changed banking, shopping, learning and communication - making life faster and easier. But this convenience brings new ethical, social and legal issues we must understand and handle responsibly.

Digital society + Netizen ∴

A society that uses digital technology in all spheres of life is a digital society. Anyone who uses digital tech with the Internet is a digital citizen or **NETIZEN**.

Good netizen = safe + ethical + legal use

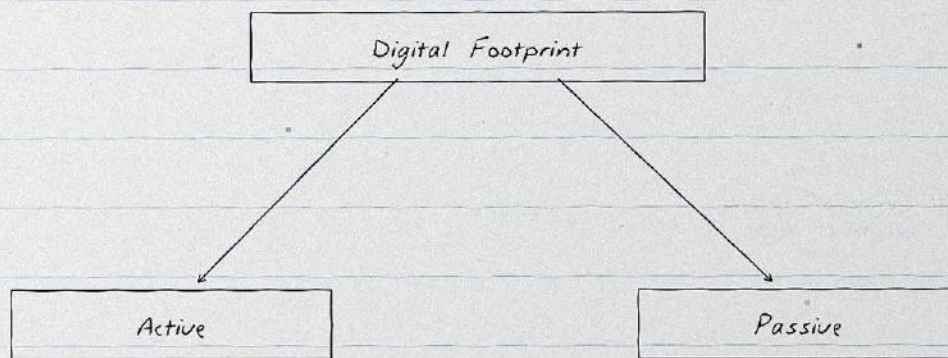
A responsible netizen abides by three sets of etiquettes:

- Net etiquettes
- Communication etiquettes
- Social media etiquettes

We study each, plus data + cyber safety.

Digital Footprint

The trail of data we leave behind while using the Internet is our digital footprint. It includes websites visited, emails sent, data submitted, plus IP address, location + device details. It can be made **WITH** or **WITHOUT** our knowledge, and may be misused for ads or fraud.



ACTIVE : data we submit intentionally^{*} - emails, posts, form entries, uploads.

PASSIVE : data trail left unintentionally - generated when we just visit a site, use an app or browse (cookies, history, IP logs).

Once online, a footprint can never be fully erased

Net Etiquettes

Proper manners while surfing the Internet. Be ethical, respectful and responsible online.

(A) Be Ethical

- No copyright violation - take permission
- before using others' material.
- Share your expertise, but only true and
- verified information.

(B) Be Respectful

- Respect privacy - do not share others'
- images/files without their consent.
- Respect diversity of knowledge, culture,
- experience in a group or forum.

(C) Be Responsible

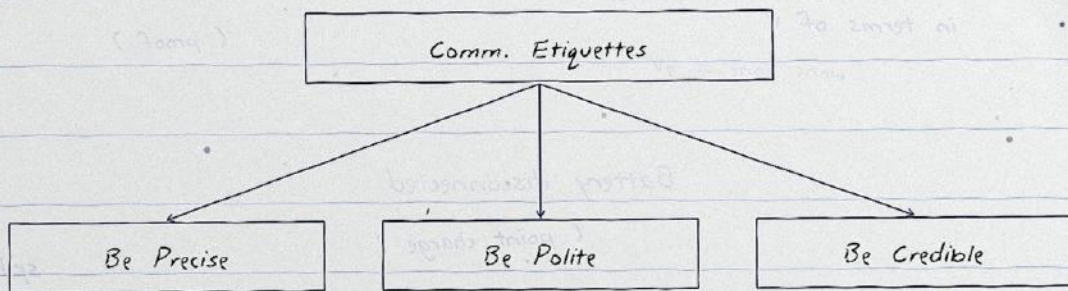
- Avoid cyber bullying - insulting, * threatening *
- or degrading online behaviour.

Do feed the ~~troll~~ troll - IGNORE trolls; they thrive only on attention, so give none.

Our actions are traceable via digital footprints.

Communication Etiquettes

Rules for email, chat, texting, calls, forum posts and video conferencing. Three headings:



Be Precise

- Respect time - do not waste it on unnecessary mails; expect no instant reply.
- Respect data limits - send compressed files or a cloud link, not huge attachments.

Be Polite + Be Credible

- Be polite + non-aggressive, even in disagreement (sync or async chats).
- Be credible - remarks over time decide whether others trust your posts.

On Spam: neither reply nor open attachments

Social Media Etiquettes

Social media (Facebook, Twitter, Instagram, YouTube...) let users create + share content.

Two etiquette headings: Be Secure, Be Reliable.

(A) Be Secure

- Choose password wisely - strong + changed often; never share username/password.
- Know who you befriend - unknown people may have malicious intent.
- Beware of fake information - validate news and posts before believing.

(B) Be Reliable

- Think before you upload - once posted, it stays on the server even after you delete.

Safety tips

- Never arrange to meet an online friend.
- Use the ~~same~~ SAME password on all sites is unsafe.
- Think carefully before sharing personal photos.

A post can be deleted, but never permanently.

Data Protection

In the digital age, data protection is mainly about the **PRIVACY** of data stored digitally.

Sensitive data

Data that can cause substantial harm, embarrassment or unfairness if breached.

- Biometric + health information
- Financial information
- Personal documents, images, audio, video

How is it protected?

- Encryption - scramble so only the authorised user can read it.
- Authentication - verify the user's identity.
- Other secure methods for legitimate use.

Data protection laws

Every country has its own data^{*} protection policies (laws) - legal documents that guide processing, storage + transmission of sensitive information, to stop misuse.

Next: IPR - copyright, patent, trademark.

Intellectual Property

A new original idea a person^{*} creates is that person's intellectual property (IP). IP covers inventions, literary + artistic works, designs, symbols, names and logos.

IP is protected by copyright, patent, trademark

IPR lets the creator earn recognition or financial benefit from their creation.

(A) Copyright

Legal right given to creators of original works - writing, photos, audio, video, software, sculptures, artistic + literary work.

- Granted AUTOMATICALLY on creation.
- Rights: copy, make derivatives, distribute, publicly display or perform the work.
- To use others' work, obtain a licence. *

Eg: R. Kipling holds the copyright to 'The Jungle Book' - copying it without permission

Patent + Trademark

(B) Patent

Granted for an INVENTION. Unlike copyright, it is ~~automatic~~ NOT automatic $\therefore$ the inventor must apply (file) for it.

- Owner gets exclusive right to stop others
- using, selling or distributing it.
- Protects an invention for 20 YEARS,
- after which anyone may use it freely.
- Encourages sharing of scientific findings.

(C) Trademark

Any visual symbol, word, name, design, slogan or label that distinguishes one brand from another.

- Eg: only Nike can use 'Nike' on shoes.
- Stops a confusingly similar mark like 'Nikke'.
- Prevents brand confusion for customers.

Copyright = auto

Patent = file, 20 yrs

IPR Types at a Glance

The three main tools that protect intellectual property, compared side by side:

Type	Protects	How got	Term
Copyright	Original creative works	Automatic	Life + years
Patent	New inventions	Must file	20 years
Trademark	Brand symbol / name / logo	Register	Renewable

Software example

- Code of the software -> Copyright
- Functional idea of the software -> Patent
- Name + logo of the software -> Trademark

One product can carry all 3 protections at once *

Violation of IPR

1. Plagiarism

Presenting someone else's idea or work as your own. Copying without citing the source, or repackaging an existing idea as new.

*

2. Copyright infringement

Using another's work without permission (or without paying, if it is sold). Being on the Internet means it is ~~free~~ NOT free to use.

3. Trademark infringement

Unauthorised use of another's trademark on products or services. Owner may sue.

How to avoid violation

- Always CITE the author / source used.
- Paraphrase in your own words + still cite.
- Check copyright status before using material.
- Take permission or a licence; pay if sold.
- Cite even freely-available public content.

Plagiarism is an ethical offence + sometimes fraud.

Public Access + Open Source

Copyright can restrict reuse. Licences give rules that let others use + build on a work.

Open source licences allow collaboration without seeking individual permission.

GPL + GNU GPL

- For SOFTWARE. Free software licence.
- Freedom to run, study, share + modify.
- Derivative works keep the same rights.

Creative Commons (CC)

- For creative works - sites, music, film, literature. Enables free distribution.
- Author decides the conditions of sharing.

FOSS

Free + Open Source Software: source code is open to access, modify + improve. Eg: Ubuntu, Fedora, LibreOffice, Mozilla Firefox.

Software piracy is ~~legal~~ illegal - unauthorised copying = copyright infringement. Always avoid it.

Licences Compared

*

Software is distributed under different terms.

Know what each type allows:

*

Type	Source code	Cost	Can modify?
FOSS	Open	Usually free	Yes
Freeware	Closed	Free	No
Shareware	Closed	Free trial, pay	No
Proprietary	Closed	Paid	No

Key differences

- Freeware: free to use but code hidden,
- no commercial redistribution (eg Skype).
- Shareware: free for a trial period, then pay.
- GPL work may still be sold for a fee -
- freedom, not always price, is the point.

Cyber Crime

Criminal offences carried out in a digital environment. Either the computer is the **TARGET**, or it is used as a **TOOL** to commit the crime.

Aim: cause physical harm, financial loss or mental harassment - to a person, group, organisation or even a country.

Virus vs Malware

- Virus: lines of malicious code that COPY themselves + damage data or the system. *
- Malware: any software made to gain
- **UNAUTHORISED** access to a computer.
- Others: worms, trojans, spyware, adware.

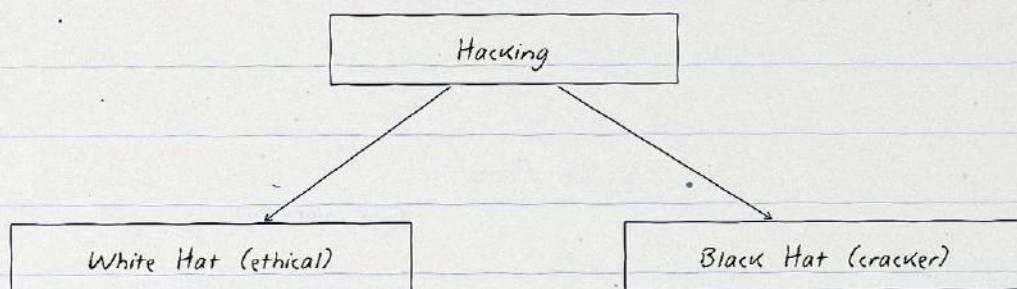
*Common cyber crimes

Hacking, phishing, identity theft, ransomware, denial-of-service, email + banking fraud, cyber bullying + cyber trolling.

We look at the major ones next.

Hacking

Unauthorised access to a computer, network or digital system. Hackers look for bugs to exploit + break into the system.



Ethical / White hat

- Positive intent - find loopholes on testing.
- Reports flaws to the owner + improves security; prepares owner against attacks.

Non-ethical / Black hat

- Gains access to steal sensitive data.
- Aims to damage or bring down systems.

Also called ~~coders~~ 'crackers' - used for identity theft, monetary gain or leaking information.

Phishing + Identity Theft

Phishing

Fake websites or emails that look authentic trick a user into giving sensitive details - usernames, passwords, bank + card numbers.

- Common method: EMAIL SPOOFING (a forged sender address that looks genuine).
- URL looks similar but is fake; uses real logos.
- Also done via fake calls + text messages.

Identity theft

Stealing personal data (email, bank details, PAN, Aadhaar, passport) to commit fraud in the victim's name. A type of phishing attack.

- Financial: stolen identity used for money.
- Criminal: used to avoid detection of true identity.
- Medical: used to seek drugs or treatment.

Check the URL carefully before you type a password

Ransomware + Bullying

Ransomware

Attacker gains access + blocks the user, usually by **ENCRYPTING** the data. Victim is blackmailed to pay a ransom for access.

- Spreads via malicious sites, doubtful
- downloads, spam attachments + bad ads.

Cyber bullying

Repeatedly insulting, threatening or embarrassing someone online - rumours, threats, posting private info, harassment.

Cyber trolling

A troll deliberately starts quarrels or posts inflammatory / off-topic messages just for amusement + attention.

Best reply is to ~~argue~~ **IGNORE** - trolls thrive on attention, so do not feed them.

Online actions can be traced by digital footprints.

Cyber Crimes Summary

Quick revision table of the major cyber crimes and what each one does:

Crime	What happens
Hacking	Unauthorised access to a system
Phishing	Fake site/email* steals credentials
Identity theft	Personal data misused for fraud
Ransomware	Data encrypted, Ransom demanded
Cyber bullying	Repeated online harassment
Cyber trolling	Inflammatory posts for attention

Report cyber crime to the cyber cell / police

Cyber Safety*

Cyber crime is mitigated by TWO steps: stay alert + take legal help. Safety measures:

Safely browsing the web

- Use antivirus + keep it updated.
- Download only from secure HTTPS sites.
- Do not visit / download from untrusted sites.
- Heed browser alerts on unverified sites.
- Refuse cookies on unknown sites.

Identity protection

- Strong password, changed periodically.
- Different password for each website.
- Alphanumeric + special characters; no
- common words or names.

Confidentiality

- On others' computers, do not save/autofill
- passwords; use a private window.
- Take regular backups of important data.
- Secure home Wi-Fi with a strong password.

Transact only on well-known secure sites.

Indian IT Act

As cyber crimes grew, India brought a legal framework to protect data + Internet users.

IT Act 2000, amended in 2008

What the Act does

- Guides processing, storage + transmission
- of sensitive information.
- Gives legal recognition to electronic
- records + digital signatures.
- Outlines cyber crimes + their penalties.
- Enables safe e-governance + e-transactions.

Cyber Appellate Tribunal

Resolves disputes from cyber crime - source tampering, hacking, using another's password, publishing personal data without consent.

Digital signature

Digital equivalent of a *paper certificate.

Uses a unique digital ID from a Certified Authority (CA) to authenticate a signer.

E-Waste

Discarded electronic devices - old computers, phones, printers, batteries - are e-waste.

As devices are replaced fast, e-waste grows.

Hazards

- Contains toxic lead, mercury, cadmium.
- Pollutes soil + water if dumped in landfills.
- Harmful fumes on burning - health risks.
- Unsafe recycling injures informal workers.

Management: 3 R's

- ① Reduce buy only what is needed;
extend a device's usable life.
- ② Reuse donate, or resell working devices; refurbish old ones.
- ③ Recycle give e-waste to authorised recyclers to recover metals safely.

*

It is fine to ~~dump~~ hand e-waste to certified recyclers,
never to open dumping or burning.

Impact on Health

More screen time (mobile, laptop, TV, gaming) in a poor posture harms us physically + mentally. Overuse can even be addictive.

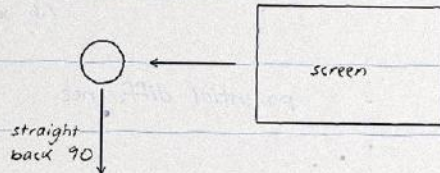
Ergonomics

Science of designing the workplace - chair, desk, screen - so it is safe + comfortable, reducing strain, fatigue + injury.

*

Health concerns

- Eye strain from screen glare - focus on



- distant objects + take outdoor breaks.
- Back, neck + shoulder pain from bad posture.
- Wrist / finger pain from overusing keyboards.
- Stress, fatigue + obesity from excess use.

Right viewing distance + 90 posture = less fatigue

Common Mistakes

① Active vs Passive

Active = we submit; Passive = auto-logged.

② Plagiarism vs Infringement

Plagiarism = no credit; infringement = no permission. Citing avoids only plagiarism.

③ Copyright vs Patent

Copyright is automatic; a patent is filed.

④ White vs Black hat

Ethical hacker helps; cracker harms.

⑤ 'On Internet = free'

Being online does NOT make content free.

Watch out

Freeware means ~~open~~ free to use but CLOSED source.

FOSS = open source; freeware just = no cost.

Do not confuse the two in the exam.

Quick Recall

Netizen = safe + ethical + legal net user.

IPR = Copyright + Patent + Trademark

Patent term = 20 years

Mnemonics

- Etiquettes = 'NCS' : Net, Comm, Social media.
- 3 R's of e-waste = Reduce, Reuse, Recycle.
- White = good Hat, Black = bad Hat.
- Comm = 3 P's : Precise, Polite, credible (Proof).

One-liners

- Phishing = fake bait for your credentials.
- Ransomware = data locked till you pay.
- Plagiarism = stealing credit; cite to avoid.
- IT Act 2000 (amended 2008) = India's cyber law.

Revise the tables on the IPR, licence + crime pages.

PYQ Trend + Summary

How it is asked

- Case study: name the cyber crime + justify
- (hacking / identity theft / bullying) - 1-2 mk.
- Plagiarism vs copyright infringement - 2 mk.
- Differentiate copyright, patent, trademark.
- Active vs passive digital footprint - 1 mk.
- FOSS / freeware / proprietary - short answer.
- Ergonomics + health measures - 2-3 mk.

Chapter in a nutshell

- Digital footprint: active + passive data trail.
- Follow net, communication + social etiquettes.
- Protect data; respect IPR (avoid 3 violations).
- Open source: GPL, CC, FOSS vs freeware.
- Cyber crimes + cyber safety measures.
- IT Act 2000/2008 gives the legal framework.
- Manage e-waste; mind health + ergonomics.

Be a responsible, safe + ethical digital citizen

Prev: Python Modules Chapter ends here.