General instructions to be followed to pass essay

Mock Test

Name: Aluina Haider
LMS ID = 38390

1- Spend time on rightly comprehension of the topic, you won't pass the essay unless and untill you addressed the asked part

English Essay

2- Try to make your main heading in the outline from the words in the question statement

Cybercrime: A Bigger Challenge for Developing Countries than for Developed nations

3- Try to add hook in the introduction. The length of introduction must be of 2 sides

Outline:

4- your topic sentence in your argument must be aligned with the ending sentence

You haven't understood the topic. You are supposed to provide comparative analysis.

(1) Introduction:

5- Avoid firstly, secondly, thirdly etc. in outline

(a) Hook

(b) Definition of cybercrime and cybersecurity

(c) Thesis Statement: While cybercrime

6- add references in your arguments with proper sources Go for diversification of references

Before the comparison

7- Do not add new idea or point in Conclusion

face more severe consequences due to weak cyber infrastructure, poor policy frameworks, and lack of awareness.

8- You won't pass the essay if make more than 4-5 grammatical mistakes

(2) Understanding the Cyber-

9- outlines that are not self explanatory or does not aligned to with the essay statement are liable to mark 0 and the essay would become null and void

2) Types of cybercrime: Challenges

data breaches, financial fraud,

identity theft, cyberterrorism.

2.2) Tools and techniques used by cyber-criminals.

(3) The Global Landscape of Cybercrime:

3.1) Cybercrime in developed vs developing nations

3.2) Ransomware attacks in the US vs Nigeria / Pakistan.

(4) Why Developing Countries are more vulnerable

4.1) Weak digital infrastructure and outdated technology.

4.2) Lack of cybersecurity legislation and enforcement

4.3) Limited investment in IT security

4.4) Low public awareness and education

4.5) Dependence on imported tech without sovereignty.

(5) Impacts on Developing Countries:

5.1) Economic: Loss of GDP due to digital fraud and attacks

5.2) Social: Erosion of public trust

in digital platforms

5.3) **Political**: Threat to national security and stability.

5.4) **Developmental**: Hindrance to digital transformation goals (e.g SDGs).

(6) Developed Nations: How they are Coping Better

6.1) Advanced cyber laws and enforcement

6.2) Regular cybersecurity audits and infrastructure upgrades.

6.3) Trained personnel and digital literacy programs.

6.4) International collaborations (e.g NATO Cyber Defence)

(7) Challenges in Addressing Cybercrime in Developing Nations

7.1) Budget constraints

7.2) Corruption and lack of political will

7.3) Global nature of crime vs national jurisdiction limitations.

(8) Recommendations :-

8.1) Policy reforms and data protection laws.

8.2) Investment in cyber infrastructure.

8.3) Public-private partnerships

8.4) Capacity building and digital literacy campaigns.

8.5) International cooperation and intelligence sharing.

(9) Conclusion:-

Essay

"The real problem is not whether machines think, but whether men do"

What it signifies?

– B.F. Skinner

In today's hyperconnected world, cyberspace has become the new battle ground — one that is boderless, stealthy, and devastating. While cybercrime is a global menace, it disproportionately affects developing nations due to their inadequate digital infrastructure, fragile governance systems, and lack of public awareness. The growing dependence on digital systems in these countries, without parallel development in cybersecurity measures, has rendered them vulnerable

Must work on your introduction

targets for increasingly sophisticated cybercriminals.

You are not required to break your intro into paragraphs

Cybercrime refers to illegal activities conducted through digital platforms or targeted at computer systems. These include identity theft, financial fraud, ransomware attacks, cyber espionage, online harassment, phishing and denial-of-service (DoS) attacks. The motivation behind cybercrimes may vary from financial gain and political moves to ideological warfare.

Modern cybercriminals operate in sophisticated networks, often with access to state-of-the art tools and anonymous online platforms like the dark web. For developing countries with limited technical capability, combating such threats becomes a daunting task.

Developing countries like the United States, United kingdom and Germany experience cyber attacks frequently but possess robust mechanisms

to detect, mitigate and recover from them. Their high investment in cybersecurity, trained professionals and well-enforced digital laws allow them to limit damage and adapt quickly.

Conversely developing countries such as Nigeria, Pakistan and Bangladesh struggle to even detect breaches in time. For instance, Pakistan's National Bank was hit by a major cyberattack in 2021, disrupting operations countrywide. Investigations revealed systemic weakneses in digital security that remained un-addressed for years.

There are several reasons why developing countries face greater challenges:-

- Weak Digital Infrastructure:- Outdated software, lack of encryption, and absence of firewalls in public and private sectors make systems easy targets.
- limited Cybersecurity Awareness:- Many users in developing nations are unaware of basic safety protocols

like strong passwords, phishing indicators or two factor verification.

- Poor Legal Frameworks: Most developing countries either lack comprehensive cyber laws or fail to enforce them effectively due to corruption and inefficiency
- Shortage of Skilled Professionals: There is a scarcity of trained cybersecurity experts in developing nations, leaving institutions underprepared.
- Dependency on Imported Technology: Much of the hardware and software is sourced from abroad, often without scrutiny for embedded vulnerabilities or backdoors.

Cybercrime inflicts both direct and indirect damages:-

- Financial Losses: Billions are lost annually to online frauds and ransomware. For struggling economies, this is a severe blow to GDP
- Erosion of Trust: Citizens lose faith in e-governance, online banking, and digital platforms, slowing down digitalization

efforts.

- National Security Risks:- Leaked data or compromised infrastructure can be explaited by hostile actors for espionage or sabotage.
- Impact on Development Goals:- Cybercrime hinders progress on digital inclusion and sustainable Development Goals (SDGs), especially related to innovation and institutional building.

Developed nations have adopted comprehensive measures to curb cyber threats:

- Strong legislation: Laws such as the General Data Protection Regulation (GDPR) in Europe ensure strict compliance and data privacy.
- Massive Investment: Billions are allocated annually to cyber defense by both public and private sectors
- Public awareness campaigns: Digital literacy is integrated into school curriculums and public outreach.
- International cooperation: Developed

platforms like Interpol and NATO Cyber Defence Center.

These advantages create a resilient ecosystem that can adapt quickly to evolving cyber threats. Even when awareness exists, certain structural issues persist:-

- Budgetary Constraints: Cybersecurity is often a low-priority area in national budgets.
- Jurisdictional Limitations: Cyber-criminals often operate internationally, making local law enforcement powerless due to lack of treaties and cross-border mechanisms.
- Political Instability: In some countries, political unrest and fragile institutions prevent a coherent response to digital threats.

To address the imbalance, developing countries must act decisively:

- **Legislative Reforms**: Update and enforce cybercrime laws aligned with international standards.

- **Cybersecurity Education:** Promote digital literacy in schools, colleges, and workplaces.
- **Public-Private Partnerships:** Engage tech firms to assisst in setting up secure infra-structures.
- **Skilled Workforce Development:** Invest in training programs for cybersecurity professionals.
- **Regional Collaboration:** Former cyber alliances for intelligence sharing and mutual defense.
- **Emergency Response Mechanisms:** Establish national-level Computer Emergency Response Teams (CERTs)

In a world increasingly governed by digital systems, cybercrime has emerged as an invisible warfront. While all countries are under threat, the disproportionate impact on developing nations is clear and alarming. Their weak defences, coupled with growing digital dependence, make them soft targets in a ruthless cyber battleground. If left unaddressed, cybercrime could stall the technological and economic progress of these nations

for decades to come.

Hence, developing countries must treat cybersecurity not as a luxury, but as a foundational pillar of national resilience and growth. Only then can they unlock the true potential of digital transformation without falling prey to its darkest underbelly.

Work on your essay pattern
Essay must be in paragraph
Not in bullet forms
Work on your topic comprehension
Must attend the tutorial session for further suggestions and mistakes