General instructions to be followed to pass essay

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

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

NBA
Mock Exam
English Essay
Date. 8- December-2025
Name. Shahvir Qazi
Batch. 1911

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

Technology is a threat to Privacy

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

Outline

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

1. Introduction
1.1 Hook
1.2 Background
1.3. Thesis: The concept of privacy is being eroded through modern means which include cyber espionage, social engineering, ransomware, sale of data, data leaks, hacker groups, spyware, Quantum computing and these require certain remedies to protect one's privacy.
2. Erosion of Privacy via Modern Means
2.1 Invention of Modern Computers
2.2 Vision of the future
3. Cyber Espionage
3.1 Vulnerabilities of digital systems
3.2 Existing Laws

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

7- Do not add new idea or point in Conclusion

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

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

work on your phrasing.

10- always try to be relevant to the topic, if even your 1 or 2 arguments are irrelevant, the examiner would not pass your essay.

4. Social Engineering Techniques
4.1 Social Media as a launching pad.
4.2 Brute-force attacks

5. Rise of Ransomware
5.1 Governments and corporations at risk
5.2 Lockbit ransomware group case

6. Sale of Online User Data
6.1 Utility of user data
6.2 Cambridge Analytica case

7. Data Leaks on the Dark Web
7.1 Ease of access to the dark web
7.2 Raidforums.com case

8. State-sponsored Hacking Groups
8.1 Cyber war
8.2 Collateral damage

9. Use of Spying Tools
9.1 Free access to Spyware
9.2 Pegasus spyware case

10. Quantum Computers
10.1 Breaking encryption
10.2 Future of the digital world

11. Remedies to Protect Privacy
11.1 End-to-end encrypted software
11.2 Minimal use of the internet

12. Conclusion

You haven't understood the topic at all. You are providing me the negative impacts of technology instead of privacy.
Work on your topic comprehension
Improve your phrasing
Word selection must be improved.
Must attend the tutorial session for further suggestions and mistakes

In exchange for the freedom to traverse the digital world, humanity has given up its right to privacy. The social fabric of the world has been altered to the point of no return. The digital reality of today is shaping humanitys future. One of the major changes being felt is the depletion of privacy. Every passing day humans surrender more and more of their private data to the online world willingly. Very few people are aware of the large number of entities that get access to that data with little or no hassale. This breach of privacy has been going on for decades and for that same time period it has been evolving. Nowadays there are dozens of ways to get the private data of users on the internet. The price of digital liberty is the willing and unwilling surrender of privacy and control over personal data. The concept of privacy is being eroded away through modern means which include cyber espionage, social engineering, ransomware, sale of online user data, data leaks, hacker groups, spyware, quantum computing, these repuire certain remedies to protect one's privacy. Technology indeed is the biggest threat to privacy.

No Argumentation, you are just providing me the information

The invention of modern computers brought revolutionary change to the world. Great names such as Alan Turing and Charles Babbage are credited with making modern computing a reality. It was once a concept which only existed in Sci-fi novels. Eventually the notion of modern computers manifested into reality. Has humanity made great strides in the field of technological development. The development of computers led to other technological marvels such as smartphones and smart watches. But little did anyone know how one day they would be used against humans to keep track of their information in the absence of consent. Instead a utopian reality was predicted where humanity would have reached the final stage of evolution. One man who did accurately predict the consequences of such a world was George Orwell through his book '1984'. His notion of 'Big Brother' in the book as an all-seeing eye of sects has come to life in the modern world. An element of this is the use of cyber-infiltration to get access to digital networks.

As time passed people began crafting ways to bypass the

digital mechanisms put in place to prevent unauthorised access. Vulnerabilities were found out and exploited to extract valuable data which included user data as well. As time went by cyber security improved, but so did cyber espionage. This set of digital penetration techniques pose the biggest threat to the privacy of people all over the globe. Almost every human on the planet uses the internet. According to Pew Research centre, by 2050 every single human being will be actively using the internet. This shows the magnitude of the threat to privacy that cyber espionage poses. One of the earliest examples of the sheer power of cyber infiltration is the Stuxnet virus. This was a CIA-made computer virus employed in 2005 which infected the nuclear command and control systems of Iran. This virus decimated the Iranian nuclear potential and caused them millions of dollars of damages. Nowadays such techniques have evolved and expanded in a way that any person with a computer and an internet connection can employ them.

Social media has emerged at the forefront of the issue

Through clever use of manipulation techniques, any normal and random user can extract his target's sensitive data through social media. This includes engineering false login pages of social media websites and uploading them online. These are then shared as harmless links on social media where any unsuspecting user can accidently handover his log-in credentials to other person. Such techniques are notorious for being easy to employ and has led to all kinds of normal and high profile users to be deprived of their privacy, money and much more. Aside from these brute-force attacks are also used where commonly used passwords are repeatedly entered until the right one matches and the attacker gets access to an individuals private account. Social engineering is reportedly increasing and those not aware of it are completely losing their privacy. Such techniques have given rise to another strain of hacking attacks known as ransomware.

Major companies of today have their data held hostage by ransomware groups. These groups lock these organizations out of their systems and demand a huge sum of money to not publically release their sensitive data.

The data held hostage often includes personal data of individuals such as names, phone numbers, medical data, credit card numbers and social security numbers of millions of users. Major banks and businesses such as Standard Chartered bank has not been immune to this. Governments world wide are at huge risk too and often get affected. Various departments of the governments of developing and underdeveloped countries have faced this. The governments of Mexico and Chile have to deal with ransomware in 2019 and 2020. The most notorious ransomware group is known as Lockbit and is terrorizing the digital world. It has been active for at least 5 years and has wreaked havoc on cyber systems of global businesses. They have extracted and accumulated millions of dollars. Their attacks led to the leaking and exposure of millions of peoples data. Whether it is data stored in a smartphone or a pager, it is constantly at risk. Many times the culprits are legal entities who sell such data for a profit.

Many companies extract user data through cookies on websites. They go on to sell this data to the highest bidder. This has concerned millions of privacy-focused

Perhaps the most infamous case in terms of breach of privacy on the dark web is a site known as Raid forums. This website was available on the clearnet along with having a dark web version as well. It is known to have hosted thousands of databases containing highly private data of over a billion people. Although it was taken down, clones and copies of the website still exist on the web. A lot of the data present on such websites is the work of state-sponsored hacking groups.

Government funded hacking groups which wage cyberwar against each other are known as state-sponsored hackers. These hackers employ the most advanced hacking techniques to damage their targets. They often target other governments and multinational businesses. These groups tend to be well-equipped and their hacking attacks affect millions of people. Often people who have no role in the cyber war get caught in the crossfire and have their digital and personal identities exposed as collateral damage. This has become a common occurance in today's era.

In very rare cases do the perpetrators behind such fierce cyber attacks get apprehended. These groups often utilize highly advanced digital spying tools.

Any internet user can get a hold of basic spyware tools and employ them against people they have a grudge with. These tools can also be coded and made with precision if one has the requisite knowledge. Those who are not well-informed regarding these often become a victim to these. Numerous online repositories have hundreds of spyware available for free and unrestrained use which puts the common user at great risk. Remote Access Trojans (RATs) are the most commonly used form of these tools. The use of the Israeli spyware of 'Pegasus' in 2022 raised grave concerns for people who took their privacy seriously. The paid use of this software allowed an entity to hack in to their targets phone using just a simple missed whatsapp call. Such advanced tools are no where near as strong as quantum computers.

The world is on the verge of a

breakthrough in the field of quantum computing. These supercomputers are potent enough to break the world's most powerful encryption known as 256 bit SHA. China and America are competing to complete this new supercomputer. As much of a great thing it will be, it will pose dangers of equal significance especially when it comes to privacy. The notion of privacy may be erased upon the completion of these machines as they will give access to every technological system in the world with ease. The future of the digital world depends upon how these novel machines will be employed.

There are time-tested ways which can be used to protect one's privacy. The best among these is the use of end-to-end encrypted software which does not sell its data to third-party applications. The use of such applications which ensure data privacy allow one to be at ease. Telegram and signal are best known when it comes to private and secure messaging. Other similar apps can also be used to ensure privacy. The most optimal measure to fully protect one's privacy is by limiting internet usage.

The minimal use of the internet allows a person to keep his mental health and privacy in tact. This is recommended strategy by many experts to prevent any sort of loss in personal privacy.

The world has ultimately evolved where we face new challenges. Many of these challenges arise from our non-stop use of modern technology. With its benefits we have also witnessed many consequences, especially those which relate our personal data being so insecure. The field of offensive cyber security has changed our approach of dealing with technology. Awareness regarding the more careful use of technology is rising exponentially. If time permits, the world can perhaps adjust to these new issues using strong counter measures. The threat to privacy can be averted.