Data Privacy and Data Protection

Data Privacy:
Data Privacy refers to the proper handling of data means how a organization or user is determining whether or what data to be shared with third parties. Data privacy is important as it keeps some data secret from others/third parties. Data privacy is all about authorized access. It is also called as Information privacy.

Example –
In Bank, A lot of customers have their account for monetary transactions. So the bank needs to keep customers data private, so that customers identity stays safe and protected as much as possible by minimizing any external risks and also it helps in maintaining the reputation standard of banks.

2. Data Protection:

Data Protection refers to the process of keeping safe the important information. In simple it refers protecting data against unauthorized access which leads to no corruption, no compromise, no loss and no security issues of data. Data protection is allowed to all forms of data whether it is personal or data or organizational data.
Example –
A bank has lot of customers, so the bank needs to protect all types of data including self bank records as well as customer information from unauthorized accesses to keep everything safe and to ensure everything is under the control of bank administration.
The terms Data Privacy and Data Security are used interchangeably and seems to be same. But actually they are not same. In reality they can have different meanings depending upon its actual process and use. But it is sure they are very closely interconnected and one complements the other during the entire process. So, now let's know how Data Privacy is different from Data Protection from the below table.

Difference between Data Privacy and Data Protection :

S.No.	Data Privacy	Data Protection
01.	Data Privacy refers maintaining secrecy or keeping control on data access.	Data Protection is the process of protecting data from external risks such corruption, loss etc.
02.	It is all about authorized access means it defines who has authorized access to data.	It is all about unauthorized access means if anyone has not access to data then it keeps the data safe from that unauthorized access.
03.	Data Privacy is a legal process/situation which helps in establishing standards and norms about accessibility.	Data Protection is a technical control system which keeps data protected from technical issues.
04.	Data Privacy is the regulations or policies.	Data protection is the procedures and mechanism.

05.	It can be said as a security from sales means holding the data from shared and sold.	It can be said as s security from hacks means keeping the information away from hackers.
06.	Data Privacy controls are mainly exits at the end user level. The users knows which data is shared with whom and which data they can access.	Data Protection is mainly controlled by the organization or company end. They tech all the required measures to protect their data from being exposed to illegal activities.
07.	Data privacy teams are made of experts with law making, policies and some engineering experts.	Data protection teams are made of experts from technical background, security background etc

Data Privacy on social media :

the main **revenue source** for the social media applications is by selling advertisements, but this is not the only way. For example, if we take the example of Facebook. Facebook does user profiling on the basis of demographics, on the basis of brands you like, movies you see etc and show you the relevant advertisements, links for apps of your interest and so on.
Facebook even **keeps a track** of all the activities that you do in offline world, that are not even shared on the platform.
Please read Terms and Conditions carefully.
Go through privacy settings in your account. Don't rely on default settings.

Stop clicking on posts like "Check your death day", "Find which celebrity do you look like" and so on.
Install a good antivirus software in your laptop and phone.

Turn off your location. Some sites even keep track of your activities in the offline world, but turning off location will at least do the least possible loss.

Don't forget to set up Security Answers.

Never leave your account logged in. You are in a way inviting cyber criminals to hack your account or act as an impostor.

Always check and analyse your post before posting. Try not to put too much revealing photos online.
Always try to create strong password for a site and try to change it in regular interval of time. Never ever set same passwords for multiple sites.
.

Below is the list of few security threats that we might face in social media accounts:

1. Most social networking sites have information like Birthday or Email address. Hacker can hack your email account by using social information and can have access to all the information he/she wants. You don't need to hide all information. You just need to take the following precautions:
    - Always set strong passwords. Don't go for the easy passwords built using your Birthday or child's name etc. i.e., from the information that is easily accessible from the social media account.
    - Don't reveal too much information in a post. Be careful with what you post online. For example, if I write *"Happy Mother's Day Mumma Richa Sahani"*. Now you see one can guess an answer to one of my security question "What is your Mother's Maiden Name?". This how it works for the thieves to get information by just analyzing your posts. They get so much information that they can even compromise your account.
    - Don't reveal your location. Try to keep the location section either blank or set it to a false location.
    - Do not use social media accounts from untrusted devices and networks in hotels, cafés, hospitals etc.
    - Do not elect to remember passwords/passphrases for social media accounts when offered by web browsers.
2. With the advent of Social Media like Twitter, there comes URL Shorteners in picture. Twitter allows a post to be maximum of 280 characters. Thus limiting the size and amount of information that can be shared. Shortened URL's can trick users into visiting harmful sites since full URL's are not visible. It is best to keep following points in mind before clicking on shortened URL to avoid being hacked.
    - Before clicking a link, place the cursor on the shortened URL. This will show the complete URL and will give you an idea about where the full URL actually points.
    - Check the shortened URL using the services that are available online like Sucuri to check whether the link is secure or not.
    - Use services like URL Void or MyWOT to check the safety status of the link.
3. Avoid posting too much details online. Will you ever stand in the middle of the crowd and shout that you are going on a vacation to so and so place? So why you post all the details of your trip on social media, with every second detail like *"Travelling to London, United Kingdom from Air India Business Lounge New Delhi"*. You are clearly giving your house keys to burglars. Try to take following precautions while posting any information online:
    - Avoid posting specific travel plans and itinerary. Never mention exact date and time.
    - Never post photos during the trip. Try to post photos after your return home from the vacation.
    - Try to stay offline during vacation.
    - Use the highest privacy controls to let only selective groups like family, selected friends to view your status updates and photos.
4. Have you ever wondered how we see a product on Flipkart and when we open another site, it will show the advertisement related to the product that we earlier searched on Flipkart. Every time we visit a website, it put invisible

marker which we call Cookies in technical terms in our computer. Job of these cookies is to track the user activity as we navigate from one site to another. This is the reason we are able to see the advertisements of our interest on the new page that we open. Cookies are the major loophole in the entire secure scenario. Most sites provide a option to opt out of the tracking feature, but if you don't get that option, Please be careful to clear the cache and the cookies on your browser regularly.

I hope after having such a detailed discussion on Privacy and Security in Social Media, you will surely try to implement these steps and Try to achieve a Private and Secure Social Media Account.

Ways to protect Online Data Privacy

There is a **cool new gaming app** available online. Now, what do you do if you want to download it? Well, you quickly run through the terms and conditions without looking and then move right on to the game. And what if a site wants to store your **credit card information**? You may allow it to do this so that you don't have to enter the data again and again.

But have you ever wondered what happens to the data that you so casually share online?

This data may end up in the hands of third-party companies that use it to analyze your online habits and create a profile that can be used in various ways like customized ads etc. And that's the relatively harmless option. In the worst-case scenario, your online data can also be used maliciously to cause great personal or financial harm. So what are the steps you can take to protect your online data privacy and prevent these things from occurring? This article provides you some basic tips that will make your online presence much more private and secure.

1. Always Browse in Anonymous Mode

Browsing in **Anonymous Mode** is only the first line of defense! Incognito Mode on Google Chrome or Private Windows on Firefox and Safari only ````````provides an extra layer of protection and not complete online privacy. That's maybe not even possible!!!

But what anonymous mode can do for you is block cookies so that most online tracking of you is defeated. Normally you see ads on websites that are tailored according to your browser history and the sites you have visited. This is achieved using **cookies** that store information about your online interactions. And browsing in Anonymous Mode is the first step in blocking these cookies and achieving more privacy online.

2. Change Your Default Search Engine with a Privacy-Focused Search Engine

Do you ever wonder how the search engine you are using is making money? How are they paying for the service they are offering you? Well, there are only 2 ways for the search engine to do that and that's either using **donations from people** or using **profits from ads**.

And if the search engine is free for you, then most likely it's making money using you!!! Search engines record all your data from your searching habits such as your likes and dislikes, your personal information, etc. Then they sell this data about customer profiles to various advertisers and make money off that.

In case you wish to avoid that, use a search engine that is funded by donations and is privacy oriented. Some examples of these alternate search engines that you can use are DuckDuckGo, Qwant, Startpage, etc.

3. Use End-to-End Encrypted Messaging Apps

Most messaging apps employ encryption, but it's only encryption in transit which means that your encrypted messages are decrypted on the provider's side and then stored in servers. But that's hardly safe! So it's best to use **end-to-end encrypted messaging apps** to provide you some privacy. The most popular end-to-end encrypted messaging app that you can use is WhatsApp. Other options are Viber, LINE, Telegram, etc.

4. Use a VPN to Protect Yourself from Service Providers

Do you think that if you are browsing the internet from your home connection your data is safe. In fact, there is a high chance that your internet service provider may actually be collecting and selling your browsing data to third parties. And it's not even illegal to do so since the data protection laws are quite unclear.
You can use a **VPN (Virtual Private Network)** that creates a private network across a public network. So your data will be encrypted in this manner and no other third party will be able to view it. Some of the good VPN services for usage are ExpressVPN, NordVPN, Hotspot Shield, IPVanish etc.

5. Enforce Browser Security with these Extensions

You can always improve your online privacy and increase your security by using some **extensions and online security tools**. For example: Make HTTPS Everywhere

extension your best friend as it will encrypt your communication with most websites leading to a secure connection with fewer chances of anyone snooping in.

The Ghostery Browser Extension is another great option as that will make your online browsing much safer by detecting and blocking all the third-party data-tracking items.

Also, another great online security tool is AdBlock. This handy little tool will filter out all the annoying ads you don't want and also protect you from malicious ads that can be used to infect your machine.
Another free cybersecurity tool is CheckShortURL that checks where shortened URLs are taking you because double-checking is always good!

6. Don't Use Public Storages for Private Information

You should definitely not use public storages that are meant for sharing data for storing private information as that is hardly safe! For example, It's not a good idea to store your **passwords** or other **confidential information** in Google Docs as it is relatively easy to access them from there.
Similarly, don't store **important scans** or other documents in your Dropbox unless they are in an encrypted archive.

Always assume that all information stored on public storages may actually become public at some point (accidentally or on purpose) and so store that information accordingly.

7. Stay Private on Wi-Fi Networks

There is no encryption on public Wi-Fi networks and so anyone can snoop onto your connections and access your data.
So if you are just using public Wi-Fi networks, you are risking the loss of your personal information, the leakage of your digital identity and even loss of money in the worst cases. So always avoid transmitting any sensitive data like **logins, credit card data, passwords,** etc. over public Wi-Fi if you are using it. Also, use a **VPN** as that creates a private network across the public Wi-Fi network. So your data will be encrypted in this manner and no other third party will be able to view it.

8. Use Secure Passwords

Using weak or basic passwords to secure your important information is like keeping the key next to the lock! So make sure to keep secure and complex passwords for your data if want them to be useful. Passwords should be sufficiently long and complex with at least **12 characters** which include upper and lower-case alphabets, numbers and special characters. Also, never use personal information like your name, birthday, pet's name, etc. for your password as that is easy information to guess.
Another basic thing to remember is that you should not use the same password for multiple applications. Now it may be difficult to remember multiple unique passwords but it is worth it if you want to protect your data.

9. Evade Tracking on Websites

Websites use **cookies** to gather information relating to your browsing history. These websites can also sell this analysis based on customer profiles to various third parties and make money off that. In case you wish to avoid that, make sure you have at least some control over where your data ends up. Therefore, it is best to control your cookies settings so that websites cannot access your data without your permission. You can do this on Chrome by clicking **Cookies** under **Privacy and Security** and then clicking off the cookies.

10. Change Your Social Media Privacy Settings

The biggest mistake you can make is just to keep on using the **default settings** as social media companies also make money as search engines do. By selling all your online data to the highest bidder!
Adjust your social media privacy settings to provide the maximum possible privacy. For example, You can change the privacy settings on Facebook to regulate your posts, locations, faces, etc. that are freely available.