SMVS
Page No.
Date : / /

Privacy Control Concept

* What is Privacy and Method to control Privacy.

=> Privacy refers to the protection of individual's personal information from unauthorized access.

It ensures that sensitive data such as personal details or financial information remain confidential.

=> Method to Control Privacy :

1 Password - Protect Everything

Use complex passwords that include a mix of letters, numbers and symbols.

Change your password regularly to reduce the risk of unauthorized access.

SMVS
Page No.
Date : / /

2 Keep Your Computer Virus-Free

Install and Regularly update reliable antivirus software to detect and remove malware.

Don't download software or files from untrusted sources.

3 Secure Your Brawser:

Ensures that website You visit use HTTPS, which encrypts the data exchanged between your brawser and the website.

4 Be careful What You share on Social Media

Avoid sharing sensitive information like your address, phone number of financial details.

5 Ask Why Others need Your Information

Alwayes question Why a service or person is asking For your personal information.

SMVS
Page No.
Date : / /

6 Don't Fall For Scams:

Be cautious of emails, message or website that ask for personal information or login details.

7 Only Use Software You Trust:

Only download software from the official website or check users reviews before download.

8 Only Use Secure Wi-Fi Connection:

Public wi-fi networks are often insecure, if you use, use a virtual private network encrp: your connection.

9 Use Multi-Factor Authentication

* Data Collection From Social Networks.

=> Data Collection from social networks involves gathering information from platforms like Facebook, Twitter or other

SMVS
Page No.
Date : / /

social media platform

This data is used to research, marketing or analyze the user work on social network.

=> Types of Data Collected

1 User Profiels : Information such as names, age, location details.

2 Behavioral Data : Data on how users interact with social platform

3 Content Data : Posts, images, videos and other media shared by user

4 Network Data : Information about a user's connection such as friend, group or follower.

5 Location Data : Geographic information collect from users.

=> Methods of Data Collection

1 APIs : Many social networks provide APIs that allow developers to

access certain types of data For third-party application.

2 Web Scraping: Extracting data directly from social network page using automate tool

3 User Consent: Collecting data with the explicit consent of the user

4 Third-Party Data Brokers: Purchasing data from companies that aggregate information.

5 Tracking Pixels and Cookies: Embedding tracking mechanism in ads or website that capture user interaction.

=> Challenges:

1 Data Breaches: Risk of unauthorized access to data.

2 Misuse of Data: Data can be used for identity theft Attack.

3 User Trust: Loss of user truct.

SMVS
Page No.
Date : / /

4 Data Accuracy : Ensure data is accurate and reliability of data.

* Pitfalls in Security :

=> Disadvantage of Security Failures :

1 Financia Losses : Companies or Organization may face immediate Financial losses due to theft of funds, ransom payment or Fraud.

2 Reputational Damage : Customers may lose confidence in a company's ability to protect data.

3 Legal and Regulatory Consequences : Affected party may takes legal action to the company for damages resulting From Data f breach.

4 Loss of Sensitive Data : Unauthorized access to personal data can lead to identity theft, Fraud and other crimes against individuals.

5 Operational Disruptions : Security incidents can cause significant

downtime, affecting productivity and service delivery.

6 Increased Security Costs : Companies may need to invest heavily for upgrading their security infrastructure.

7 Employee Morale and Productivity: Employee may lose confidence in the company's ability to protect their data or personal information.

8 Impacts on Customers and Partners : Customers may experience interruption in service or delays, leading to loss of business.

* Privacy Policing and Preserving :

=> Privacy Policing :

Privacy Policing involves monitoring, enforcing and ensuring compliance with ~~poli~~ privacy laws.

SMVS
Page No.
Date : / /

-> Aspects :

1 Regulatory Compliance :

Organizations must comply with privacy laws such as GDPR, CCPA and HIPAA.

Regular audits and assessments are conducted to ensure adherence to these regulations.

2 Data Monitoring and Auditing :

Continuous monitoring of data access and usage helps detect the unauthorized activities and potential privacy breaches.

3 Incident Response and Reporting :

Organizatons must have a clear incident response plan to address data breaches or privacy violations quickly.

4 Employee Traning and Awereness :

Employees are trained on privacy

policies, regulation and best practices ensure they understand the importance of protecting personal data.

5 Third-Party Compliance:

Organizations must ensure that third-party vendors and partners also comply with privacy regulation.

=> Privacy Preserving:

Privacy Preserving techniques focus on protecting personal or sensitive user data.

-> Key Method:

1 Data Anonymization:

Personal identifires are removed or obfuscated so that individuals can not be easily identified from the data.

2 Encryption:

Use Encryption Algorithm, For

SMVS
Page No.
Date : / /

data rest and transit to protect it from unauthorized access.

3 Data Minimization:

Organizations collect only the data that is necessary for specific purposes reducing the risk of exposure.

4 Differential Privacy:

A technique that adds statistical noise of data, that ensure individual data points cannot be identified even in aggregated datasets.

5 Access Control:

Strict access control ensure that only authorized personnel can access sensitive data.

* Information Privacy disclosure, Effects and Impact in OSM and Networks.

=> Information Privacy disclosure, Effects and Impact in Online

SMVS
Page No.
Date : / /

Social Media Network.

Disclosure refers to act of sharing personal information online, whether intentionally or unintentionally.

-> Information Privacy Disclosure in OSM and Networks:

Using disclosure, we can get the sensitive information of user like name, address, photo, and more sensitive data.

- Comman Types:

1 Personal Identification Information: Users Information like name, date of birth, address, number etc.

2 Sensitive Personal Data: Users Health record, Financial data or Social Security Number etc.

3 Behavioral Data: Browsing History, Social interaction, Preference and habits of user.

Page No.
Date : / /

4 Location Data: Realtime or historical location information from GPS-enabled devices.

5 Professional Information: Job details, company affiliation, Linkedin Profile of users.

-> Effect of Information Disclosure in OSM

1 Privacy Risk: Exposed personal information can be used to impersonate idividuals, leading to fraud, Financial loss and other crime.

2 Social Effect: Attackers can use disclosure information to manipulate or deceive individuals, leading to security breaches.

3 Reputation Damage: Inappropriate or sensitive information disclosure publicly can harm a person's reputation

4 Financial Loss: Disclosed financial information can be exploited for fraud leading to direct loss.

SMVS
Page No.
Date : / /

5 Legal Issues: Unlawful disclosure of sensitive information can result in legal action against individual or Organization.

-> Impact of Information Revelation in OSM

1 Impact on Individuals:

Users might unintentionally used more information than intended due to complex privacy settings.

Sensitive personal data might be exposed due to inadequate setting measures.

2 Impact on Network:

Network that do not adequately protect user data may suffer from breaches, leading to loss of trust of user.

Network and platform that fail to safeguard personal information may face penalties.