Social Media Security (23CY717)

UNIT – V

Policies and Privacy

5.1 Blocking Users

Blocking prevents unwanted users from contacting or viewing profiles.

Benefits

1. Protection from Harassment

Definition

Protection from harassment refers to safeguarding users from abusive, threatening, offensive, or unwanted behavior on social media platforms.

Harassment can take many forms, including cyberbullying, stalking, hate speech, and repeated unwanted contact.

Types of Online Harassment

Cyberbullying

Using social media to insult, threaten, embarrass, or humiliate others repeatedly.

Cyberstalking

Monitoring someone's activities continuously and sending unwanted messages that create fear or discomfort.

Hate Speech

Posting discriminatory comments targeting race, religion, gender, or ethnicity.

Sexual Harassment

Sending inappropriate messages, images, or comments without consent.

Trolling

Posting offensive remarks intentionally to provoke or upset others.

How Social Media Protects Users

Blocking Users

Users can block individuals who engage in abusive behavior.

Reporting Mechanisms

Platforms allow reporting of harmful content and inappropriate accounts.

Restricting Comments

Users can limit who can comment on their posts.

Message Controls

Settings can prevent messages from unknown users.

Content Filters

Offensive language filters automatically hide harmful comments.

Benefits

- Creates a safer online environment.
- Reduces emotional stress and anxiety.
- Encourages positive interactions.
- Protects mental well-being.
- Increases user confidence in using social media.

Example

If a person receives repeated threatening messages from an unknown user on Instagram, they can block and report the account, preventing further contact.

2. Better Privacy

Definition

Better privacy means giving users greater control over who can access, view, and use their personal information on social media platforms.

Privacy settings help users determine what information is shared and with whom.

Privacy Features

Profile Visibility Controls

Users can choose whether profiles are public or private.

Audience Selection

Posts can be shared only with selected friends or groups.

Location Sharing Controls

Users can disable automatic location tracking.

Tagging Permissions

Approval can be required before others tag users in posts or photographs.

Data Access Permissions

Applications requesting access to personal data can be managed.

Friend Request Controls

Users can restrict who can send friend requests.

Benefits

- Protects personal information.
- Prevents unauthorized access.
- Reduces the risk of identity theft.
- Maintains confidentiality.
- Gives users control over their digital presence.
- Enhances trust in online interactions.

Example

A Facebook user sets their account to "Friends Only," ensuring that personal photographs and updates are visible only to trusted contacts.

3. Reduced Spam

Definition

Reduced spam refers to minimizing unwanted advertisements, fraudulent messages, fake promotions, and irrelevant content received through social media platforms.

Spam often aims to deceive users or disrupt their online experience.

Common Types of Spam

Promotional Spam

Repeated advertisements and sales messages.

Phishing Messages

Fraudulent messages designed to steal sensitive information.

Fake Giveaways

False offers promising rewards or prizes.

Malicious Links

Messages containing links that install malware or redirect users to fake websites.

Bot Messages

Automated messages generated by fake accounts.

Methods to Reduce Spam

Blocking Spam Accounts

Prevent further interaction from suspicious users.

Reporting Spam

Notify platform administrators about spam content.

Filtering Messages

Separate unknown messages into request folders.

Restricting Contact Permissions

Allow communication only from approved users.

Using Security Features

Enable spam detection tools provided by the platform.

Benefits

- Improves the user experience.
- Reduces exposure to scams and fraud.
- Saves time by eliminating irrelevant content.
- Protects devices from malicious software.
- Enhances trust in social media communication.

Example

A user receives multiple fake lottery messages on WhatsApp. By blocking the sender and reporting the messages as spam, future spam communications can be prevented.

Uses

- Blocking cyberbullies
- Preventing unwanted communication

5.2 Controlling App Privacy

Privacy settings help users control who can access their information.

Privacy Controls

- Profile visibility
- Friend requests
- Photo sharing permissions
- App permissions

Importance

- Protects personal data
- Reduces security risks

Best Practices

- Review settings regularly
- Limit public access
- Disable unnecessary permissions

5.3 Location Awareness

Many apps track user location.

Risks

- Tracking by strangers
- Privacy invasion
- Physical security threats

Prevention

- Disable location sharing
- Share location only when necessary
- Check app permissions

5.4 Security

Security in social media protects users from cyber threats.

Security Practices

- Strong passwords
- Two-factor authentication
- Antivirus software
- Secure browsing

Importance

- Protects accounts
- Prevents hacking
- Maintains privacy

5.5 Fake Accounts

Fake accounts are created using false identities.

Purposes

- Fraud
- Scams
- Spreading misinformation

Risks

- Identity theft
- Financial fraud
- Online harassment

Prevention

- Verify profiles
- Report fake accounts
- Avoid suspicious users

5.6 Passwords

Passwords are the first line of defense for online accounts.

Characteristics of Strong Passwords

- Long length
- Combination of letters, numbers, and symbols
- Unique for every account

Weak Password Problems

- Easy hacking
- Account theft

Best Practices

- Use password managers
- Change passwords regularly
- Do not share passwords

5.7 Privacy and Information Sharing

Users must carefully manage the information they share online.

Information That Should Not Be Shared

- Bank details
- Passwords
- Personal addresses
- Confidential documents

Risks of Oversharing

- Identity theft
- Financial fraud
- Stalking

Safe Sharing Practices

- Share limited information
- Use privacy settings
- Verify audience before posting