#### **1: Introduction to Social Media Privacy**

* **Overview:**
  + With the growing use of social media platforms like Facebook, Instagram, Twitter, and TikTok, privacy concerns have become more important than ever.
  + This lecture will discuss the various **privacy concerns** on social media, **best practices** to protect your personal information, and tools/technologies to enhance privacy.
* **Real-Life Example:**A college student shares personal photos and information on Instagram. Without proper privacy settings, anyone can view these posts, potentially leading to unwanted attention or identity theft.

#### **2: Privacy Concerns on Social Media Platforms**

* **Data Collection:**
  + Social media platforms collect a vast amount of personal information, such as name, location, and interests.
  + **Concern:** How is this data used? Many platforms use your data for advertising purposes, selling it to third parties or using it to target you with ads .
* HOW IS IT HAPPENING - AI systems , Powerful algorithms
* **Real-Life Example:**Ever noticed how after searching for shoes online, you start seeing shoe ads on Facebook? This happens because social media platforms track your activity and use that data to target advertisements.
* **Identity Theft:**
  + Publicly sharing personal details (birthdays, addresses, phone numbers) can make users vulnerable to identity theft.
* **Real-Life Example:**A person posts a photo of their new driver’s license on Facebook. Scammers use this information to open fraudulent accounts in their name.

#### **3: Privacy Concerns on Social Media (Continued)**

* **Location Tracking:**
  + Many apps track your **location** by default. When sharing your location in real-time, you risk your privacy by making it easier for others to know your exact whereabouts.
* You download apps by looking at ads as soon as you download them they will start tracking you .
* **Real-Life Example:**People on Instagram often tag their locations when they post photos. A thief once robbed a person’s house after noticing they were on vacation from their Instagram posts.XD
* **Social Engineering Attacks:**
  + Hackers can gather information from public social media profiles to launch **social engineering** attacks, tricking you into revealing more personal details.

#### **4: Real-Life Case Study – Early Internet Privacy Breach**

* **Yahoo Data Breach (2013):**
  + **What Happened?**Yahoo, an early giant of the internet world, faced a massive breach where over 3 billion user accounts were affected. Hackers stole names, email addresses, phone numbers, and security questions.
  + **Why It Matters:**This breach revealed how vulnerable early internet services were, leading to stronger security measures over time.
  + **Key Takeaway:**Always use strong passwords and be cautious about the information you share online, even on well-known platforms.

#### **5: Real-Life Case Study – Recent Incident**

* **LinkedIn Data Leak (2021):**
  + **What Happened?**In 2021, personal data from 700 million LinkedIn users was scraped and posted for sale on the dark web. The leak included personal information like names, email addresses, and job titles.
  + **Impact:**Although LinkedIn claimed the data was publicly available, the incident raised concerns about how easily personal data can be collected without users' knowledge.
  + **Key Takeaway:**Be cautious about the amount of personal data you make public on social media, especially on professional platforms like LinkedIn.

#### **5 . 1: Best Practices for Protecting Privacy**

1. **Adjust Privacy Settings:**
   * Always review and adjust your privacy settings on social media platforms. For example, make your Facebook or Instagram profile private so only your approved friends can see your posts.
2. **Real-Life Example:**A teenager posts about a new job on LinkedIn without adjusting privacy settings. Strangers can access personal details from their profile.
3. **Limit Personal Information Sharing:**
   * Avoid sharing sensitive information like your phone number, home address, or financial details on your profiles.
4. **Real-Life Example:**A person posts their full address for a housewarming party invite, which a scammer later uses for fraudulent activities.

#### **6: Best Practices for Protecting Privacy (Continued)**

1. **Use Strong, Unique Passwords:**
   * Ensure that you use **different passwords** for each of your social media accounts. This prevents hackers from gaining access to all your accounts if one password is stolen.
2. **Enable Two-Factor Authentication (2FA):**
   * 2FA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, when logging in.
3. **Real-Life Example:**A person’s Twitter account was hacked because they didn’t enable two-factor authentication. The hacker posted harmful content in their name.

#### **7: Tools and Technologies for Enhancing Social Media Privacy**

1. **Password Managers:**
   * Tools like **LastPass** or **1Password** help generate and store strong passwords so that you don’t have to remember them all.
2. **Virtual Private Networks (VPNs):**
   * A **VPN** encrypts your internet connection, making it harder for anyone to track your online activities or location.

* Dark Web browser
* Onion Routing

1. **Real-Life Example:**

A college student uses a VPN while using public Wi-Fi at a coffee shop to protect their personal data from hackers.

1. **Ad Blockers:**
   * **Ad blockers** like **uBlock Origin** can help prevent websites from tracking you and displaying personalized ads based on your social media activity.

#### **8: Tools for Enhancing Social Media Privacy (Continued)**

1. **Privacy-Focused Browsers:**
   * Browsers like **Brave** and **DuckDuckGo** help block tracking cookies and offer more privacy-friendly features than mainstream browsers.
2. **Real-Life Example:**A user switches to Brave and notices fewer targeted ads after browsing their favorite sites.
3. **Anti-Tracking Software:**
   * Tools like **Ghostery** can block social media platforms from tracking you across different websites.

#### **10: Best Practices for Social Media Privacy**

1. **Review Permissions for Third-Party Apps:**
   * Be cautious about giving third-party apps access to your social media profiles. Always check what data they can access.
2. **Real-Life Example:**A game on Facebook asks for access to your friends list, posts, and photos. If not careful, your data can be shared with advertisers or hackers.
3. **Log Out of Social Media on Shared Devices:**
   * Always log out of your accounts when using shared devices or public computers.
4. **Real-Life Example:**A student forgets to log out of their Instagram on a library computer, and someone else accesses their account.

#### **11: Common Social Media Privacy Threats**

* **Phishing Attacks:**
  + Scammers send fake messages or emails pretending to be from social media platforms, asking for login information.
* **Data Mining:**
  + Some companies and individuals collect your data from public profiles and use it for marketing or malicious purposes.

-Selenium

#### **12: Best Practices for Reducing Privacy Risks**

1. **Turn Off Location Sharing:**
   * Many platforms share your location by default. Make sure to turn it off unless necessary.
2. **Real-Life Example:**A person posts pictures from their home with location sharing turned on, allowing strangers to see their home address.
3. **Be Careful with What You Post:**
   * Avoid posting personal updates, such as when you’re on vacation, to prevent burglars from knowing your home is empty.

#### **13: The Role of Governments in Social Media Privacy**

* **Governments worldwide are increasingly implementing stronger data privacy laws to protect users.**
  1. **General Data Protection Regulation (GDPR):**
     + Introduced by the European Union in 2018, the **GDPR** requires companies to be more transparent about how they collect and use personal data.
     + It gives users more control over their data and allows them to request deletion of their information.
  2. **Example:**A European Facebook user can ask the platform to delete all of their data under the GDPR.
  3. **India's Personal Data Protection Bill (PDPB):**
     + India is working on its own version of privacy laws through the **Personal Data Protection Bill**.
     + This bill focuses on ensuring that Indian citizens’ data is protected, especially from misuse by large companies and social media platforms.
  4. **Example:**A company collecting personal data from Indian users must now comply with the regulations and ensure data is not misused.

#### **14: The Future of Social Media Privacy**

* **Artificial Intelligence (AI) and Privacy:**Social media platforms are increasingly using **AI** to monitor user activity, detect suspicious behavior, and protect user data. AI helps identify hacking attempts and unusual login patterns to prevent unauthorized access.
* **Blockchain for Data Privacy:**Some companies are exploring **blockchain technology** to protect social media data. Blockchain can make data storage more transparent and harder to manipulate, as every change in the data is recorded permanently.  
  **Example:**Future social media platforms may allow users to control exactly who sees their data and ensure that no unauthorized parties can change or access it without their knowledge.

#### **15: Group Activity – Social Media Privacy Audit**

* **Instructions:**Students will review the privacy settings on their own social media accounts (Facebook, Instagram, etc.).
  + Identify weak spots, such as public posts or unnecessary permissions for third-party apps.
  + Make necessary adjustments to strengthen privacy.

#### **16: Quiz Time!**

1. **What does two-factor authentication (2FA) provide?**
   * a) More personalized ads
   * b) An extra layer of security
   * c) Free social media features  
     **Answer:** b) An extra layer of security.
2. **Which tool can help you store strong passwords securely?**
   * a) Facebook Ads
   * b) VPN
   * c) Password Manager  
     **Answer:** c) Password Manager.

### **Group Activity – Social Media Privacy Audit (Updated)**

**Instructions:**

1. **Review Privacy Settings on Common Apps:**
   * **WhatsApp**
   * **Instagram**
   * **Snapchat**
   * **Other apps you frequently use**
2. **Steps to Take to Strengthen Privacy:**

**1. Disable Location Sharing (All Apps)**

* **Why?**Apps often track your location, which could be used by advertisers or hackers. Keeping your GPS off unless necessary ensures your movements aren’t being constantly tracked.
* **How:**
  + Go to your phone’s settings (Android/iOS) and disable **location services** for each social media app.
  + Some apps allow you to share your location only when the app is in use, so adjust the settings accordingly.

**2. Review and Limit Who Can See Your Profile (Instagram, WhatsApp, Snapchat)**

* **Instagram:**
  + Set your profile to **Private** so only approved followers can see your posts.
  + **How:** Go to **Settings** → **Privacy** → **Account Privacy** → Toggle on **Private Account**.
* **WhatsApp:**
  + Limit who can see your **Profile Photo**, **Last Seen**, and **Status**. Choose **My Contacts** instead of **Everyone**.
  + **How:** Go to **Settings** → **Privacy** → Adjust visibility settings for **Profile Photo**, **Last Seen**, and **Status**.
* **Snapchat:**
  + Only allow **Friends** to see your snaps and stories, instead of making them public. Disable the **Snap Map** location feature to hide your location.
  + **How:** Go to **Settings** → **Who Can...** → Adjust visibility for **Snaps** and **Stories**.

**3. Disable Read Receipts and Status Views (WhatsApp)**

* **Why?**Disabling read receipts prevents people from knowing when you’ve seen their messages, adding a layer of privacy.
* **How:**
  + **WhatsApp:** Go to **Settings** → **Privacy** → Toggle off **Read Receipts**.

**4. Review App Permissions for Third-Party Apps (All Apps)**

* **Why?**Third-party apps sometimes request unnecessary access to your contacts, camera, or microphone. Regularly review and revoke these permissions.
* **How:**
  + Go to **Phone Settings** → **App Permissions** → Check which permissions (e.g., camera, microphone, contacts) each app has and revoke any that aren’t necessary.

**5. Avoid Linking Your Social Media Accounts (All Apps)**

* **Why?**Linking accounts (e.g., Instagram with Facebook) allows platforms to share data across services, leading to more personalized ads and a greater risk of privacy breaches.
* **How:**
  + Review account linking in **Settings** for each app and avoid unnecessary connections between social media accounts.

**6. Review Privacy for Posts and Stories (Instagram, Snapchat)**

* **Instagram:**
  + Use the **Close Friends** feature to share stories with a select group rather than your entire follower list.
  + **How:** Post a story → Click on **Close Friends** instead of sharing with everyone.
* **Snapchat:**
  + Share **Snaps** and **Stories** only with friends, not publicly.
  + **How:** Go to **Settings** → **Who Can...** → **View My Story** → Select **My Friends**.

**7. Be Mindful of What You Post Publicly (All Apps)**

* **Why?**Even seemingly harmless posts can give away personal details like your current location, habits, or relationships. Limit what you share publicly and use settings to control who sees your posts.

**8. Turn Off Activity Status (Instagram, WhatsApp)**

* **Why?**Activity status shows when you’re online or were last active, which can be used by people to track your availability.
* **How:**
  + **Instagram:** Go to **Settings** → **Privacy** → **Activity Status** → Toggle off **Show Activity Status**.
  + **WhatsApp:** Go to **Settings** → **Privacy** → **Last Seen** → Set it to **Nobody**.

**9. Use Two-Factor Authentication (2FA) for Account Security (All Apps)**

* **Why?**Adding 2FA provides an extra layer of security by requiring a code sent to your phone or email whenever you log in.
* **How:**
  + **Instagram:** Go to **Settings** → **Security** → **Two-Factor Authentication**.
  + **WhatsApp:** Go to **Settings** → **Account** → **Two-Step Verification**.
  + **Snapchat:** Go to **Settings** → **Two-Factor Authentication**.

**10. Regularly Review and Update Your Passwords (All Apps)**

* **Why?**Using the same password for multiple accounts makes you more vulnerable to hacking. Use strong, unique passwords and change them regularly.
* **How:**
  + Use a **Password Manager** (e.g., LastPass, Bitwarden) to generate and store secure passwords.
  + Avoid using easy-to-guess passwords like birthdays or common phrases.