Module 4: Digital Privacy and Security

Lesson Plans

Lesson 1: How Your Data Is Collected and Used

This lesson explores how **personal data is collected, tracked, and used** by **data brokers, online tracking systems, and facial recognition technology**. It highlights the risks and potential consequences of mass data collection.

Key Learning Objectives:

1. Understand **how data brokers collect and sell personal information**.
2. Learn about **online tracking techniques** and how companies monitor user activity.
3. Analyze the **risks of facial recognition technology** and its impact on privacy.

Lesson Plan: How Your Data Is Collected and Used

Section 1: Data Brokers and Online Tracking

- **What Are Data Brokers?**
  - Companies that **collect, analyze, and sell** personal data.
  - Gather data from **public records, social media, purchases, and web activity**.
  - Sell information to **advertisers, financial institutions, and even law enforcement**.
- **How Online Tracking Works**
  - **Cookies** – Small files stored on devices to track user behavior.
  - **Fingerprinting** – Identifies users based on browser/device settings.
  - **Location Tracking** – Apps collect **real-time GPS data** to sell to third parties.
- **Who Uses Your Data?**
  - **Advertisers** – Targeted marketing based on browsing habits.
  - **Tech Companies** – Google, Facebook, and Amazon track users to improve algorithms.
  - **Government Agencies** – Data is sometimes accessed for surveillance or law enforcement.

Section 2: The Risks of Facial Recognition Technology

- **How Facial Recognition Works**
    - AI-powered software **scans and analyzes facial features**.
    - Used in **law enforcement, retail stores, airports, and social media**.
    - Cross-checks faces against **databases** to identify individuals.
- **Privacy Risks**
    - **Mass Surveillance** – Governments and corporations can monitor people in public spaces.
    - **Misidentification** – Errors in AI **lead to wrongful arrests or identity mismatches**.
    - **Lack of Consent** – Many users' faces are scanned without permission.
- **Who's Using Facial Recognition?**
    - **Law enforcement agencies** – Used to track suspects, but raises ethical concerns.
    - **Retailers and advertisers** – Track customer movements in stores.
    - **Airports and border control** – Used for security screenings.
- **How to Protect Your Privacy**
    - **Use a VPN and privacy tools** to limit tracking.
    - **Disable location tracking** on apps and browsers.
    - **Opt-out of data collection** where possible.

Video Script: Lesson 1 – How Your Data Is Collected and Used

[Opening Scene: Host standing in front of a city skyline with digital overlays]

HOST:
*"Your data is being tracked—right now. But by whom, and for what purpose? Today, we're breaking down **how companies collect your data, how facial recognition is used, and what you can do to protect yourself.**"*

[Cut to animated text: "Data Brokers and Online Tracking"]
*"First, let's talk about **data brokers**. These companies collect and sell your personal data—without you even realizing it."*

[Scene: Animated diagram showing data flow from websites, apps, and social media to data brokers]
*"Every time you **browse online, make a purchase, or sign up for an account**, your data is stored, analyzed, and sold to advertisers."*

[Scene: List of tracking methods appearing on screen]

- **Cookies** track which websites you visit.
- **Fingerprinting** collects data about your browser and device settings.
- **Location tracking** follows your **GPS movement** in real time.

[Scene: Footage of ads appearing after a user searches for shoes online]
"Ever wondered why ads seem to 'follow' you online? ***Companies track your searches and shopping habits*** *to target you with personalized ads."*

[Cut to animated text: "The Risks of Facial Recognition"]
"But tracking goes beyond just ads. ***Facial recognition technology*** *is being used everywhere, from* ***airports to police departments****."*

[Scene: AI scanning people's faces in a crowd]
"Here's how it works: AI scans your face, compares it to a database, and can ***identify you instantly****—sometimes without your consent."*

[Scene: List of privacy risks appearing on screen]

- **Mass Surveillance** – Government and corporations can track people in public spaces.
- **Misidentification** – AI errors **wrongfully identify individuals**.
- **Lack of Consent** – Your face could be in a database without you knowing.

[Scene: Footage of a protest against facial recognition technology]
"Critics argue that facial recognition ***violates privacy rights and increases the risk of government overreach****."*

[Cut to animated text: "How to Protect Your Data"]
"So, what can you do to protect yourself from mass data collection?"

[Scene: List of privacy tips appearing on screen]

1. **Use a VPN and privacy-focused browsers** (like Brave or DuckDuckGo).
2. **Turn off location tracking** on your phone and apps.
3. **Opt out of data collection** when possible.
4. **Cover your webcam and avoid uploading high-resolution selfies.**

[Cut to Host]
"Your data is valuable—don't give it away for free. What are you doing to protect your privacy? Let's discuss in the comments."

[End Scene: Call to Action]

- **Subscribe for More Privacy Tips!**
- **Download the Lesson Guide Below**
- **Take the Quiz to Test Your Knowledge**

Lesson 2: Protecting Yourself Online

This lesson explores essential strategies for safeguarding personal information online. It covers **password security, two-factor authentication (2FA), VPNs, ad blockers, and encrypted messaging**—all crucial tools for digital self-defense.

Key Learning Objectives:

1. Understand **password security best practices** and the importance of **two-factor authentication**.
2. Learn how **VPNs, ad blockers, and encrypted messaging tools** enhance online privacy.
3. Identify **common cyber threats** and how to mitigate them.

Lesson Plan: Protecting Yourself Online

Section 1: Password Security and Two-Factor Authentication

- **Why Password Security Matters**
  - Weak passwords are the leading cause of account breaches.
  - Cybercriminals use **brute-force attacks and credential stuffing** to hack accounts.
- **Best Practices for Strong Passwords**
  - Use **long passwords** (at least 12-16 characters).
  - Combine **uppercase, lowercase, numbers, and special characters**.
  - Avoid using **personal information** (birthdays, pet names, etc.).
  - Use a **password manager** to store and generate passwords securely.
- **Understanding Two-Factor Authentication (2FA)**
  - Adds an extra layer of security beyond a password.
  - Methods include:
    - **SMS-based 2FA** (least secure, but better than nothing).
    - **App-based 2FA** (Google Authenticator, Authy).
    - **Hardware security keys** (YubiKey, Titan Security Key).
- **How to Enable 2FA**
  - Go to account settings on major platforms (Google, Facebook, banking apps).

    - Choose a secure 2FA method (preferably app-based or hardware key).
    - Store backup codes safely in case you lose access.

Section 2: VPNs, Ad Blockers, and Encrypted Messaging

- **What is a VPN and Why Use It?**
    - **VPN (Virtual Private Network)** encrypts your internet connection and hides your IP address.
    - Prevents **ISP tracking, government surveillance, and hacking on public Wi-Fi**.
    - Recommended VPNs: **ProtonVPN, Mullvad, NordVPN** (avoid free VPNs—they often log data!).
- **Ad Blockers and Privacy Extensions**
    - **Why block ads?** Many contain tracking scripts that monitor online behavior.
    - Recommended tools:
        - **uBlock Origin** (ad and tracker blocker)
        - **Privacy Badger** (prevents hidden trackers)
        - **DuckDuckGo Privacy Essentials** (blocks hidden data collection)
- **Encrypted Messaging for Secure Communication**
    - **Why encryption matters**: Stops third parties (hackers, governments, advertisers) from reading private messages.
    - Recommended apps:
        - **Signal** (best for end-to-end encryption)
        - **ProtonMail** (encrypted email service)
        - **WhatsApp** (encrypted but owned by Meta—use with caution)
    - Avoid: **SMS, Facebook Messenger (unsecured by default).**

Video Script: Lesson 2 – Protecting Yourself Online

[Opening Scene: Host at a coffee shop using a laptop]

HOST:
"Ever used public Wi-Fi at a café? You might be exposing your data to hackers. Today, we're learning ***how to protect yourself online****—from* ***password security to encrypted messaging.****"*

[Cut to animated text: "Password Security and Two-Factor Authentication"]

“First up: passwords. A weak password is like leaving your front door unlocked. Cybercriminals use ***brute-force attacks*** *to guess passwords and gain access to your accounts.”*

[Scene: Visual of a hacker running a brute-force attack]

“Here’s how to create ***a strong password****:”*

- **Use at least 12-16 characters**.
- **Include uppercase, lowercase, numbers, and symbols**.
- **Never reuse passwords across multiple sites**.
- **Use a password manager** (like Bitwarden or 1Password).

[Cut to animated text: “Two-Factor Authentication (2FA)”]

“Even a strong password isn’t enough. That’s why you need ***two-factor authentication (2FA).****”*

[Scene: Side-by-side comparison of login with and without 2FA]

“2FA requires a second verification step—like a ***security code from an app or a physical security key.****”*

[Cut to animated text: “Using a VPN for Privacy”]

“A ***VPN (Virtual Private Network)*** *encrypts your internet traffic, hiding your IP address from hackers, advertisers, and even your internet provider.”*

[Scene: VPN app being turned on, IP address changing]

“With a VPN, you can browse anonymously and avoid tracking. ***Top VPNs include ProtonVPN, Mullvad, and NordVPN.****”*

[Cut to animated text: “Blocking Trackers and Ads”]

“Did you know ads don’t just annoy you—they track you? That’s why using an ***ad blocker*** *is essential.”*

[Scene: Browser before and after enabling uBlock Origin]

“Recommended ad blockers: ***uBlock Origin, Privacy Badger, DuckDuckGo Privacy Essentials.****”*

[Cut to animated text: “Encrypted Messaging: Keeping Conversations Private”]

“Not all messaging apps are secure. ***Hackers, advertisers, and even governments*** *can access unencrypted messages.”*

[Scene: Comparison of unsecured vs. encrypted messages]

“For private conversations, use ***Signal or ProtonMail****—both provide* ***end-to-end encryption****.”*

[Closing Scene: Host summarizing tips]

“Staying private online doesn’t have to be complicated. ***Use strong passwords, enable 2FA, browse with a VPN, and switch to encrypted messaging.****”*

“What’s your top online privacy tip? Let’s discuss in the comments!”

[End Scene: Call to Action]

- **Subscribe for More Cybersecurity Tips!**
- **Download the Lesson Guide Below**
- **Take the Quiz to Test Your Knowledge**

Lesson 3: The Role of Big Tech and Surveillance

This lesson explores **how major tech companies track personal data and the role of government surveillance laws**, particularly the **Patriot Act**. Understanding these topics helps individuals make informed choices about their digital privacy and personal data protection.

Key Learning Objectives:

1. Understand **what major tech companies collect** about users and how they use this data.
2. Learn how **government surveillance programs operate** under laws like the **Patriot Act**.
3. Identify ways to **limit exposure to corporate and government tracking**.

Lesson Plan: The Role of Big Tech and Surveillance

Section 1: What Major Companies Track About You

- **Who Are the Biggest Data Collectors?**

    - Google, Facebook (Meta), Apple, Amazon, Microsoft.
    - Social media platforms, search engines, online shopping sites, and cloud services.
- **What Data is Being Tracked?**
    - **Search history & browsing activity** (Google, Bing, DuckDuckGo).
    - **Location data** (GPS tracking from phones, smart devices).
    - **Shopping and spending habits** (Amazon, credit card tracking).
    - **Personal messages & calls** (Meta Messenger, WhatsApp metadata).
    - **Device data & app usage** (Smartphones, smart speakers, fitness trackers).
- **Why Do Companies Collect This Data?**
    - **Targeted advertising** – Personalized ads based on browsing history.
    - **AI & Algorithm Training** – Improving services by analyzing user behavior.
    - **Selling data to third parties** – Companies profit from personal information.
- **How to Reduce Tracking?**
    - Adjust **privacy settings** on devices and apps.
    - Use **privacy-focused browsers** (Brave, Firefox, Tor).
    - Disable **location tracking** on apps and social media.
    - Avoid using **social media sign-ins** for other websites.

Section 2: Government Surveillance and the Patriot Act

- **What is the Patriot Act?**
    - A law passed after **9/11 to expand government surveillance powers**.
    - Allows law enforcement to **monitor phone calls, emails, and internet activity**.
- **How Does the Government Track Citizens?**
    - **Phone Metadata Collection** – NSA tracks phone numbers and call duration.
    - **Internet Monitoring** – Government agencies track **emails, web traffic, and social media**.
    - **Facial Recognition & CCTV Surveillance** – Used in public spaces and airports.
    - **Data Requests from Big Tech** – Government subpoenas user data from Google, Apple, and Facebook.
- **Controversies and Privacy Concerns**
    - **Edward Snowden's Revelations (2013)** – Leaked NSA documents exposing mass surveillance.
    - **Lack of Transparency** – Many surveillance programs operate **without public knowledge**.
    - **Impact on Free Speech** – Fear of being monitored can **limit open discussions** online.
- **How to Protect Yourself?**
    - Use **encrypted messaging apps** (Signal, ProtonMail).
    - Avoid public Wi-Fi without a **VPN**.
    - Limit **social media sharing** of personal information.

- Read privacy policies before signing up for services.

Video Script: Lesson 3 – The Role of Big Tech and Surveillance

[Opening Scene: Host standing in front of a cityscape with digital overlays]

HOST:
*"Every time you search online, shop, or use social media—someone is watching. But who? Today, we're diving into **how Big Tech tracks your data and how government surveillance laws impact your privacy.**"*

[Cut to animated text: "What Major Companies Track About You"]
*"Tech giants like **Google, Facebook, Amazon, and Apple** collect **huge amounts of data**—but do you know how much?"*

[Scene: Animated diagram showing data collection points]

- **Search history** – Google tracks every query.
- **Location data** – GPS logs your movements.
- **Shopping habits** – Amazon monitors your purchases.
- **Private messages** – Some apps scan texts for advertising purposes.

[Scene: Footage of a user seeing an ad for something they just searched]
*"Ever noticed ads **following you around** after searching for a product? That's because **companies use your data to target you with personalized ads.**"*

[Cut to animated text: "How to Reduce Tracking"]
"So, how can you protect your privacy?"

[Scene: List of privacy tips appearing on screen]

1. **Use privacy-focused browsers** (Brave, Firefox, DuckDuckGo).
2. **Adjust app permissions** to limit data collection.
3. **Disable location tracking** when not needed.
4. **Don't use social media logins** for other websites.

[Cut to animated text: "Government Surveillance and the Patriot Act"]
*"But it's not just companies tracking you. **The government also has access to a massive amount of personal data.**"*

[Scene: Footage of CCTV cameras scanning a crowd]
*"After 9/11, the **Patriot Act** gave U.S. agencies **sweeping surveillance powers.**"*

[Scene: Diagram of surveillance methods]

- **Phone metadata collection** – Who you call and when.
- **Internet monitoring** – Emails, social media, and web searches.
- **Facial recognition** – Tracking individuals in public places.
- **Big Tech cooperation** – Companies sharing user data with law enforcement.

[Scene: News clip of Edward Snowden's NSA leaks]
*"In 2013, **Edward Snowden** revealed that the NSA was spying on millions of Americans—without their knowledge."*

[Cut to animated text: "How to Protect Your Data from Surveillance"]

1. **Use encrypted messaging apps** (Signal, ProtonMail).
2. **Avoid public Wi-Fi** unless using a VPN.
3. **Turn off location tracking** on your phone.
4. **Be mindful of what you share online.**

[Cut to Host]
*"We live in a world where data is constantly being collected. The question is—**how much control do you have over your own information?** Let's talk about it in the comments."*

[End Scene: Call to Action]

- **Subscribe for More Privacy Tips!**
- **Download the Lesson Guide Below**
- **Take the Quiz to Test Your Knowledge**

Lesson 4: Digital Rights and Advocacy

This lesson explores **digital rights, data privacy advocacy, and how individuals can take control of their online data**. It covers **how to request data removal from companies and governments** and highlights **organizations working to protect digital privacy and internet freedoms**.

Key Learning Objectives:

1. Understand **how to request personal data removal** from websites, data brokers, and online platforms.
2. Learn about **laws that protect digital rights**, such as the **GDPR (General Data Protection Regulation)** and **CCPA (California Consumer Privacy Act)**.
3. Identify **key organizations advocating for digital privacy and free internet access**.

Lesson Plan: Digital Rights and Advocacy

Section 1: How to Request Data Removal

- **Why Does Your Data Exist Online?**
    - Websites, apps, and data brokers collect **personal data from social media, search engines, and public records**.
    - Even **deleted accounts may still store data** in archives.
- **Your Right to Data Removal**
    - **GDPR (EU law)** – Grants individuals the **"right to be forgotten."**
    - **CCPA (California law)** – Allows residents to **opt-out of data collection and request deletion.**
- **Steps to Request Data Removal**
    - **Find out where your data is stored** (Google yourself, use data removal tools like **HaveIBeenPwned** or **DeleteMe**).
    - **Check if the company offers an opt-out option** (Visit privacy policies, look for **data removal forms**).
    - **Submit a formal request** (Many sites require an **email or form submission** to delete data).
    - **Follow up if necessary** (Companies may delay or deny requests—be persistent).
- **Key Websites for Data Removal Requests**
    - **Google Removal Tool** – Request deletion of sensitive search results.
    - **Facebook & Instagram Privacy Settings** – Adjust data-sharing settings.
    - **Data Broker Opt-Outs** – Some brokers (e.g., **Spokeo, Whitepages, MyLife**) allow removals.

Section 2: Organizations Fighting for Digital Rights

- **Why Digital Rights Matter**
    - Protects **free speech, privacy, and online security**.
    - Prevents **mass surveillance and corporate exploitation of personal data**.
- **Major Digital Rights Organizations**
    - **Electronic Frontier Foundation (EFF)** – Fights for digital privacy, free speech, and encryption rights.
    - **Access Now** – Advocates for internet freedoms worldwide.
    - **Fight for the Future** – Campaigns against censorship, surveillance, and online tracking.
    - **Privacy International** – Works on global privacy rights and government surveillance issues.
    - **The Tor Project** – Develops **anonymous browsing tools** to protect privacy.
- **How You Can Get Involved**

    - **Sign petitions** supporting digital rights policies.
    - **Donate or volunteer** for privacy advocacy groups.
    - **Use encrypted communication tools** to support digital privacy.
    - **Spread awareness** by educating others on digital security practices.

Video Script: Lesson 4 – Digital Rights and Advocacy

[Opening Scene: Host standing in front of a computer screen with privacy settings open]

HOST:
*"Have you ever searched for your name online—only to find personal information you never shared? Today, we're talking about **how to remove your data from the internet and the organizations fighting for your digital rights.**"*

[Cut to animated text: "How to Request Data Removal"]
*"Many companies store **years' worth of personal data**—even after you delete an account. But you have the right to take control."*

[Scene: Screenshot of a Google search showing personal info]
*"Your personal information can appear on **search engines, social media, and data broker websites** without your permission."*

[Scene: Breakdown of data removal steps appearing on screen]

1. **Find where your data is stored** (Google your name, check data broker sites).
2. **Check for opt-out options** on websites.
3. **Submit a formal request** to remove your data.
4. **Follow up** to ensure compliance.

[Scene: Example of a user submitting a data removal request to a data broker]
*"Some companies allow **opt-outs**, but others make the process difficult. Stay persistent!"*

[Cut to animated text: "Organizations Fighting for Digital Rights"]
*"Fortunately, there are groups **fighting for stronger digital privacy laws**."*

[Scene: Logos of EFF, Access Now, Fight for the Future, Privacy International]

- **EFF (Electronic Frontier Foundation)** – Defends digital privacy and encryption.
- **Access Now** – Advocates for human rights in the digital space.
- **Fight for the Future** – Organizes protests against government surveillance.

[Scene: Footage of a digital rights protest]
*"These organizations help **fight against mass surveillance, corporate tracking, and government overreach.**"*

[Cut to animated text: “How You Can Get Involved”]

1. **Sign petitions** supporting digital rights laws.
2. **Use privacy-friendly tools** like encrypted messaging and VPNs.
3. **Donate or volunteer** for advocacy groups.
4. **Educate others** on the importance of digital privacy.

[Cut to Host]
"Your online privacy is in your hands. Have you ever tried removing your data from the internet? Let’s discuss in the comments."

[End Scene: Call to Action]

- **Subscribe for More Privacy Tips!**
- **Download the Lesson Guide Below**
- **Take the Quiz to Test Your Knowledge**