

Tiết 5

BÀI 3: PHÒNG CHỐNG TỆ NẠN XÃ HỘI Ở VIỆT NAM TRONG THỜI KỲ HỘI NHẬP QUỐC TẾ

(2 tiết)

I. MỤC TIÊU

1. Kiến thức:

- Nêu được một số loại hình tội phạm và tệ nạn xã hội; hình thức, cách thức hoạt động của các loại tội phạm và tệ nạn xã hội, đặc biệt là tội phạm công nghệ cao ở Việt Nam trong thời kì hội nhập quốc tế.

- Nêu được quy định của pháp luật về phòng chống tệ nạn xã hội, phòng chống tội phạm công nghệ cao.

2. Năng lực:

Năng lực chung: Năng lực tự học; Năng lực hợp tác; Năng lực thẩm mỹ; Năng lực giao tiếp.

- Năng lực số:

- Phân tích và đánh giá được độ tin cậy của các nguồn thông tin về an ninh mạng và tệ nạn xã hội trên các cổng thông tin điện tử và mạng xã hội. (1.2.NC1a)

- Áp dụng linh hoạt các biện pháp bảo mật như xác thực hai yếu tố, quản lý mật khẩu mạnh để bảo vệ dữ liệu cá nhân và danh tính số trước các thủ đoạn lừa đảo công nghệ cao. (4.2.NC1a)

- Sử dụng công nghệ số và mạng xã hội để tương tác, chia sẻ thông tin tuyên truyền, thực hiện trách nhiệm công dân trong phòng chống tội phạm công nghệ cao. (2.3.NC1a)

- Năng lực trí tuệ nhân tạo (AI):

- 11.B2.1: Nhận biết và phân loại được các rủi ro hoặc sự cố liên quan đến việc sử dụng AI có thể dẫn đến vi phạm quy định của nhà trường hoặc các văn bản pháp luật liên quan (như công nghệ Deepfake giả mạo khuôn mặt/giọng nói, chatbot lừa đảo).

- 11.C2.1: Trình bày được cách AI hỗ trợ quá trình học tập và tìm hiểu quy định pháp luật.

- 11.C3.1: Xác định và vận dụng được một số kỹ thuật prompt nâng cao để tra cứu quy định pháp luật và giải quyết các bài tập tình huống phòng chống tội phạm.

- Năng lực chuyên biệt:

- Tuyên truyền các biện pháp phòng, chống, không để các đối tượng phạm tội móc nối, lôi kéo bản thân và gia đình vi phạm pháp luật.

- Vận dụng được các kiến thức đã học vào trong công cuộc bảo vệ Tổ quốc.

Mục tiêu điều chỉnh cho học sinh khuyết tật (Khuyết tật vận động, Khuyết tật nói):

+ *Nêu/chỉ ra được một số loại tội phạm, tệ nạn xã hội và thủ đoạn lừa đảo qua mạng ở mức độ đơn giản thông qua hình ảnh trực quan, thẻ từ hoặc câu hỏi lựa chọn Trắc nghiệm/Đúng-Sai.*

+ *Thực hiện tương tác, trả lời câu hỏi bằng cách tích chọn trên thiết bị số, giơ thẻ đáp án hoặc chỉ tay thay cho việc phát biểu trực tiếp hay thao tác viết phức tạp.*

3. Phẩm chất:

- Xác định và thực hiện được ý thức trách nhiệm của công dân trong quản lý, xây dựng và bảo vệ biên giới quốc gia, giữ gìn an ninh trật tự xã hội.

II. THIẾT BỊ DẠY HỌC VÀ HỌC LIỆU

1. Giáo viên:

- Chuẩn bị phòng học, trang phục của GV và HS đúng theo quy định.
- Nghiên cứu bài 3 trong SGK, máy tính nối mạng, máy chiếu/bảng tương tác, các phần mềm/ứng dụng số (Padlet/Mentimeter, công cụ AI).
- Phiếu học tập, thẻ đáp án/thẻ từ trực quan hỗ trợ HSKT (vận động, nói).

2. Học sinh:

- Đọc trước bài 3 trong SGK, chuẩn bị thiết bị di động/máy tính có kết nối mạng (nếu GV yêu cầu).

III. TIẾN TRÌNH DẠY HỌC

A. HOẠT ĐỘNG MỞ ĐẦU (5 phút)

a. Mục tiêu: Tạo tâm thế cho học sinh đi vào tìm hiểu bài mới; tương tác thông qua môi trường số để nhận diện các thủ đoạn lừa đảo trực tuyến phổ biến hiện nay. (2.1.NC1a)

- [Dành cho HSKT hòa nhập]: Tham gia hoạt động khởi động bằng cách quan sát hình ảnh và tích chọn đáp án trên ứng dụng hoặc giơ thẻ chọn thay cho việc đứng dậy phát biểu.*

b. Nội dung: Làm thủ tục lên lớp; giới thiệu nội dung bài mới; Kiểm tra bài cũ thông qua câu hỏi khởi động.

c. Sản phẩm: Ý kiến đóng góp của HS trên ứng dụng số, câu trả lời trực tuyến của HS.

d. Tổ chức thực hiện:

- Làm thủ tục lên lớp: tên bài, mục đích yêu cầu, nội dung trọng tâm, thời gian, tổ chức phương pháp.
- Giới thiệu bài mới thông qua phần khởi động:

- GV hướng dẫn HS truy cập đường link hoặc quét mã QR để vào bảng tương tác Padlet, thực hiện chia sẻ và phân loại các hình thức lừa đảo trực tuyến theo nhóm (lừa đảo tài chính, đánh cắp thông tin, giả mạo cơ quan chức năng). (2.1.NC1a)

- GV sử dụng công cụ tương tác trực tuyến (như Padlet hoặc Mentimeter) để HS cùng liệt kê nhanh các thủ đoạn lừa đảo qua mạng mà các em đã gặp hoặc biết đến.

- [Dành cho HSKT hòa nhập]: GV phân công bạn cùng bàn hỗ trợ HSKT vận động thao tác bấm chọn trên điện thoại/máy tính; HSKT nói thực hiện trả lời bằng cách chỉ vào thẻ biểu tượng ứng với loại hình lừa đảo.*

1. Kể tên một số thủ đoạn của tội phạm lừa đảo trên không gian mạng mà em biết.

2. Em hãy cho biết tác hại của một số loại tệ nạn xã hội ở nước ta hiện nay.

B. HOẠT ĐỘNG HÌNH THÀNH KIẾN THỨC MỚI (30 phút)

Hoạt động 1: I. MỘT SỐ NỘI DUNG CƠ BẢN VỀ TỘI PHẠM (15 phút)

a. Mục tiêu: HS tìm hiểu về khái niệm tội phạm, một số loại tội phạm và cách thức hoạt động phổ biến của tội phạm; truy cập và duyệt tìm kiếm thông tin về quy định pháp luật trên các trang thông tin điện tử chính thống của Chính phủ. (1.1.NC1a) Phân tích và đánh giá độ tin cậy của các nội dung văn bản pháp luật thu thập được trên Internet. (1.2.NC1a) **Vận dụng kỹ thuật prompt nâng cao để tra cứu văn bản quy phạm pháp luật và so sánh các loại vi phạm pháp luật.** (11.C3.1, 11.C2.1)

- [Dành cho HSKT hòa nhập]: Nhận biết được khái niệm tội phạm và một số loại tội phạm phổ biến thông qua bảng tóm tắt ngắn và hình ảnh trực quan.*

b. Nội dung: HS đọc SGK, sử dụng thiết bị số và công cụ AI tra cứu, thảo luận để hoàn thành nhiệm vụ GV giao.

c. Sản phẩm: Bảng tóm tắt hoặc sơ đồ tư duy kỹ thuật số tổng hợp khái niệm, các loại tội phạm và cách thức hoạt động phổ biến.

d. Tổ chức thực hiện:

HOẠT ĐỘNG CỦA HS - GV	SẢN PHẨM DỰ KIẾN
Bước 1: Chuyển giao nhiệm vụ: GV yêu cầu HS trả lời các câu hỏi: Câu hỏi 1: Tội phạm là gì? Câu hỏi 2: Em hãy nêu một số loại tội phạm và cách thức hoạt động phổ biến của tội phạm? GV hướng dẫn HS <u>sử dụng thiết bị số truy cập vào các trang web chính thống của Chính phủ hoặc Thư viện Pháp luật để tra cứu chính xác định nghĩa tội phạm theo</u>	I. MỘT SỐ VẤN ĐỀ CHUNG VỀ TỘI PHẠM 1. Khái niệm tội phạm - Tội phạm là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự hoặc pháp nhân thương mại thực hiện một cách cố ý hoặc vô ý, xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Tổ quốc, xâm phạm

<u>Bộ luật Hình sự hiện hành.</u> (1.1.NC1a) GV hướng dẫn HS thực hành đặt câu lệnh (prompt) nâng cao trên công cụ AI: "Tóm tắt các đặc điểm chính của tội phạm theo Bộ luật Hình sự Việt Nam và so sánh với các loại vi phạm pháp luật thông thường, trình bày dưới dạng bảng" để hỗ trợ tổng hợp thông tin. (11.C3.1, 11.C2.1) Bước 2: Thực hiện nhiệm vụ: HS đọc SGK, kết hợp tra cứu số và công cụ AI để chuẩn bị nội dung trả lời. HS <u>đôi chiếu, phân tích và đánh giá độ tin cậy của nội dung do AI cung cấp so với SGK và văn bản pháp luật chính thống trên Cổng thông tin điện tử Chính phủ.</u> (1.2.NC1a) <i>[Dành cho HSKT hòa nhập]: HSKT theo dõi nội dung tóm tắt trên màn hình chiếu, trả lời câu hỏi bằng phiếu học tập trắc nghiệm điền từ hoặc chỉ định đáp án đúng dưới sự hướng dẫn của GV/bạn cùng bàn.</i> Bước 3: Báo cáo, thảo luận: Đại diện HS trình bày câu trả lời hoặc trình chiếu sơ đồ tư duy kỹ thuật số tổng hợp các loại tội phạm; cả lớp nhận xét và bổ sung. Bước 4: Kết luận, nhận định: GV kết luận kiến thức, chốt các nội dung trọng tâm. HS nghe và ghi chép ý chính.	chế độ chính trị, chế độ kinh tế, nền văn hoá, quốc phòng, an ninh, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, xâm phạm quyền con người, quyền, lợi ích hợp pháp của công dân, xâm phạm những lĩnh vực khác của trật tự pháp luật xã hội chủ nghĩa mà theo quy định của Bộ luật này phải bị xử lý hình sự. 2. Một số loại tội phạm - Một số loại tội phạm hiện nay như: giết người, cố ý gây thương tích, cướp tài sản, trộm cắp tài sản, mua bán trái phép chất ma túy, tổ chức đua xe trái phép, đánh bạc, tổ chức đánh bạc,... 3. Cách thức hoạt động phổ biến của các loại tội phạm - Cấu kết thành các băng nhóm, tổ chức để hoạt động. - Sử dụng vũ khí, công cụ, phương tiện trong hoạt động phạm tội. - Hoạt động mang tính lưu động trên phạm vi nhiều tỉnh, thành phố, xuyên quốc gia và có tính chất quốc tế. - Sử dụng công nghệ cao trong quá trình hoạt động phạm tội.
--	--

Hoạt động 2: II. PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO (15 phút)

a. Mục tiêu: HS nêu được các hình thức, thủ đoạn của tội phạm công nghệ cao và quy định pháp luật về phòng chống tội phạm công nghệ cao; áp dụng các biện pháp an toàn để bảo vệ dữ liệu cá nhân và danh tính số. (4.2.NC1a) Sử dụng công nghệ số để tương tác, tuyên truyền trách nhiệm công dân trong phòng chống tội phạm mạng. (2.3.NC1a) **Nhận biết và phân loại được các rủi ro từ việc lạm dụng AI (như Deepfake, Chatbot lừa đảo) gây vi phạm pháp luật.** (11.B2.1)

- [Dành cho HSKT hòa nhập]: Nhận diện được các thủ đoạn lừa đảo qua mạng đơn giản và nêu được biện pháp tự bảo vệ tài khoản cá nhân thông qua tranh ảnh hoặc phiếu trắc nghiệm.*

b. Nội dung: HS khai thác tài liệu, thảo luận nhóm, phân tích tình huống thực tế về tội phạm công nghệ cao và giải pháp bảo vệ dữ liệu.

c. Sản phẩm: Kết quả thảo luận nhóm, danh sách các giải pháp an toàn thông tin cá nhân và quy tắc phòng tránh tội phạm công nghệ cao.

d. Tổ chức thực hiện:

HOẠT ĐỘNG CỦA HS - GV	SẢN PHẨM DỰ KIẾN
Bước 1: Chuyển giao nhiệm vụ: GV chia lớp thành các nhóm, giao nhiệm vụ thảo luận: - Nhóm 1, 2: Nêu các hình thức, thủ đoạn hoạt động phổ biến của tội phạm công nghệ cao hiện nay. - Nhóm 3, 4: Nêu các quy định cơ bản của pháp luật về phòng chống tội phạm công nghệ cao và trách nhiệm của học sinh. GV yêu cầu các nhóm tìm hiểu và phân tích rủi ro liên quan đến việc các đối tượng xấu sử dụng AI (như giả mạo khuôn mặt/giọng nói Deepfake) để lừa đảo chiếm đoạt tài sản. (11.B2.1) GV hướng dẫn HS <u>thảo luận và đề xuất các biện pháp bảo vệ dữ liệu cá nhân, danh tính số (mật khẩu mạnh, bảo mật 2 lớp, không chia sẻ OTP) để không bị tội phạm mạng lợi dụng.</u> (4.2.NC1a) Bước 2: Thực hiện nhiệm vụ: HS trong nhóm thảo luận, tổng hợp ý kiến vào phiếu học tập hoặc bài trình chiếu. HS <u>thiết kế một thông điệp tuyên truyền số ngắn để thực hiện trách nhiệm công dân trong việc cảnh báo tội phạm công nghệ cao trên mạng xã hội.</u> (2.3.NC1a) <i>[Dành cho HSKT hòa nhập]: HSKT tham gia nhóm bằng cách dán thẻ bài tập, chỉ tay chọn các biểu tượng hành vi an toàn/không an toàn trên không gian mạng dưới sự trợ giúp của bạn học.</i> Bước 3: Báo cáo, thảo luận: Đại diện các nhóm báo cáo kết quả thảo luận. Các nhóm khác lắng nghe, phản biện và đóng góp ý kiến. Bước 4: Kết luận, nhận định: GV nhận xét thái độ làm việc, đánh giá kết quả	II. PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO 1. Một số hành vi vi phạm pháp luật sử dụng công nghệ cao - Lừa đảo chiếm đoạt tài sản trên không gian mạng. - Đánh cắp, mua bán, sử dụng trái phép thông tin, dữ liệu cá nhân. - Phát tán phần mềm độc hại, tấn công mạng, phá hoại hệ thống thông tin. - Giả mạo các cơ quan nhà nước, tổ chức, cá nhân (sử dụng AI Deepfake tạo hình ảnh, giọng nói giả) để lừa đảo. 2. Quy định của pháp luật về phòng, chống tội phạm công nghệ cao - Trích dẫn các điều luật cơ bản trong Luật An ninh mạng và Bộ luật Hình sự về xử lý vi phạm trên không gian mạng. 3. Trách nhiệm của học sinh - Chấp hành nghiêm các quy định của pháp luật về an ninh mạng. - Bảo vệ mật khẩu, thông tin cá nhân và tài khoản số. - Tích cực tuyên truyền, cảnh báo thủ đoạn tội phạm cho người thân và cộng đồng. - Tố giác kịp thời các hành vi vi

thảo luận của các nhóm, chốt lại nội dung kiến thức trọng tâm.	phạm pháp luật trên không gian mạng tới cơ quan chức năng.
--	--

a. Mục tiêu:

- HS hiểu được khái niệm tội phạm công nghệ cao, cách thức hoạt động và các quy định pháp luật về xử lý tội phạm công nghệ cao; biết thực hiện các biện pháp bảo mật thông tin cá nhân và phòng tránh lừa đảo trên không gian mạng. (4.2.NC1a)

- **Phân tích được các rủi ro tiềm ẩn khi đối tượng xấu sử dụng AI tạo sinh để lừa đảo chiếm đoạt tài sản. (11.A2.1)**

- *[Dành cho HSKT hòa nhập]: Chỉ ra được 2-3 quy tắc an toàn cơ bản khi dùng mạng xã hội (không chia sẻ OTP, không click link lạ) thông qua bảng tranh minh họa; HSKT nói/vận động có thể thực hiện bằng cách chỉ vào thẻ tranh hoặc dùng bảng đáp án ĐÚNG/SAI dưới sự hỗ trợ của bạn học.*

b. Nội dung: HS quan sát video, phân tích các kịch bản lừa đảo thực tế, thảo luận quy tắc bảo mật thông tin và tác động của AI.

c. Sản phẩm: Câu trả lời của HS về phương thức phòng chống tội phạm công nghệ cao và bảng quy tắc an toàn thông tin cá nhân.

d. Tổ chức thực hiện:

HOẠT ĐỘNG CỦA HS - GV	SẢN PHẨM DỰ KIẾN
Bước 1: Chuyển giao nhiệm vụ: GV yêu cầu HS trả lời các câu hỏi: Câu hỏi 3: Thế nào là tội phạm sử dụng công nghệ cao? Em hãy nêu một số cách thức hoạt động phổ biến và một số hành vi phạm tội của tội phạm sử dụng công nghệ cao. Câu hỏi 4: Em hãy nêu các quy định của pháp luật về phòng chống tội phạm sử dụng công nghệ cao và các hành vi bị nghiêm cấm? GV trình chiếu video clip minh họa về một vụ án tội phạm công nghệ cao điển hình. GV phân tích rủi ro tiềm ẩn khi tội phạm lừa đảo sử dụng công nghệ AI tạo sinh (như Deepfake tạo hình ảnh/giọng nói giả mạo, chatbot lừa đảo) để chiếm đoạt tài sản (11.A2.1). GV hướng dẫn HS phân tích các kỹ thuật tấn công phi kỹ thuật (Social Engineering), kịch bản lừa đảo (phishing, link độc hại, chiếm đoạt tài khoản) và <u>thực hành xây</u>	II. PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO 1. Khái niệm tội phạm sử dụng công nghệ cao - Tội phạm sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội do người có năng lực trách nhiệm hình sự thực hiện bằng việc cố ý sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ thông tin ở trình độ cao tác động trái pháp luật đến thông tin số được lưu trữ, xử lý, truyền tải trong hệ thống máy tính, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền, lợi ích hợp pháp của các tổ chức, cá nhân và theo quy định của Bộ luật Hình sự phải bị xử lý hình sự. 2. Một số hành vi phạm tội sử dụng công nghệ cao ở Việt Nam hiện nay - Lừa đảo chiếm đoạt tài sản trên không gian mạng.

<u>dụng quy trình xử lý khi bị lộ thông tin cá nhân, thực hiện quy tắc "vàng" bảo vệ dữ liệu cá nhân như không chia sẻ OTP, bất xác thực 2 lớp. (4.2.NC1a)</u> Bước 2: Thực hiện nhiệm vụ: HS theo dõi video, thảo luận nhóm phân tích phương thức gây án và các giải pháp phòng tránh. <i>[Dành cho HSKT hòa nhập]: HSKT được cung cấp phiếu học tập in sẵn các quy tắc an toàn; HSKT chỉ cần tích chọn đáp án ĐÚNG/SAI hoặc sử dụng bảng thẻ chữ ĐÚNG/SAI để trả lời (đặc biệt phù hợp với HSKT khuyết tật nói/vận động) dưới sự trợ giúp của bạn học.</i> Bước 3: Báo cáo, thảo luận: Đại diện các nhóm trình bày kết quả phân tích kịch bản lừa đảo và cách phòng chống. HS <u>đề xuất các biện pháp bảo vệ danh tính số và thực hiện trách nhiệm tuyên truyền phòng chống tội phạm công nghệ cao trong nhà trường và cộng đồng.</u> (2.3.NC1a) Bước 4: Kết luận, nhận định: GV chốt lại các quy tắc "vàng" để bảo vệ an toàn thông tin cá nhân trên môi trường số. HS nghe và ghi chép các quy định pháp luật quan trọng.	- Đánh bạc, tổ chức đánh bạc trên không gian mạng. - Môi giới mại dâm trên không gian mạng. - Lợi dụng các quyền tự do, dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân. - Làm, tàng trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam. 3. Quy định của pháp luật về phòng chống tội phạm sử dụng công nghệ cao - Một số hành vi vi phạm pháp luật về phòng, chống tội phạm sử dụng công nghệ cao bị nghiêm cấm: + Sản xuất, mua bán, trao đổi hoặc tặng, cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật. + Phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. + Cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. + Đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. + Xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác. + Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản. + Thu thập, tàng trữ, trao đổi, mua bán, công khai hoá trái phép thông tin về tài khoản ngân hàng. + Sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh.
---	---

C. HOẠT ĐỘNG LUYỆN TẬP

a. Mục tiêu:

- Củng cố kiến thức, giúp học sinh luyện tập và khắc sâu các kiến thức đã học về phòng chống tội phạm sử dụng công nghệ cao.

- Phân tích và đánh giá độ tin cậy của các thông tin, hình ảnh, âm thanh giả mạo trên không gian mạng để phòng tránh rủi ro lừa đảo. (1.2.NC1a)

- **Nhận biết và phân loại được các rủi ro hoặc sự cố liên quan đến việc sử dụng AI (Deepfake) có thể dẫn đến vi phạm quy định của nhà trường hoặc các văn bản pháp luật liên quan.** (11.B2.1)

- *[Dành cho HSKT hòa nhập]:* Nêu được ít nhất 1-2 hành vi vi phạm pháp luật về công nghệ cao thông qua việc lựa chọn phương án đúng trên phiếu học tập/bảng trả lời chọn đáp án A/B/C/D, không bắt buộc phát biểu bằng lời nói.

b. Nội dung:

- HS phân tích tình huống video/âm thanh giả mạo (Deepfake), thảo luận về trách nhiệm đạo đức của người tạo ra công cụ AI và cách thức nhận diện các dấu hiệu giả mạo để phòng tránh rủi ro.

- HS tham gia trò chơi trắc nghiệm trên nền tảng Kahoot hoặc Quizizz để luyện tập nhận diện các hành vi vi phạm pháp luật về tội phạm công nghệ cao và trả lời câu hỏi: Kể tên các hành vi vi phạm pháp luật về phòng chống tội phạm sử dụng công nghệ cao?

c. Sản phẩm:

- Kết quả thảo luận tình huống Deepfake và câu trả lời hoàn thành bài tập/trò chơi trắc nghiệm của học sinh.

d. Tổ chức thực hiện:

Hoạt động của giáo viên	Hoạt động của học sinh
Bước 1: Chuyển giao nhiệm vụ - GV đưa ra một tình huống video/âm thanh giả mạo (Deepfake) và yêu cầu HS thảo luận về trách nhiệm đạo đức của người tạo ra công cụ AI này và nhận biết, phân loại các rủi ro liên quan đến nội dung do AI tạo sinh để phòng tránh vi phạm pháp luật và rủi ro lừa đảo (11.B2.1). - GV tổ chức trò chơi trắc nghiệm trên nền tảng Kahoot hoặc Quizizz để HS luyện tập nhận diện các hành vi vi phạm pháp luật về tội phạm công nghệ cao. - <i>[Dành cho HSKT hòa nhập]:</i> GV cung cấp bảng lựa chọn đáp án A/B/C/D hoặc thẻ quan sát cho HS khuyết tật nói/vận động để tham gia chọn đáp án mà không gặp trở ngại về giao tiếp.	- HS lắng nghe, quan sát video tình huống và nhận nhiệm vụ từ giáo viên. - Chuẩn bị thiết bị di động/máy tính có kết nối mạng để sẵn sàng tham gia trò chơi trắc nghiệm trực tuyến.
Bước 2: Thực hiện nhiệm vụ	- Sử dụng thiết bị số để truy cập

- GV theo dõi các nhóm thảo luận về tình huống Deepfake, gợi ý các dấu hiệu nhận biết giả mạo. - GV điều phối trò chơi trắc nghiệm trên nền tảng trực tuyến, theo dõi tiến độ và kết quả trả lời của HS.	<u>ứng dụng Kahoot/Quizizz và thực hiện thao tác tương tác trả lời các câu hỏi trắc nghiệm luyện tập.</u> (2.1.NC1a) - Các nhóm thảo luận nhanh về trách nhiệm đạo đức khi sử dụng công nghệ AI tạo sinh.
Bước 3: Báo cáo, thảo luận - GV khái quát lại những nội dung chủ yếu của bài học, nhấn mạnh nội dung trọng tâm của bài khơi gợi câu trả lời. - GV gọi đại diện HS trả lời câu hỏi: Kể tên các hành vi vi phạm pháp luật về phòng chống tội phạm sử dụng công nghệ cao.	- HS theo dõi bảng xếp hạng trò chơi trắc nghiệm. - Đại diện HS trình bày câu trả lời và ý kiến thảo luận về tình huống Deepfake. - <i>[Dành cho HSKT hòa nhập]: HS thực hiện gior thẻ đáp án hoặc chỉ vào bảng lựa chọn để trả lời câu hỏi (dành cho HS khuyết tật nói, vận động).</i>
Bước 4: Kết luận, đánh giá - GV nhận xét kết quả trò chơi trắc nghiệm, tuyên dương các HS/nhóm HS có kết quả tốt. - GV chốt lại nội dung kiến thức về nhận diện hành vi vi phạm pháp luật và các biện pháp phòng tránh rủi ro trên không gian mạng.	- HS lắng nghe, ghi chép các nội dung trọng tâm vào vở.

D. HOẠT ĐỘNG VẬN DỤNG

a. Mục tiêu:

- Học sinh vận dụng những kiến thức đã học vào giải quyết các nhiệm vụ thực tiễn về **phòng chống tội phạm sử dụng công nghệ cao**.

- Tạo lập và chỉnh sửa nội dung sản phẩm truyền thông số (Infographic, Podcast hoặc Video ngắn) tuyên truyền quy tắc ứng xử văn minh và an toàn trên không gian mạng. (3.1.NC1a)

- **Sử dụng công cụ AI (như Canva Magic Design, CapCut AI) hỗ trợ thiết kế và biên tập nội dung sản phẩm tuyên truyền phòng chống lừa đảo mạng một cách an toàn, hiệu quả và có trách nhiệm.** (11.C2.MR1)

- *[Dành cho HSKT hòa nhập]: Tham gia vào nhóm thiết kế sản phẩm truyền thông số với các nhiệm vụ phù hợp khả năng vận động và giao tiếp (sưu tầm hình ảnh, chọn màu sắc, nhập liệu văn bản ngắn) và hoàn thành phiếu học tập cá nhân ở mức độ cơ bản (5-6 câu hỏi).*

b. Nội dung:

- Thiết kế một sản phẩm truyền thông số (Infographic, Podcast hoặc Video ngắn dưới 1 phút) trên các nền tảng trực tuyến (Canva, CapCut) thể hiện quy tắc

ứng xử văn minh và an toàn trên không gian mạng, **tuyên truyền cách phòng chống lừa đảo mạng cho người thân và cộng đồng.**

- Học sinh vận dụng kiến thức đã học để hoàn thành phiếu bài tập trắc nghiệm về **phòng chống tội phạm sử dụng công nghệ cao.**

c. Sản phẩm:

- Sản phẩm truyền thông số (Infographic, Podcast hoặc Video ngắn) do các nhóm học sinh thiết kế.

- Phiếu học tập gồm câu trả lời trắc nghiệm đã hoàn thành của học sinh.

d. Tổ chức thực hiện:

Hoạt động của giáo viên	Hoạt động của học sinh
Bước 1: Chuyển giao nhiệm vụ - GV giao nhiệm vụ thực hiện dự án nhỏ theo nhóm: <u>Sử dụng các nền tảng trực tuyến tích hợp AI (Canva, CapCut) để sáng tạo một sản phẩm truyền thông số (Infographic, Podcast hoặc video ngắn dưới 1 phút) thể hiện quy tắc ứng xử văn minh, an toàn trên không gian mạng và tuyên truyền cách phòng chống tội phạm công nghệ cao.</u> (3.1.NC1a) - GV hướng dẫn HS đặt câu lệnh (prompt) cơ bản cho AI để gợi ý ý tưởng kịch bản và tự động tạo bố cục thiết kế nhanh chóng. (11.C2.MR1) - GV chuẩn bị phiếu học tập gồm 10 câu hỏi trắc nghiệm để đánh giá mức độ hiểu bài của học sinh ngay tại lớp. - <i>[Dành cho HSKT hòa nhập]: GV phân công bạn học hỗ trợ HSKT (khuyết tật vận động/nói) thao tác trên máy tính/điện thoại; điều chỉnh số lượng câu hỏi phiếu bài tập (5-6 câu mức độ nhận biết) và hỗ trợ kỹ thuật khi cần.</i>	- HS tiếp nhận nhiệm vụ dự án truyền thông số và phiếu học tập từ giáo viên.
Bước 2: Thực hiện nhiệm vụ - GV tổ chức cho HS làm phiếu học tập trắc nghiệm tại lớp. - GV hướng dẫn các nhóm phân công nhiệm vụ, lên ý tưởng kịch bản/nội dung cho sản phẩm truyền thông số để thực hiện ngoài giờ học.	- HS hoàn thành các câu hỏi trắc nghiệm trong phiếu học tập. - Các nhóm hợp tác phân công nhiệm vụ, sử dụng các phần mềm số trực tuyến và công cụ AI để thiết kế, biên tập sản phẩm tuyên truyền an toàn mạng. (2.4.NC1a) - <i>[Dành cho HSKT hòa nhập]: HSKT hỗ trợ nhóm tìm kiếm hình ảnh, đóng góp ý kiến bằng chữ viết (nếu khó nói) và thực hiện các thao</i>

	<i>tác chỉnh sửa đơn giản dưới sự trợ giúp của các bạn trong nhóm.</i>
Bước 3: Báo cáo, thảo luận - GV thu phiếu học tập của HS. - <u>GV hướng dẫn các nhóm chia sẻ đường link sản phẩm truyền thông số lên không gian lưu trữ chung của lớp (Google Drive/Padlet) sau khi hoàn thành. (2.2.NC1a)</u>	- HS nộp phiếu bài tập cho GV. - Các nhóm nộp sản phẩm truyền thông số lên hệ thống lưu trữ đúng thời gian quy định.
Bước 4: Kết luận, đánh giá - GV nhận xét chung về thái độ làm việc của HS, đánh giá sơ bộ kết quả làm phiếu học tập và đưa ra tiêu chí chấm sản phẩm truyền thông số.	- HS lắng nghe rút kinh nghiệm để hoàn thiện sản phẩm dự án.

HƯỚNG DẪN VỀ NHÀ

- Dẫn dò HS học bài cũ, hoàn thiện sản phẩm vận dụng truyền thông số theo nhóm.
- Đọc và tìm hiểu trước nội dung bài học mới.
- Nhận xét, rút kinh nghiệm buổi học.

RÚT KINH NGHIỆM BỔ SUNG

- Kiểm tra sỹ số, vật chất: ...
- Nội dung bài dạy: ...
- Phương pháp giảng dạy: ...