

Kiến thức kỹ thuật số 101:
TÀI LIỆU HỘI THẢO DÀNH CHO CÁC NHÀ HOẠT ĐỘNG
VÌ QUYỀN LỢI THANH THIẾU NIÊN



Giới thiệu

Đây là khóa đào tạo nâng cao năng lực kỹ thuật số dành cho thanh thiếu niên, mang tính chất nhập môn và là nguồn tài liệu hữu ích giúp cải thiện hiểu biết và khả năng tự bảo vệ quyền lợi của giới trẻ trong không gian kỹ thuật số. Tài liệu đào tạo và hội thảo kỹ thuật số này được phát triển dựa trên sự tham vấn với nhiều cộng đồng khác nhau bằng các phương pháp tham gia có sự đóng góp của cộng đồng.

Tài liệu hội thảo trong văn bản này nhằm hỗ trợ người điều phối hội thảo nâng cao kỹ năng sử dụng công nghệ số cho cộng đồng thanh thiếu niên trong ba lĩnh vực chính:

1. Tác hại của số hóa
2. Khả năng phục hồi kỹ thuật số
3. Cải thiện quyền của chúng ta

Các mục tiêu tiềm năng của hội thảo bao gồm:

- Trang bị cho người tham gia các công cụ để bảo vệ quyền lợi của họ khi truy cập dữ liệu sức khỏe
- Nâng cao kỹ năng của người tham gia trong việc xác minh dữ liệu sức khỏe và tìm kiếm các nguồn thông tin chính xác trực tuyến
- Cung cấp cho người tham gia các công cụ để bảo vệ bản thân và thông tin cá nhân của họ

Cấu trúc tổng thể của hội thảo bao gồm ba phần với các câu hỏi hướng dẫn cùng với một loạt các hoạt động được thiết kế để giúp người tham gia khám phá các câu hỏi hướng dẫn đó. Người điều phối có thể chọn các hoạt động phù hợp nhất với đối tượng mục tiêu, mục đích và các yếu tố ngữ cảnh khác, nhưng chúng tôi chia sẻ hai lộ trình được đề xuất trong “Chương trình hội thảo” bên dưới.

Hội thảo có thể diễn ra trực tiếp hoặc trực tuyến với các công cụ từ xa như nền tảng hội nghị, bảng trắng ảo và tài liệu cộng tác. Nếu làm việc từ xa, tốt nhất nên có ít nhất một người điều phối, một người hỗ trợ kỹ thuật để chuyển đổi suôn sẻ sang các phòng thảo luận nhóm và không gian cộng tác, cũng như xử lý các vấn đề kết nối cá nhân, và một người ghi chép nếu cần ghi lại hoặc suy ngẫm sau hội thảo.

Khi đọc những tài liệu này, hãy chú ý đến các biểu tượng cảm xúc sau:



: mục tiêu



: phương pháp



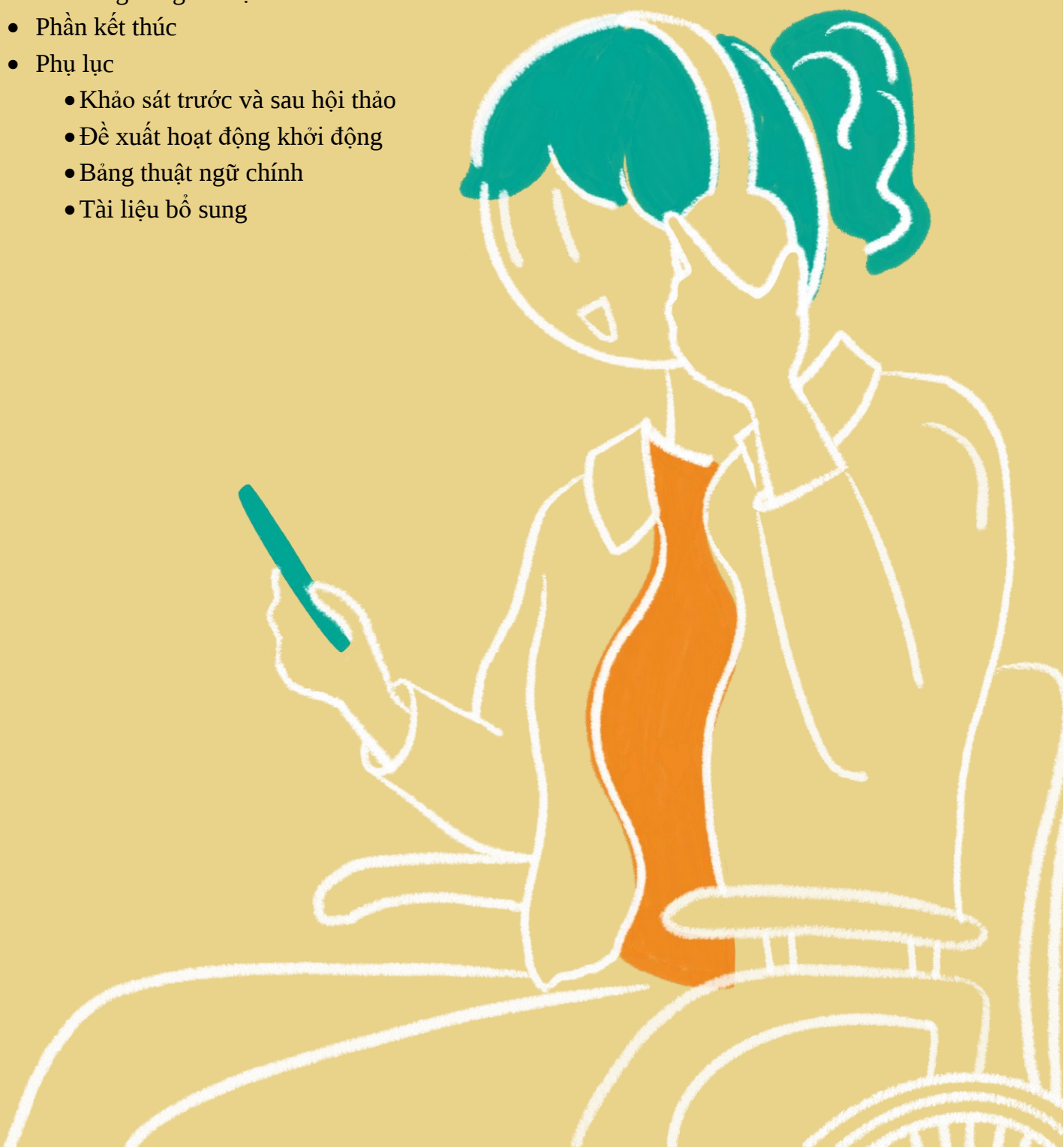
: mẹo

Chúng tôi hy vọng bạn sẽ có những trải nghiệm thú vị, học hỏi được nhiều điều và giúp các bạn trẻ cảm thấy an toàn và tự tin khi tiếp cận với sức khỏe kỹ thuật số!

Nội dung tài liệu hội thảo

Tài liệu này bao gồm:

- Các đề xuất về chương trình hội thảo
- Chương trình học theo từng phần
 - Phần 1: Tác hại của số hóa
 - Phần 2: Khả năng phục hồi kỹ thuật số
 - Phần 3: Vận động cho quyền kỹ thuật số và công bằng dữ liệu
- Phân kết thúc
- Phụ lục
 - Khảo sát trước và sau hội thảo
 - Đề xuất hoạt động khởi động
 - Bảng thuật ngữ chính
 - Tài liệu bổ sung



Các đề xuất cho chương trình hội thảo

PHIÊN BẢN NGẮN HƠN

90 phút

- Giới thiệu 10 phút
- Hành trình dữ liệu của tôi - 15 phút
- Cân bằng rủi ro 15 phút
- Sự thật hay không? 20 phút
- Tìm kiếm trên internet 15 phút
- Kết luận và tài liệu bổ sung 15 phút

PHIÊN BẢN DÀI HƠN

180 phút

- Giới thiệu 10 phút
- Phổ đồ 25 phút
- Câu chuyện dữ liệu 30 phút
- Cân bằng rủi ro 15 phút
- Sự thật hay không? 20 phút
- Tìm kiếm trên internet 15 phút
- Sức khỏe tinh thần trong thời đại kỹ thuật số 20 phút
- Hiểu rõ quyền của mình 30 phút
- Kết thúc và tài liệu bổ sung 15 phút

Chương trình giảng dạy

Buổi hội thảo được thiết kế tập trung vào các hoạt động, nhưng các câu hỏi hướng dẫn trong mỗi phần có thể được sử dụng để chuẩn bị cho người điều phối, giới thiệu và hỗ trợ các hoạt động, và/hoặc khuyến khích suy ngẫm và thảo luận. Các liên kết và thông tin sau mỗi câu hỏi hướng dẫn có thể được chia sẻ khi cần thiết và khi có liên quan. Ví dụ, nếu người tham gia gặp khó khăn trong việc suy nghĩ về cách dữ liệu có thể bị lạm dụng, bạn có thể chia sẻ một số ví dụ được liệt kê trong Phần 1.

PHẦN 1: Tác hại của số hóa

- Những dữ liệu nào về chúng ta đang được lưu trữ? Ai nắm giữ thông tin đó? Ai khác có thể truy cập?
- Điều gì sẽ xảy ra nếu dữ liệu của chúng ta rơi vào tay kẻ xấu?
- "Không phải việc của ai khác ngoài tôi", công trình nghiên cứu của Privacy International về các ứng dụng theo dõi kinh nguyệt và việc khai thác dữ liệu
- Bài báo năm 2018 về việc Grindr chia sẻ tình trạng nhiễm HIV với các nhà cung cấp bên thứ ba, Vox
- Ứng dụng sức khỏe kỹ thuật số có thể khai thác dữ liệu người dùng như thế nào, Privacy International
- Đường dây nóng hỗ trợ người tự tử chia sẻ dữ liệu với công ty con vì lợi nhuận, đặt ra những câu hỏi về đạo đức, Politico
- Những câu chuyện nào có thể được kể về chúng ta bằng dữ liệu đó? Những câu chuyện đó có thể gây hại cho chúng ta như thế nào?

Hoạt động: Kể chuyện bằng dữ liệu (30 phút)



Để hiểu những giả định có thể được đưa ra về chúng ta chỉ với một vài điểm dữ liệu.



Thảo luận mở, chuyển sang suy ngẫm cá nhân và làm việc nhóm nhỏ, rồi quay lại thảo luận nhóm chính.



Nếu mọi người im lặng trong phần thảo luận mở, hãy chọn một ứng dụng mà bạn biết nhiều người trong nhóm sử dụng và hỏi cả nhóm, “Người khác có thể biết được gì về bạn dựa trên việc bạn sử dụng ứng dụng này?” Khuyến khích mọi người gõ, giơ tay, bật mic và/hoặc gõ vào khung chat.

Thảo luận mở: Các ứng dụng chúng ta sử dụng thu thập dữ liệu về chúng ta. Trong các nhóm nhỏ, hãy xem xét các ứng dụng mà nhân vật tưởng tượng của chúng ta, Chandra, thường xuyên sử dụng. Hãy xem xét loại dữ liệu mà mỗi ứng dụng có thể đang thu thập và dữ liệu đó có thể cho chúng ta biết điều gì về Chandra.

Điều gì sẽ xảy ra khi bạn kết hợp tất cả các tập dữ liệu này lại với nhau??

Các ứng dụng mà Chandra sử dụng nhiều nhất bao gồm:

- Google Maps để chỉ đường đến các cuộc hẹn và sự kiện
- Uber Eats và Zwiggy để giao đồ ăn
- Remitly để chuyển tiền cho bạn bè
- TikTok để giải trí
- Zoom để gặp gỡ chuyên gia trị liệu
- Spotify để nghe nhạc và podcast
- Google Search để tra cứu mọi thứ

Suy ngẫm cá nhân và làm việc nhóm nhỏ (2-3 người): Bây giờ, hãy dành vài phút để lập danh sách các ứng dụng bạn sử dụng nhiều nhất và một số dữ liệu mà bạn nghĩ các ứng dụng này đang thu thập. Thảo luận với các thành viên trong nhóm nhỏ của bạn về những câu chuyện, dù đúng hay sai, mà mỗi người có thể kể về nhau.

Báo cáo lại cho cuộc thảo luận chính: Điều này khiến bạn cảm thấy thế nào?



Đề cùng nhau khám phá dữ liệu chúng ta đang chia sẻ và những gì có thể xảy ra với nó.



Tự đánh giá cá nhân, tốt nhất là trên một tài liệu hoặc nền tảng chung như EasyRetro.



Hãy bật nhạc lofi trong khi người tham gia làm việc để tạo không khí suy tư, sáng tạo thay vì ngồi im lặng.

Hãy tự trả lời các câu hỏi trong bảng (sao chép/dán bảng vào tài liệu của riêng bạn, ghi chép vào sổ tay, v.v.) dựa trên hiểu biết tốt nhất của bạn.

Xem ví dụ ở hàng đầu tiên để bắt đầu. Sau đó, hãy thoải mái chia sẻ với nhóm những điều bạn đã học được hoặc thắc mắc. Vào thời gian rảnh, bạn có thể sử dụng bảng này để tìm thêm câu trả lời về các mẫu đơn dịch vụ hoặc thỏa thuận. Bạn cũng có thể sử dụng nó như một cách để đánh giá các ứng dụng và công cụ khác mà bạn quan tâm trước khi tải xuống hoặc đăng ký, giúp bạn đưa ra lựa chọn sáng suốt hơn..

Ai đang giữ dữ liệu của tôi?	Họ lấy nó bằng cách nào?	Liệu có dữ liệu nào trong số đó là dữ liệu nhạy cảm không?	Liệu điều đó có cần thiết cho dịch vụ mà họ cung cấp không?	Họ sử dụng dữ liệu của tôi như thế nào?	Họ đang chia sẻ dữ liệu của tôi với ai?	Điều gì sẽ xảy ra nếu nó rơi vào tay kẻ xấu?	Tôi có thể làm gì để giải quyết vấn đề này?
Diễn đàn trò chuyện về sức khỏe	Từ thông tin tài khoản, có lẽ từ những gì tôi đã nói trên diễn đàn?	Vâng! Giới tính và tình trạng HIV của tôi	Không, chỉ một số thông tin tài khoản như email	Tôi không biết	Tôi hy vọng là không ai biết. Nhưng tôi không biết	Tôi có thể mất việc hoặc bị đuổi khỏi nhà thờ	Hãy kiểm tra điều khoản dịch vụ và tìm một diễn đàn an toàn hơn nếu cần

- Thông tin sai lệch và thông tin xuyên tạc lan truyền trên mạng như thế nào?
- Thông tin xuyên tạc về giới tính liên quan đến bệnh đậu mùa khi, Hiệp hội Truyền thông Tiến bộ
- Các chiến thuật và sai lầm cần lưu ý về nội dung: Tiêu đề giật gân, ý kiến được trình bày như sự thật (thường các bài viết ý kiến được trình bày trên mạng xã hội như sự thật), thiếu nguồn tin, nguồn tin mang tính đảng phái hoặc không đáng tin cậy giả vờ là công bằng hoặc hợp pháp, thiếu ngữ cảnh, dữ liệu đơn lẻ (dữ liệu đơn lẻ trong tiêu đề giật gân tạo ấn tượng sai lệch), chỉnh sửa ảnh, deepfake
- Các chiến thuật kỹ thuật số cần cảnh giác: Bot, tài khoản giả mạo, quảng cáo nhắm mục tiêu, người có ảnh hưởng được trả tiền, tràn ngập không gian mạng, ngăn chặn thông tin

KHỐI 2: Khả năng phục hồi kỹ thuật số

- Chúng ta có thể tìm thấy các luật và quy định hiện hành nào có thể giúp bảo vệ quyền của chúng ta trong không gian kỹ thuật số? Những tổ chức và cộng đồng hoạt động nào cung cấp trợ giúp pháp lý hoặc kiến tụng chiến lược trong các lĩnh vực này?
- <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- Các tổ chức toàn cầu: Access Now, EFF, Amnesty International, Article 19
- Những công cụ và lời khuyên nào khác mà chúng ta hiện có để tự bảo vệ mình tốt hơn trên mạng?

Hoạt động: Cân bằng rủi ro (15 phút)



Để biết cách đưa ra những quyết định sáng suốt hơn về rủi ro và cơ hội của y tế kỹ thuật số.



Suy ngẫm cá nhân, tốt nhất là trong một tài liệu chung hoặc nhóm nhỏ, sau đó là thảo luận mở. Nếu làm nhóm nhỏ, mỗi nhóm nên tập trung vào một vấn đề.



Không quan trọng liệu người tham gia đã thực hiện hay có kế hoạch thực hiện những điều được nêu trong các vấn đề đó hay chưa. Họ có thể làm việc trên bất kỳ vấn đề nào, vì mục đích là để suy nghĩ một cách chiến lược về những gì chúng ta làm trực tuyến.

Mỗi ngày chúng ta đều đưa ra những quyết định về việc chấp nhận rủi ro—from việc băng qua đường đến việc ăn thức ăn thừa không đảm bảo vệ sinh. Có thể bạn có một bài kiểm tra quan trọng ở trường vào ngày mai. Bạn cần thức khuya để học bài, nhưng bạn biết rằng thiếu ngủ sẽ ảnh hưởng đến kết quả bài kiểm tra, vì vậy bạn quyết định lựa chọn nào tốt nhất cho mình hoặc tìm một sự thỏa hiệp giữa hai điều đó. Chúng ta đã nói nhiều về rủi ro liên quan đến dữ liệu, quyền riêng tư và giám sát, nhưng chúng ta cần phải biết cách sử dụng các công cụ kỹ thuật số mà chúng ta có trong tay.

Hãy cùng tìm cách cân bằng một số rủi ro này với nhu cầu và mong muốn của chúng ta trên mạng. Chọn một trong những câu sau và trả lời các câu hỏi bên dưới. Sau đó, hãy thoải mái chia sẻ với nhóm cảm nhận của bạn về các rủi ro và những gì bạn có thể làm.

1. Tôi muốn sử dụng một ứng dụng trò chuyện để thảo luận về các vấn đề sức khỏe với những người khác cũng đang gặp phải vấn đề tương tự.
 - a. Bạn có muốn chia sẻ thông tin trong các cuộc trò chuyện mà bạn không muốn người ngoài ứng dụng biết được không?
 - b. Điều gì sẽ xảy ra nếu những người đó phát hiện ra?
 - c. Bạn có phải sử dụng tên thật và các thông tin nhận dạng cá nhân khác để đăng ký không?
 - d. Ứng dụng bạn chọn có chính sách bảo mật và chia sẻ dữ liệu mà bạn cảm thấy thoải mái không?
 - e. Có bất kỳ việc chia sẻ dữ liệu nào mà bạn có thể từ chối không?
 - f. Ứng dụng có mã hóa đầu cuối giúp tăng cường bảo mật cho việc liên lạc không?
 - g. Nếu bạn trả lời không cho các câu hỏi C-E, có ứng dụng trò chuyện nào khác bảo mật tốt hơn và bạn có sẵn sàng sử dụng nó không?
 - h. Nếu bạn trả lời không cho câu hỏi F, bạn có sẵn sàng chấp nhận rủi ro trong câu hỏi B không?
 - i. Có những bước nào khác bạn có thể thực hiện để bảo vệ bản thân và dữ liệu của mình khi sử dụng ứng dụng này?
2. Tôi muốn sử dụng dịch vụ khám chữa bệnh từ xa, tức là gặp bác sĩ trực tuyến.
 - a. Điều gì sẽ xảy ra nếu thông tin y tế của bạn bị chia sẻ với bên thứ ba mà bạn không đồng ý (ví dụ: gia đình, nơi làm việc, công ty tư nhân, chính phủ, công chúng nói chung)?

- b. Nhà cung cấp dịch vụ khám chữa bệnh từ xa của bạn có các chính sách về quyền riêng tư và chia sẻ dữ liệu mà bạn cảm thấy thoải mái không?
 - c. Có thông tin nào mà nhà cung cấp muốn bạn cung cấp (thông qua đăng ký hoặc các biểu mẫu khác, chẳng hạn) mà có vẻ không liên quan (ví dụ: tôn giáo của bạn) không?
 - d. Có bất kỳ hình thức chia sẻ dữ liệu nào mà bạn có thể từ chối?
 - e. Bạn có biết điều gì sẽ xảy ra với dữ liệu của bạn sau khi bạn không còn là bệnh nhân nữa không?
 - f. Nếu nhà cung cấp sử dụng nền tảng video, bạn có thể truy cập chính sách bảo mật của nền tảng đó hoặc tìm thông tin về các giao thức bảo mật của nó, chẳng hạn như việc sử dụng mã hóa đầu cuối hoặc các lỗ hổng bảo mật hay không?
 - g. Nếu bạn trả lời không cho các câu hỏi B, D, E và F, liệu có nhà cung cấp dịch vụ khám chữa bệnh từ xa nào khác đảm bảo quyền riêng tư tốt hơn không và bạn có sẵn sàng chuyển sang nhà cung cấp đó không?
 - h. Nếu bạn trả lời không cho câu hỏi G, bạn có sẵn sàng chấp nhận rủi ro trong câu hỏi A không?
 - i. Bạn có thể thực hiện thêm những biện pháp nào khác để bảo vệ bản thân và dữ liệu của mình khi sử dụng nhà cung cấp dịch vụ khám chữa bệnh từ xa này?
- 3 Tôi muốn lên tiếng mạnh mẽ về các vấn đề liên quan đến HIV trên các ứng dụng mạng xã hội của mình..
- a. Quốc gia của bạn có luật và thực tiễn mạnh mẽ về tự do ngôn luận không?
 - b. Nếu không, điều gì có thể xảy ra nếu chính phủ thấy hoạt động vận động của bạn hoặc ai đó báo cáo cho họ?
 - c. Bạn có lo lắng về việc lạm dụng trực tuyến và cách nó có thể dẫn đến bạo lực thể chất không?
 - d. Nếu có những người trong cuộc sống của bạn mà bạn không muốn họ thấy hoạt động vận động của mình, điều gì sẽ xảy ra nếu họ thấy?
 - e. Bạn có phải sử dụng tên thật và các thông tin nhận dạng cá nhân khác để đăng ký không?
 - f. Dựa trên câu trả lời của bạn cho A, B, C và D, có thông tin nhận dạng cá nhân nào bạn nên hạn chế trên mạng xã hội (ví dụ: tên đầy đủ, thành phố, ảnh, kết nối với người địa phương, sự hiện diện tại các sự kiện) không?
 - g. Bạn có hệ thống hỗ trợ từ bạn bè và gia đình và/hoặc các dịch vụ pháp lý và tâm lý xã hội có thể giúp bạn đối phó với các phản ứng trừng phạt từ nhà nước, lạm dụng trực tuyến hoặc các vấn đề nghiêm trọng khác không?
 - h. Mạng xã hội bạn chọn có chính sách về quyền riêng tư và chia sẻ dữ liệu mà bạn cảm thấy thoải mái không?
 - i. Có bất kỳ việc chia sẻ dữ liệu nào bạn có thể từ chối không?
 - j. Dựa trên câu trả lời của bạn cho các câu hỏi trên, bạn có cảm thấy việc chấp nhận rủi ro đó là đáng giá không?
 - k. Bạn có thể thực hiện thêm những bước nào khác để bảo vệ bản thân và dữ liệu của mình khi sử dụng các nền tảng này?

- Từ chối cookie
- Sử dụng công cụ tìm kiếm không theo dõi bạn (ví dụ: DuckDuckGo)
- Tạo mật khẩu mạnh và sử dụng trình quản lý mật khẩu
- Sử dụng mã hóa đầu cuối bất cứ khi nào có thể
- Cập nhật phần mềm
- Dữ liệu điện thoại thông minh
- Đọc kỹ chính sách chia sẻ dữ liệu trong điều khoản dịch vụ, sử dụng TOS; để có cái nhìn tổng quan đơn giản
- Kiểm tra phần quyền riêng tư của ứng dụng cho từng ứng dụng trong App Store của Apple và Google Play
- Không kết nối ứng dụng với tài khoản mạng xã hội; tạo tài khoản đăng nhập riêng biệt
- Điều chỉnh cài đặt quyền riêng tư trên ứng dụng và thiết bị để hạn chế theo dõi, đặc biệt là mạng xã hội
- Quyền riêng tư của ứng dụng hẹn hò

- Những phương pháp nào là tốt nhất và dễ nhất để tìm kiếm hoặc xác minh thông tin trực tuyến

Hoạt động: Sự thật hay không? (20 phút)



Mục tiêu là xác định cách thức lan truyền tin giả trên mạng và trang bị cho người tham gia các công cụ để phát hiện thông tin sai lệch và xuyên tạc.



Hoạt động nhóm nhỏ, sau đó là thảo luận chính.



Trước khi chia nhóm nhỏ, hãy chia sẻ hình ảnh minh họa 7 loại thông tin sai lệch và xuyên tạc bên dưới bằng cách chia sẻ màn hình hoặc sao chép/dán vào tài liệu được chia sẻ. Quay lại nhóm chính vào cuối buổi, hãy cân nhắc chia sẻ các chiến thuật kiểm chứng thông tin như SURE, IMVAIN từ chương trình học trong một buổi động não về cách kiểm chứng thông tin liên quan đến sức khỏe trên mạng.

Chúng ta đang sống trong một hệ sinh thái thông tin, nơi cả sự thật và thông tin sai lệch đều có thể lan truyền với tốc độ rất nhanh. Ai cũng thường xuyên bắt gặp những câu chuyện giả mạo và thông tin không chính xác trên mạng, và chúng ta thường khuếch đại những câu chuyện này vì không biết cách kiểm tra tính chính xác của chúng.

Hãy cùng suy nghĩ về một số cách thức và lý do tại sao thông tin giả mạo được tạo ra và chia sẻ trực tuyến, và tất cả chúng ta có thể làm gì để phân biệt giữa sự thật và thông tin sai lệch trong các tương tác kỹ thuật số hàng ngày.

Mỗi nhóm có bảy phút để đưa ra các tiêu đề liên quan đến sức khỏe cho mỗi loại – lấy cảm hứng từ những câu chuyện họ bắt gặp trong thế giới thực hoặc do cả nhóm tự nghĩ ra. Sau đó, hãy quay lại nhóm chính để chia sẻ những tiêu đề yêu thích của bạn, cùng với lý do và cách bạn nghĩ rằng những tiêu đề đó lan truyền nhanh chóng.

7 LOẠI THÔNG TIN SAI LỆCH VÀ THÔNG TIN KHÔNG CHÍNH XÁC



Nguồn: <https://firstdratnews.org/articles/fake-news-complicated/>

- Học cách nhận diện các chiến thuật
 - Bot hay không?, Tactical Tech
 - Những gì bạn thấy có thực sự là sự thật? Khám phá thông tin sai lệch trực quan, Tactical Tech
 - Sức khỏe so với tin giả, Tactical Tech
 - Chống tin giả, UNESCO
 - 7 công cụ xác minh để kiểm chứng thông tin tốt hơn, Reuters
 - Phương pháp IMVAIN, Trung tâm Tài nguyên Kỹ thuật số
 - Phương pháp SURE, Chính phủ Singapor

- Tìm kiếm các nguồn tin đáng tin cậy, xem xét nguồn phát hành, tác giả, ngày tháng, thậm chí cả người tài trợ cho nghiên cứu
- Thử 2-3 công cụ tìm kiếm khác nhau để xem kết quả mỗi công cụ cho ra
- Tìm hiểu các mẹo tìm kiếm của Google về cách nhập từ khóa
- Kiểm tra chéo thông tin với các nguồn khác hoặc các trang web kiểm chứng thông tin
- Tìm kiếm thêm chi tiết hoặc ngữ cảnh
- Cách tìm kiếm hiệu quả trên internet

Hoạt động: Tìm kiếm trên internet (15 phút)



Mục đích của buổi học là thực hành cách tìm kiếm dữ liệu chính xác trực tuyến và cách người tham gia có thể tìm kiếm thông tin trên internet một cách thông minh và hiệu quả.



Các nhóm nhỏ được chia thành các nhóm nhỏ, sau đó là thảo luận chính.



Nếu người tham gia phát biểu gặp sự cố kết nối trong nhóm chính mà không thể khắc phục nhanh chóng, hãy tắt tiếng họ nếu cần và thông báo, đồng thời viết vào khung chat rằng có vấn đề về âm thanh và họ có thể viết ý kiến của mình vào khung chat hoặc liên hệ với bộ phận hỗ trợ kỹ thuật để cải thiện âm thanh. Bằng cách này, các vấn đề kỹ thuật cá nhân sẽ không làm gián đoạn cuộc thảo luận.

Bây giờ, hãy chọn một trong những câu chuyện giả yêu thích của bạn từ buổi chơi "Sự thật hay Lời nói dối" trước đó, và cố gắng tìm thông tin chính xác về câu chuyện đó, cùng với các thành viên khác trong nhóm nhỏ của bạn. Sau đó, bạn sẽ quay lại và chia sẻ những gì mình tìm được với nhóm chính.

Một số điều cần lưu ý khi đánh giá một trang web trong quá trình tìm kiếm trực tuyến của bạn:

Thẩm quyền	Ai là tác giả của trang web này? Họ có được nêu rõ thông tin về bằng cấp của mình không? Họ có được coi là chuyên gia trong lĩnh vực đó không? (Có thể nên kiểm tra thêm các nguồn khác để tìm hiểu) Họ có cung cấp thông tin liên hệ không? Mục đích của họ khi tạo ra trang web này là gì?
Độ tin cậy	Hãy kiểm tra tên miền trong URL. Nó thuộc về một tổ chức giáo dục (edu hoặc ac), một cơ quan chính phủ (gov hoặc govt) hay một tổ chức thương mại (com hoặc co)? Mục đích của trang web là gì?
Tiền tệ	Trang web được cập nhật lần cuối khi nào? Thông tin này có được ghi rõ không?
Tính phù hợp	Thông tin do trang web cung cấp có đáp ứng nhu cầu nghiên cứu của bạn không? Chỉ vì nó có trên internet không có nghĩa là đó là nguồn thông tin tốt nhất. Hãy hỏi thủ thư để tìm các nguồn thông tin khác.
Tính toàn diện	Thông tin trên trang web có đầy đủ và toàn diện không? Trang web có cung cấp thông tin từ nhiều góc độ hay chỉ một góc độ duy nhất? Sự chính xác Thông tin trên trang web có chính xác không? Nếu không chắc chắn, hãy kiểm tra lại với các nguồn thông tin khác.
Khả năng sử dụng	Trang web này thân thiện với người dùng đến mức nào? Tốc độ tải có nhanh và dễ điều hướng không? Có chức năng tìm kiếm giúp bạn tìm kiếm thông tin cần thiết không?

- Tìm kiếm thông tin hữu ích trên internet, Scientific American
- Tìm kiếm thông tin đáng tin cậy trực tuyến, Leslie Stebbins

KHỐI 3: Khả năng phục hồi kỹ thuật số và vận động cho công bằng dữ liệu

- Chúng ta có thể làm gì nếu số hóa đang gây hại đến sức khỏe của chúng ta?

Hoạt động: Chăm sóc sức khỏe bản thân (20 phút)



Xác định các cách để giảm bớt căng thẳng và lo lắng liên quan đến hoạt động kỹ thuật số..



Nên tự suy ngẫm cá nhân, tốt nhất là trong một tài liệu chung hoặc nhóm nhỏ, sau đó là thảo luận mở. Nếu làm nhóm nhỏ, mỗi nhóm nên tập trung vào một vấn đề.



Người tham gia có thể đề cập đến những chủ đề và trải nghiệm khó khăn. Nếu bạn gặp khó khăn trong việc dẫn dắt cuộc trò chuyện, hãy tập trung vào việc lắng nghe, khẳng định và nhấn mạnh các cách để đối phó. Ở cuối tài liệu này, bạn sẽ tìm thấy các nguồn tài liệu để chia sẻ và, nếu phù hợp, hãy cân nhắc liên hệ riêng với bất kỳ ai mà bạn quan tâm.

Tôi biết có thể bạn đang cảm thấy căng thẳng khi nghĩ về những vấn đề như lạm dụng dữ liệu và thông tin sai lệch. Chắc hẳn tất cả chúng ta đều từng gặp phải những vấn đề liên quan đến việc sử dụng internet, như bắt nạt hoặc quấy rối trên mạng xã hội, lướt tin tức tiêu cực và so sánh bản thân với người khác. Chúng ta hãy chia thành các nhóm nhỏ để thảo luận về cách internet ảnh hưởng đến sức khỏe tinh thần của chúng ta và cách chúng ta có thể tự chăm sóc bản thân. Hãy chọn một người ghi chép để có thể chia sẻ những điểm nổi bật khi chúng ta quay lại nhóm chính.

- Thế giới kỹ thuật số ảnh hưởng tiêu cực đến sức khỏe tinh thần của chúng ta như thế nào? Hãy nghĩ về các hoạt động trực tuyến có thể tác động tiêu cực đến chúng ta, chẳng hạn như cờ bạc trực tuyến, so sánh bản thân với người khác và hội chứng sợ bỏ lỡ (FOMO), hoặc cách mà các động lực và định kiến xã hội có thể bị khuếch đại trên mạng.
- Chúng ta có thể tự chăm sóc bản thân như thế nào khi điều này xảy ra? Chúng ta có thể thực hiện những thay đổi nhỏ, thiết thực nào, chẳng hạn như tắt thông báo hoặc tránh lướt tin tức tiêu cực? Những bước lớn hơn nào có thể hữu ích?
- Chúng ta muốn cảm thấy như thế nào khi trực tuyến?
- Có những công cụ, phương pháp, cộng đồng nào chúng ta có thể dựa vào để giúp chúng ta cảm thấy như vậy khi trực tuyến?

- Những khoảng trống trong vận động chính sách về sức khỏe trong quyền kỹ thuật số hiện nay ở cấp địa phương và toàn cầu là gì? Làm thế nào để xác định chúng? Ai là các bên liên quan cần tham gia vào các chiến dịch vận động chính sách ở địa phương?



Để hiểu cách thức quyền và công lý kỹ thuật số áp dụng cho sức khỏe, các hướng đi khả thi để đòi hỏi sự thay đổi và sự hỗ trợ mà chúng ta có thể tìm kiếm khi những quyền đó bị xâm phạm.



Bảng trắng hoặc giấy ghi chú, nhóm chính, nhóm nhỏ và quay lại nhóm chính.



Tôi sẽ chuẩn bị một khoảng trống trong tài liệu ghi chú chung cho mỗi nhóm nhỏ để làm việc về vấn đề sức khỏe kỹ thuật số của họ với các câu hỏi đính kèm..

Bảng trắng hoặc giấy ghi chú: Trong bản bổ sung năm 2016 cho Tuyên ngôn Toàn cầu về Nhân quyền, Liên Hợp Quốc đã nêu rõ: “Những quyền mà con người có được ngoài đời thực cũng phải được bảo vệ trên mạng”. Trên bảng trắng (hoặc trên giấy ghi chú), hãy ghi thêm bất cứ điều gì bạn thấy: 1) là một “quyền” hoặc luật ở quốc gia của bạn, hoặc điều mà bạn cho rằng nên là một quyền hoặc một luật và 2) có liên quan đến cuộc sống của chúng ta trên internet. Hãy suy nghĩ về những gì mọi người hoặc các tổ chức nên hoặc không nên được phép làm, và những gì họ phải làm. Ví dụ:

Hoạt động: Tìm hiểu các quyền của tôi (30 phút)

Nếu bác sĩ của tôi phải bảo vệ hồ sơ y tế của tôi tại phòng khám, thì họ cũng phải bảo vệ chúng trên mạng.

Nhóm chính: Bây giờ chúng ta đã suy nghĩ về quyền, hãy nói về công bằng. Đôi khi, cách thức thu thập, chia sẻ và sử dụng dữ liệu có thể đặc biệt gây hại cho các cộng đồng như chúng ta. Bạn muốn những người trong lĩnh vực sức khỏe kỹ thuật số tiếp cận dữ liệu của bạn như thế nào? Họ có thể giúp chúng ta tận dụng tối đa dữ liệu của mình cho sức khỏe như thế nào? Họ nên biết gì về việc sử dụng dữ liệu của chúng ta có thể gây hại cho chúng ta như thế nào? Các cộng đồng như chúng ta có thể kiểm soát dữ liệu của mình như thế nào? Chúng ta có thể là người quyết định điều gì sẽ xảy ra với dữ liệu đó không? Chúng ta có thể làm gì để đạt được công bằng kỹ thuật số?

Nhóm nhỏ: Bây giờ hãy thảo luận về một vấn đề sức khỏe kỹ thuật số với nhóm nhỏ của bạn và ghi chú vào tài liệu ghi chú chung để chúng ta có thể học hỏi lẫn nhau. Các câu hỏi của nhóm nhỏ sẽ giúp chúng ta khám phá cách vận động cho sự thay đổi.

- Hãy xác định một vấn đề sức khỏe kỹ thuật số mà bạn muốn thấy được giải quyết trong bối cảnh của mình. (Ví dụ nếu cần: thu thập và chia sẻ/bán dữ liệu quá mức, thiếu không gian an toàn cho thảo luận, hình sự hóa hoặc hạn chế một số hình thức biểu đạt trực tuyến, thông tin sai lệch về bệnh đậu mùa khỉ, thiếu dữ liệu y tế công cộng chính xác, thiếu quyền truy cập vào dữ liệu sức khỏe của chính bạn, việc tắt internet và các vấn đề truy cập khác.)
- Nhóm nào bị ảnh hưởng nhiều nhất bởi vấn đề này?
- Ai có quyền hành động về vấn đề này? Hãy nghĩ về những người ra quyết định ở các cấp độ khác nhau (chính phủ, khu vực tư nhân, cộng đồng, cá nhân, những người giống như bạn, v.v.)
- Hành động cụ thể mà bạn muốn họ thực hiện là gì?
- Cách tốt nhất để thuyết phục hoặc gây áp lực lên họ là gì?
- Những nhóm nào (các nhà hoạt động cơ sở, các nhóm vận động, các bên liên quan trong khu vực tư nhân, giới học thuật, các chuyên gia pháp lý, cử tri, v.v.) có thể cung cấp sự hỗ trợ cần thiết xung quanh các vấn đề này?
- Bạn cần những nguồn lực nào để khiến họ hành động? Những gì bạn đã có sẵn? Làm thế nào bạn có thể có được những thứ còn thiếu?
- Những phong trào và cộng đồng toàn cầu nào đang ủng hộ quyền kỹ thuật số mạnh mẽ hơn trong lĩnh vực y tế? Làm thế nào chúng ta có thể tiếp cận những cộng đồng này?
- Quyền nữ quyền/quyền của phụ nữ, quyền LGBTQI+, công lý cho người khuyết tật, công lý cho người di cư, quyền và sức khỏe tình dục và sinh sản (SRHR), quyền kỹ thuật số
- Những bộ công cụ, hướng dẫn và tài nguyên đáng tin cậy và cập nhật nào hiện có mà chúng ta có thể sử dụng?
- Hướng dẫn Bảo vệ Dữ liệu, Privacy International
- Hướng dẫn FOI, Privacy International
- Tăng cường các phương pháp tiếp cận đa chiều trong vận động bảo vệ dữ liệu và quyền kỹ thuật số trong đại dịch, The Engine Room
- Giải thích Chính sách, Hiệp hội Truyền thông Tiến bộ
- Liên minh Năng động về Sức khỏe Kỹ thuật số của Diễn đàn Quản trị Internet
- Bộ công cụ CNTT cho Xây dựng Phong trào Nữ quyền, JASS

Kết thúc

(15 phút)

- Để kết thúc buổi hội thảo một cách ý nghĩa, ngắn gọn và thiết thực.
- Phân tự suy ngẫm cá nhân, sau đó là thảo luận nhóm chính.
- Trong thời gian này, người điều phối có thể chia sẻ một số tài liệu cuối cùng từ chương trình học hoặc phần ‘Tài liệu bổ sung’. Một cách để làm điều này là liệt kê chúng trong một tài liệu ghi chú chung hoặc tài liệu cộng tác khác và yêu cầu người tham gia bổ sung thêm bất kỳ tài liệu nào của riêng họ.

Hãy dành vài phút để trả lời các câu hỏi sau đây, có thể trong tài liệu ghi chú chung hoặc bất cứ nơi nào bạn đang ghi chú cho riêng mình.

- Ba điểm chính hoặc ‘bài học’ quan trọng nhất từ buổi hội thảo hôm nay là gì?
- Bạn có câu hỏi nào về những gì chúng ta đã thảo luận hôm nay không?
- Bạn muốn tìm hiểu thêm về điều gì?

Bạn có bất kỳ suy nghĩ cuối cùng hoặc tài liệu nào muốn chia sẻ không?

Phụ lục

KHẢO SÁT TRƯỚC VÀ SAU KHÓA HỌC

Lưu ý dành cho người điều phối: Nếu muốn đo lường tác động của hội thảo, hãy yêu cầu người tham gia làm khảo sát này trong thời gian dành cho phần giới thiệu hoặc trước khi bắt đầu hội thảo. Trong phần kết thúc hoặc sau hội thảo, hãy yêu cầu người tham gia làm khảo sát lại để xem phản hồi của họ cho thấy sự gia tăng kiến thức như thế nào. Chúng tôi khuyến nghị sử dụng nền tảng khảo sát với một liên kết cho bài kiểm tra trước và một liên kết khác cho bài kiểm tra sau để tổng hợp kết quả riêng biệt.

Hướng dẫn: Vui lòng chọn mức độ đồng ý của bạn với các phát biểu sau trên thang điểm từ 1 đến 5, với 1 là "hoàn toàn đồng ý" và 5 là "hoàn toàn không đồng ý".

1. Tôi biết các ứng dụng, nền tảng và dịch vụ kỹ thuật số đang thu thập loại dữ liệu nào về tôi.
2. Tôi biết cách hạn chế việc dữ liệu của mình bị theo dõi, lưu trữ và chia sẻ khi có thể.
3. Tôi nhận thức được những cách mà mọi người có thể bị tổn hại bởi các hệ thống kỹ thuật số và việc thu thập dữ liệu hàng loạt.
4. Tôi biết cách tự bảo vệ mình trực tuyến và những công cụ tôi có để tăng cường an ninh mạng.
5. Tôi thường có thể nhận biết được thông tin mình thấy trực tuyến có đáng tin cậy hay không.
6. Tôi biết nơi tìm kiếm thông tin chính xác trực tuyến và cách tìm kiếm những thứ tôi quan tâm.
7. Tôi quản lý tốt các giới hạn kỹ thuật số của mình và có sự cân bằng lành mạnh giữa cuộc sống trực tuyến và ngoại tuyến.
8. Tôi biết các quyền của mình khi truy cập, sử dụng, tạo hoặc chia sẻ nội dung trực tuyến.
9. Tôi biết nên liên hệ với ai để được bảo vệ pháp lý nếu quyền kỹ thuật số của tôi bị xâm phạm.
10. Tôi đã quen thuộc với các bộ công cụ, hướng dẫn và nguồn tài nguyên có thể giúp tôi sử dụng internet một cách an toàn và bảo mật.

CÁCH KHỞI ĐỘNG

Lời giới thiệu: Tạo không khí vui vẻ (10 phút)

- Để tạo không gian cho mỗi người tham gia nhanh chóng giới thiệu bản thân với nhóm,

Mọi người viết tên, cộng đồng/các cộng đồng mà họ đại diện, và một thông tin hoàn toàn ngẫu nhiên về bản thân mà họ cảm thấy thoải mái chia sẻ với nhóm. Mọi người đọc to và những người khác có thể đặt câu hỏi về những thông tin ngẫu nhiên đó..

Lời giới thiệu: Tạo không khí vui vẻ (10 phút)

- Tạo không gian để nhóm có thể hiểu nhau hơn, trở nên thân mật hơn và xây dựng lòng tin giữa các thành viên.

Người điều phối vẽ một đường ngang trên ứng dụng bảng trắng, viết một trong hai thái cực của phổ ở mỗi đầu:

- Tôi cảm thấy hào hứng và tự tin khi sử dụng các ứng dụng sức khỏe kỹ thuật số.
- Tôi cảm thấy lo lắng và không chắc chắn khi sử dụng các ứng dụng sức khỏe kỹ thuật số.
- Yêu cầu người tham gia vẽ một chữ X ở đâu đó trên đường thẳng để thể hiện vị trí của họ trên phổ. Hỏi xem có ai muốn chia sẻ lý do tại sao họ cảm thấy như vậy không.

BẢNG THUẬT NGỮ CHÍNH

Chúng tôi khuyến nghị người điều phối nên làm quen với các thuật ngữ dưới đây và sử dụng các định nghĩa và ví dụ này khi cần thiết trong suốt buổi hội thảo.

- **Điểm dữ liệu:** Một mẫu thông tin đơn lẻ
 - Ví dụ: tuổi
- **Tập dữ liệu:** Một tập hợp các điểm dữ liệu, thường liên quan đến các điểm dữ liệu khác
 - Ví dụ: Kết quả xét nghiệm của bệnh nhân trong năm qua
- **Thông tin nhận dạng cá nhân (PII):** Dữ liệu có thể được sử dụng để xác định danh tính một cá nhân
 - Ví dụ: Kết quả xét nghiệm của bệnh nhân trong năm qua
- **Dữ liệu cá nhân nhạy cảm:** Dữ liệu mà một người muốn được bảo mật và giữ kín tuyệt đối
 - Ví dụ: Dữ liệu liên quan đến đời sống tình dục của một người
- **Siêu dữ liệu:** Dữ liệu cung cấp thông tin về các dữ liệu khác
 - Ví dụ: Dấu thời gian trên ảnh
- **Sự đồng ý có hiểu biết:** Khi một người tự nguyện đồng ý cho phép một tổ chức khác thu thập, lưu trữ, chia sẻ hoặc xử lý dữ liệu của họ. Lý tưởng nhất, sự đồng ý nên là:
 - Được cho đi một cách tự nguyện
 - Có thể đảo ngược
 - Được thông báo
 - Nhiệt tình
 - Cụ thể
- Ví dụ: Một nhà cung cấp dịch vụ chăm sóc sức khỏe kỹ thuật số sẽ hướng dẫn bạn quy trình xử lý dữ liệu của họ, thông báo rằng họ sẽ thu thập dữ liệu về tình trạng sức khỏe của bạn để cung cấp dịch vụ chăm sóc phù hợp. Dữ liệu có thể được chia sẻ với các chuyên gia y tế khác trong nhóm của họ trong trường hợp phức tạp, và bất kỳ dữ liệu nào họ sử dụng cho nghiên cứu nội bộ sẽ được ẩn danh. Dữ liệu của bạn sẽ không được chia sẻ với các tổ chức khác. Bạn có quyền thay đổi ý định và yêu cầu xóa dữ liệu của mình bất cứ lúc nào. Bạn có cơ hội đặt câu hỏi hoặc tìm kiếm thêm thông tin. Bạn cảm thấy thoải mái với quy trình và ký vào tài liệu.
- **Chia sẻ dữ liệu:** Cung cấp cho các đối tác quyền truy cập vào dữ liệu mà họ chưa sở hữu. Trong nhiều trường hợp, việc này được thực hiện với sự đồng ý của cá nhân, nhưng đôi khi sự đồng ý không được yêu cầu mặc dù nên có.
- Ví dụ có sự đồng ý: Một nhà cung cấp dịch vụ chăm sóc sức khỏe chia sẻ dữ liệu bệnh nhân với công ty bảo hiểm y tế của bệnh nhân theo các điều khoản được mô tả trong mẫu đơn đồng ý mà bệnh nhân đã ký.
- Ví dụ không có sự đồng ý: Một nhà cung cấp dịch vụ chăm sóc sức khỏe chia sẻ dữ liệu bệnh nhân với một công ty tiếp thị không được đề cập trong mẫu đơn đồng ý.
- **Ẩn danh:** Loại bỏ thông tin nhận dạng cá nhân (PII) khỏi tập dữ liệu. Ví dụ: Một cơ quan y tế chính phủ loại bỏ thông tin nhận dạng cá nhân như tên, địa chỉ và ngày sinh khỏi các bộ dữ liệu về các trường hợp mắc Covid trước khi công khai dữ liệu.
- **Hiệu ứng ghép ảnh:** Khi một số điểm dữ liệu mà khi sử dụng riêng lẻ sẽ không xác định được một người, nhưng khi kết hợp lại sẽ cho phép xác định được người đó.
- Ví dụ: “Được khơi nguồn từ một nghiên cứu cho thấy Mohammed là cái tên phổ biến nhất trong số các tài xế taxi ở thành phố New York, một công dân tư nhân đã so sánh thời gian cầu nguyện của người Hồi giáo với dữ liệu công khai từ Ủy ban Taxi & Xe Limousine thành phố New York để xác định những tài xế có thể là người Hồi giáo. Chỉ cần ghép hai bộ dữ liệu này lại với nhau đã cho thấy những cá nhân có khoảng thời gian không hoạt động trùng khớp rõ rệt với năm lời kêu gọi cầu nguyện hàng ngày. Mặc dù bộ dữ liệu đã được loại bỏ cẩn thận các thông tin nhận dạng cá nhân—tên, số biển số xe, số hiệu giấy phép—nhưng các nhóm cụ thể, có khả năng nhạy cảm, vẫn được xác định rõ ràng chỉ với một chút thao tác.”

- Thuật toán: Một quy trình sử dụng dữ liệu để giải quyết vấn đề hoặc hoàn thành nhiệm vụ, thường được thực hiện bởi máy tính.
- Thuật toán của Netflix sử dụng lịch sử xem, xếp hạng, dữ liệu từ những người dùng khác có sở thích tương tự, dữ liệu phim (thể loại, diễn viên, v.v.), thời gian xem, thời lượng xem và thiết bị bạn sử dụng để đưa ra đề xuất phim.
- Thông tin sai lệch: Thông tin sai sự thật hoặc gây hiểu nhầm được chia sẻ với mục đích lừa dối.
- Ví dụ: Một chương trình tin tức truyền hình cố tình lấy dữ liệu từ một nghiên cứu sức khỏe ra khỏi ngữ cảnh, bỏ qua những hạn chế của nghiên cứu và phân tích của các nhà nghiên cứu để thúc đẩy một quan điểm mang tính chính trị.
- Thông tin không chính xác: Thông tin sai sự thật hoặc gây hiểu nhầm được chia sẻ mà không có mục đích lừa dối.
- Ví dụ: Thành viên gia đình bạn nhìn thấy một bài đăng trên mạng xã hội mà không biết rằng nó đã lấy kết quả của một nghiên cứu sức khỏe ra khỏi ngữ cảnh, dẫn đến việc mọi người tin rằng một biện pháp phòng ngừa cụ thể không hiệu quả.
- Bot: Một ứng dụng được lập trình để thực hiện các nhiệm vụ nhất định.
- Ví dụ: Trên mạng xã hội, bot thường là các tài khoản giả mạo đăng bài, chia sẻ và thích nội dung.
- Tài khoản giả mạo (Sock puppet): Một tài khoản giả do một người tạo ra.
- Ví dụ: Trên mạng xã hội, một cá nhân thường tạo ra nhiều tài khoản giả để thao túng dư luận.
- Deep fake: Video, âm thanh hoặc hình ảnh đã được chỉnh sửa kỹ thuật số để trông giống như ai đó đang làm hoặc nói điều gì đó mà họ không hề làm.
- Ví dụ: Một video năm 2022 về Tổng thống Ukraine Volodymyr Zelenskyy ra lệnh cho binh lính đầu hàng.
- Bảo vệ dữ liệu: Các chính sách, giao thức và quy định để bảo vệ dữ liệu khỏi bị mất, hư hỏng và lạm dụng.
- Ví dụ: Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (EU GDPR), Đạo luật bảo vệ thông tin cá nhân (POPIA), Tài nguyên bảo vệ dữ liệu và quyền riêng tư Covid-19, Nguyên tắc của OECD về Trí tuệ nhân tạo, Bảo vệ dữ liệu cá nhân trong hệ thống thông tin y tế của WHO.
- An ninh mạng: Các công cụ và mẹo để bảo vệ thiết bị kỹ thuật số, tài khoản và dữ liệu.
- Ví dụ: Sử dụng mật khẩu/cụm mật khẩu duy nhất cho mỗi tài khoản.
- Khả năng thích ứng kỹ thuật số: Kiến thức, kỹ năng và sự tự tin để tự bảo vệ mình trong thời đại kỹ thuật số. Điều này có thể bao gồm an ninh mạng, hiểu biết công nghệ, sức khỏe kỹ thuật số, mạng lưới hỗ trợ và các nguồn lực. Nó cho phép chúng ta tận dụng tối đa cuộc sống trực tuyến của mình đồng thời hạn chế những tác hại.
- Mã hóa đầu cuối: Một phương pháp bảo mật ngăn chặn bất kỳ ai ngoài người gửi và người nhận dự định truy cập vào tin nhắn.
- WhatsApp sử dụng mã hóa đầu cuối để ngay cả chính công ty cũng không thể đọc được tin nhắn của bạn.
- Quyền kỹ thuật số: Một loạt các quyền liên quan đến hoặc bị ảnh hưởng bởi công nghệ kỹ thuật số.
- Ví dụ: Quyền truy cập internet, quyền truy cập thông tin, tự do ngôn luận, quyền được bảo vệ khỏi bạo lực, quyền riêng tư (đặc biệt là về giao tiếp và dữ liệu)

- Công bằng dữ liệu: Một cách tiếp cận công bằng về cách dữ liệu thể hiện con người, đặc biệt là các cộng đồng bị thiệt thòi trong lịch sử
- Ví dụ: Tính minh bạch trong cách thức hoạt động của thuật toán, bao gồm các loại dữ liệu được thu thập và cách chúng được sử dụng để tạo ra đề xuất
- Quản trị Internet: Luật, chính sách và thực tiễn định hình Internet
- Ví dụ: Liên minh năng động về quyền truy cập công cộng trong thư viện

TÀI LIỆU THAM KHẢO BỔ SUNG

Khai thác dữ liệu

- Công nghệ quảng cáo, Privacy International
- Nhắm mục tiêu vi mô, Privacy International
- Quyền dữ liệu cho cộng đồng, Digital Empowerment Foundation
- “Dữ liệu là dấu vân tay”: Tại sao bạn không ẩn danh như bạn nghĩ trên mạng, Guardian

An ninh mạng và tự bảo vệ

- Thoát khỏi các thiết lập mặc định, Tactical Tech
- Làm mới và đổi mới: Quản lý danh tính và tài khoản trực tuyến của bạn, Tactical Tech
- Bộ dụng cụ sơ cứu kỹ thuật số
- Tự chăm sóc bản thân, Digital First Aid
- Hướng dẫn tự làm về an ninh mạng nữ quyền, Hackblossom
- Lấy lại quyền kiểm soát công nghệ! Đường dây trợ giúp an ninh mạng của Access Now
- Cộng đồng HeartMob dành cho những người bị quấy rối trực tuyến
- Nghiện cờ bạc và game trực tuyến: Mẹo hữu ích, Healthline
- Cách vượt qua nỗi sợ bỏ lỡ (FOMO), Psychology Today
- Giải độc kỹ thuật số, Học viện Nhân khoa Hoa Kỳ

Sức khỏe và quyền riêng tư kỹ thuật số

- Sức khỏe kỹ thuật số: Điều đó có ý nghĩa gì đối với quyền và tự do của bạn, Privacy International
- Rủi ro về quyền riêng tư của Zoom, CNET
- Mozilla kiểm tra chính sách bảo mật của BetterHelp

Vận động và xây dựng phong trào

- Cải cách chính sách: Hướng tới sự chuyển đổi và thay đổi theo hướng nữ quyền, GenderIT
- Trường Quản trị Internet Châu Phi (AFRISIG)
- RightsCon
- MozFest
- Lễ hội Tự do Internet

Lời cảm ơn

Tài liệu đào tạo này là kết quả của sự hợp tác giữa hai tổ chức thành viên của liên minh Dự án Sức khỏe và Quyền Kỹ thuật số (Digital Health and Rights Project) cùng với Young Experts: Tech 4 Health (YET4H).

Mạng lưới Toàn cầu những người sống chung với HIV (GNP+) và STOPAIDS đã hợp tác với YET4H, trong đó The Engine Room đóng vai trò là đối tác giám sát quá trình phát triển kỹ thuật thông qua phương pháp tham vấn và tham gia.

Tài liệu đào tạo được thiết kế và minh họa bởi Bai Design Studio.

For inquiries related to this document, please do not hesitate to contact us at info@yet4h.org and communication@gnpplus.net

1 Dự án Sức khỏe và Quyền Kỹ thuật số (DHRP) là một liên minh gồm các nhà nhân chủng học, luật sư nhân quyền và mạng lưới toàn cầu các nhà hoạt động xã hội dân sự làm việc theo phương pháp nghiên cứu hành động tham gia xuyên quốc gia, kết hợp nghiên cứu dân tộc học, suy ngẫm, phân tích và tham gia chính sách để vận động cho nhân quyền trong quản trị kỹ thuật số.

Các thành viên của liên minh DHRP bao gồm Trung tâm Phương pháp luận Liên ngành tại Đại học Warwick, Mạng lưới Toàn cầu những người sống chung với HIV, Mạng lưới Vấn đề Pháp lý & Đạo đức về HIV và AIDS của Kenya (KELIN), Mạng lưới Người sống chung với HIV tại Việt Nam (VNP+), Mạng lưới Người sống chung với HIV/AIDS tại Ghana (NAP+), Privacy International, Restless Development, STOPAIDS và Đại học Los Andes. Ấn phẩm này không phải là ấn phẩm của toàn bộ liên minh, và danh sách các thành viên liên minh không ngụ ý sự chứng thực. Thông tin về dự án có thể được tìm thấy trực tuyến tại đây.



ẤN BẢN ĐẦU TIÊN

Được phát triển vào năm 2022

Xuất bản năm 2023