

Swipe Safe – An toàn trên mạng

Thanh thiếu niên

Sổ tay hướng dẫn đào tạo



Mục lục

Buổi 1:
Các yếu tố quan trọng –
Các tính chất chính của Internet
(180 PHÚT)

Gói đào tạo thanh thiếu niên1

Cung cấp các buổi đào tạo1

Giới thiệu về sổ tay hướng dẫn đào tạo này1

Giới thiệu về điện thoại đào tạo2

Bảo vệ trẻ em2

Lời cảm ơn2

Chào mừng và khảo sát trước đào tạo4

Mạng xã hội ngoài đời thực.....4

Sử dụng công nghệ4

Lập biểu đồ rủi ro để bảo vệ trẻ em trên mạng5

Giới thiệu các yếu tố quan trọng6

Yếu tố "**Công khai**"6

Tra cứu bản thân trên Google6

Cài đặt quyền riêng tư7

Yếu tố "**Vĩnh viễn**"7

Tính năng “Ngày này năm xưa” trên Facebook8

Yếu tố "**Kết nối**"8

Trang web9

Yếu tố "**Ẩn danh**"9

Yếu tố "**Nguồn thông tin**"10

Con rắn đói bụng11

Yếu tố "**Tôn trọng**"11

Bài đăng không tử tế ngoài đời thực11

Chơi game và các yếu tố quan trọng12

Biểu đồ rủi ro – Chơi game13

Tóm tắt13

Buổi 2:
Lên mạng có trách nhiệm
(180 PHÚT)

Giới thiệu16

Bạn muốn làm gì? 16

Lên mạng có trách nhiệm17

Danh tiếng của bạn 17

Bí kíp tương tác trên mạng 18

Viết lại bài đăng18

Biểu đồ rủi ro – Chia sẻ nội dung trên mạng..... 18

Tội phạm lừa đảo trên mạng, tin tặc và tổng tiền dưới sự đe dọa chia sẻ hình ảnh20

Bí kíp bảo vệ chống tội phạm lừa đảo và tin tặc21

Buổi 3:
Ngăn chặn và ứng phó với các vấn đề nghiêm trọng trên mạng
(180 PHÚT)

Lời khuyên trong trường hợp bị lừa đảo 22

Tôi đang trò chuyện với ai qua mạng?..... 22

Chiến lược bảo vệ 23

Bàn tay an toàn 24

Chặn trên Facebook, Instagram và TikTok24

Tóm tắt 25

Giới thiệu 27

Trò chơi nháy mắt27

Nội dung mang tính công kích trên mạng 27

Tìm kiếm an toàn28

Báo cáo trên Facebook, Instagram và TikTok 28

Chặn dắt và xâm hại tình dục trẻ em trên mạng.....29

Dấu hiệu cảnh báo hành vi xâm hại tình dục trẻ em trên mạng 31

Bí kíp phòng tránh tội phạm trên mạng31

Bắt nạt qua mạng 32

Đóng kịch33

Ứng phó với tình trạng bắt nạt qua mạng và xâm hại33

Tóm tắt và Khảo sát sau đào tạo34

Giới thiệu

Gói đào tạo thanh thiếu niên

Sổ tay hướng dẫn này dành cho các chuyên viên đào tạo có nhiệm vụ thực hiện khóa đào tạo Swipe Safe – An toàn trên mạng cho thanh thiếu niên. Đây là sự kiện nằm trong khuôn khổ gói đào tạo toàn diện, được cung cấp cho bạn nhằm hỗ trợ đào tạo thanh thiếu niên. Gói này bao gồm các tài liệu sau:

- **Sổ tay hướng dẫn đào tạo:** Đây là đề cương chi tiết dành cho chuyên viên đào tạo của ba buổi đào tạo dành cho thanh thiếu niên.
- **Video:** Các video 2A, 2B, 3 và 4 có sẵn trực tuyến qua các siêu liên kết và trên USB.
- **Gói thẻ 1 và 2:** Thẻ dùng trong một số hoạt động.
- **Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng:** Hướng dẫn tham khảo dành cho chuyên viên đào tạo về cách truy cập các tính năng đảm bảo an toàn trên những nền tảng được đề cập trong buổi đào tạo.
- **Điện thoại đào tạo:** Người tham gia sẽ sử dụng điện thoại di động (hoặc máy tính bảng) cho một số hoạt động
- **Điện thoại trình chiếu:** Một điện thoại trình chiếu có thể kết nối với máy chiếu bằng cáp/chức năng truyền/phản chiếu để chuyên viên đào tạo minh họa.
- **Máy chiếu:** Có thể kết nối với điện thoại trình chiếu bằng cáp/chức năng truyền/phản chiếu.

Cung cấp các buổi đào tạo

Khóa đào tạo *Swipe Safe – An toàn trên mạng* dành cho thanh thiếu niên dự kiến sẽ do chuyên viên đào tạo trẻ có nhiều kinh nghiệm với các nền tảng mạng xã hội, chơi game và trò chuyện thực hiện. Các chuyên viên đào tạo sẽ chỉ lớn hơn người tham gia vài tuổi. Ngoài ra, do nội dung phức tạp, nên hạn chế số lượng người tham gia trong các nhóm để chuyên viên đào tạo có thể duy trì kiểm soát và hỗ trợ từng người một khi cần thiết. Hai chuyên viên đào tạo có thể phối hợp với nhau: một người dẫn dắt buổi đào tạo, người còn lại sẽ xử lý sự cố và hỗ trợ từng người tham gia.

Có thể tổ chức ba buổi đào tạo dưới dạng hội thảo kéo dài 1,5 ngày hoặc ba buổi đào tạo riêng biệt (tức là mỗi tuần một buổi chiều, kéo dài trong ba tuần).

Các nhóm tham gia nên:

- Là các nhóm gồm tối đa 20 người.
- Từ 12 đến 18 tuổi, nhưng ưu tiên các nhóm bạn cùng tuổi.
- Mỗi người tham gia phải truy cập vào một điện thoại đào tạo cá nhân.
- Các nhóm có thể đào tạo chung hoặc riêng nam – nữ.
- Nên cung cấp hỗ trợ để tạo điều kiện cho người khuyết tật tham gia (chẳng hạn như có thêm chuyên viên đào tạo để hỗ trợ riêng cho một số người tham gia).

Giới thiệu về sổ tay hướng dẫn đào tạo này

Gói sổ tay hướng dẫn đào tạo dành cho thanh thiếu niên này cung cấp mô tả tường thuật cho những thông tin phải chia sẻ với người tham gia. Bạn không cần phải đọc hoặc ghi nhớ chính xác nội dung, chỉ cần diễn đạt những ý tưởng này theo cách của mình.

Sổ tay hướng dẫn này cũng bao gồm nhiều chỉ dẫn cho chuyên viên đào tạo về một số hoạt động. Các chỉ dẫn đều giả định rằng chuyên viên đào tạo đã có đầy đủ kiến thức và kỹ năng về các hoạt động cụ thể, chẳng hạn như sử dụng các tính năng đảm bảo an toàn trên nền tảng. Đảm bảo bạn đã quen thuộc với các hoạt động mà mình sẽ dẫn dắt. Thực hành trước các hoạt động đó và thường xuyên kiểm tra trước mỗi buổi đào tạo vì nhiều nền tảng sẽ sắp xếp lại menu và tùy chọn. Bạn có thể tham khảo Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng để xem hướng dẫn chung. Tuy nhiên, hãy lưu ý rằng các tùy chọn có thể khác biệt đôi chút.

Các biểu tượng được sử dụng trong sổ tay hướng dẫn này:



Giảng dạy trực tiếp phần này cho người tham gia



Đặt câu hỏi này để gợi mở cuộc thảo luận



Minh họa bằng điện thoại trình chiếu



Hướng dẫn cho hoạt động tương tác



Câu trả lời dự kiến từ người tham gia



Chiếu video clip đã chỉ định

Giới thiệu về điện thoại đào tạo

Người tham gia sẽ sử dụng điện thoại đào tạo trong nhiều hoạt động của gói đào tạo Swipe Safe – An toàn trên mạng dành cho thanh thiếu niên. Xin lưu ý rằng trong buổi đào tạo trước đó, người tham gia có thể đã xóa ứng dụng, không đăng xuất khỏi tài khoản hoặc thực hiện các thay đổi khác. Những vấn đề này có thể sẽ làm trì hoãn buổi đào tạo. Nhớ kiểm tra mọi thứ trên điện thoại trước khi người tham gia có mặt.

Trước mỗi buổi đào tạo, hãy mở từng điện thoại và kiểm tra để đảm bảo:

- Đã sạc pin.
- Có đủ dung lượng để sử dụng dữ liệu.
- Ứng dụng không đăng nhập vào tài khoản cá nhân.
- Không có ứng dụng nào dùng trong buổi đào tạo đang chờ cập nhật.
- Đã bật các tùy chọn tìm kiếm an toàn.

Bảo vệ trẻ em

Khóa đào tạo Swipe Safe – An toàn trên mạng bao gồm một số chủ đề nhạy cảm và khó chấp nhận. Một số thanh thiếu niên có thể tiết lộ rằng mình đã từng bị xâm hại hoặc bắt nạt trên mạng. Nếu bạn rất lo ngại về một cá nhân hay tình huống đang diễn ra, bạn nên:

- Lập tức nêu lên quan ngại với nhân viên ChildFund, người sẽ tư vấn về các bước cần thực hiện.
- Nếu không thể liên hệ với nhân viên, bạn có thể gửi email trực tiếp đến địa chỉ childsafeguarding@childfund.org.au để trình bày về quan ngại.
- Trong trường hợp gặp các vấn đề hình sự khẩn cấp, bạn có thể gọi điện trực tiếp vào đường dây nóng của công an theo số 113
- Bạn cũng có thể giới thiệu dịch vụ hỗ trợ sau:
 - Tổng đài điện thoại Quốc gia Bảo vệ trẻ em 111
 - Mạng lưới Bảo vệ trẻ em trên môi trường mạng <https://vn-cop.vn/>
- Nếu mối lo ngại liên quan đến nhân viên ChildFund, bạn có thể bí mật trình báo bằng cách gửi email đến wpo@childfund.org.au

Chính sách Bảo vệ Trẻ em và Chính sách chống Bóc lột, Xâm hại và Quấy rối Tình dục của ChildFund có sẵn trên www.childfund.org.au.

Lời cảm ơn

ChildFund xin chân thành cảm ơn Evident Consulting đã hỗ trợ tái xây dựng các gói đào tạo Swipe Safe – An toàn trên mạng vào năm 2022.

Dự án này được Chính phủ Úc hỗ trợ.

© ChildFund Australia, 2022.

Chỉ được sao chép các đoạn trích từ ấn phẩm này khi có sự cho phép của ChildFund Australia và ghi nguồn trích dẫn.

Buổi 1: Các yếu tố quan trọng

Các tính chất chính của Internet

Mục tiêu học tập

- o Người tham gia hiểu cơ sở hạ tầng cơ bản của Internet.
- o Người tham gia hiểu và có thể áp dụng sáu tính chất chính của Internet.
- o Người tham gia có thể kể tên một số rủi ro và lợi ích khi tương tác trên mạng.

Buổi đào tạo này cần có

- o Sổ tay hướng dẫn đào tạo
- o Điện thoại đào tạo và điện thoại trình chiếu
- o Máy chiếu
- o Loa
- o Áp phích Các yếu tố quan trọng
- o Nhãn dán thẻ tên (chỉ khi người tham gia không biết nhau)
- o Gói thẻ 1: Trực tuyến hay Trực tiếp
- o Bảng trắng hoặc tập giấy lật
- o Bút dạ
- o Cuộn dây
- o Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng (có sẵn để chuyên viên đào tạo tham khảo)
- o Liên kết tới: Khảo sát trước đào tạo
- o Liên kết tới: [VIDEO 2A – Các khái niệm chính về Internet](#)
- o Liên kết tới: [Video 5 – Snake eats car](#)
- o Quét mã QR tham gia khảo sát trước đào tạo trên tờ (màu cam)

Chuẩn bị

- o Sắp xếp 20 ghế theo hình bán nguyệt.
- o Yêu cầu người tham gia lấy thẻ tên (nếu các em không biết nhau).
- o Treo áp phích Các yếu tố quan trọng lên.
- o Bật tất cả điện thoại đào tạo lên và đảm bảo điện thoại đã được sạc pin, cập nhật và có sẵn dữ liệu.
- o Kết nối máy chiếu và loa, đảm bảo mọi thiết bị đều hoạt động.
- o Kết nối điện thoại trình chiếu với máy chiếu và đảm bảo điện thoại hoạt động tốt.
- o Kiểm tra để đảm bảo liên kết video vẫn hoạt động hoặc sử dụng USB để mở video.
- o Đảm bảo bạn có thông tin chi tiết của tài khoản hư cấu trên các nền tảng.
- o Bạn sẽ trình chiếu tính năng “Ngày này năm xưa” trên Facebook trong buổi đào tạo này. Kiểm tra tài khoản của riêng bạn hoặc tài khoản hư cấu để đảm bảo các bài đăng sẽ chiếu đều phù hợp.

Chào mừng và khảo sát trước đào tạo

5 PHÚT

Chào mừng người tham gia và giới thiệu ngắn gọn về các chuyên viên đào tạo.

Nhiệm vụ đầu tiên yêu cầu người tham gia hoàn thành khảo sát ngắn trước đào tạo. Giải thích rằng đây là bài khảo sát dạng trắc nghiệm và chỉ mất 5 phút.

Yêu cầu các em quét mã QR trên tờ màu cam và hoàn thành khảo sát trước đào tạo.

Sau khi các em làm xong khảo sát, tránh giới thiệu hay chuẩn bị dài dòng và nói ngay với người tham gia rằng hoạt động đầu tiên sẽ tiến hành có tên gọi là “mạng xã hội ngoài đời thực”. Bắt đầu nhanh chóng để tạo nhịp độ nhanh cho khóa đào tạo.

Mạng xã hội ngoài đời thực

10 PHÚT

1. Giải thích rằng bạn sẽ yêu cầu người tham gia chào hỏi bạn bên cạnh và tìm hiểu một điều về người đó trong giây lát. Sau 2 phút, bạn sẽ yêu cầu các em nói chuyện với một bạn mới. Sau 2 phút nữa, bạn sẽ lại ngắt lời và yêu cầu các em nói chuyện với một bạn mới. Vậy là các em sẽ phải nói chuyện với tổng cộng ba bạn.
2. Sau khi nói chuyện với ba bạn, yêu cầu các em trở về chỗ ngồi.
3. Tóm tắt hoạt động bằng cách giải thích rằng việc người tham gia vừa làm chính là một kiểu “giao lưu xã hội” – gần giống với cách chúng ta giao tiếp trên mạng, nhưng hoạt động này được thực hiện “ngoài đời thực”.
4. Chỉ ra rằng có một số người tham gia đã quen biết nhau trước khi trò chuyện. Nói rằng một số bạn có thể biết đôi chút về nhau, nhưng không thường xuyên nói chuyện.
5.  **Hỏi xem có những ai gặp nhau lần đầu tiên.**
6.  **Hỏi người tham gia về mức độ thoải mái khi chia sẻ thông tin của bản thân. Các em có thấy khác lạ hay chia sẻ những điều khác lạ với người các em đã quen biết hoặc chưa quen biết không?**
 Cảm thấy xấu hổ/tránh chia sẻ những thông tin cá nhân.
7. Giải thích rằng tương tác xã hội ngoài đời thật và trên mạng vừa giống nhưng cũng vừa khác nhau. Tuy nhiên, việc nghĩ đến cách tương tác ngoài đời thực có thể giúp định hướng hành động trên mạng của chúng ta.
8. Giải thích rằng qua những buổi đào tạo này, chúng ta sẽ cùng nhau thảo luận về thông tin nên hoặc không nên chia sẻ trên mạng cũng như cách xác định những thông tin đó.

Sử dụng công nghệ

2 PHÚT

Giải thích rằng khóa đào tạo được thiết kế để người tham gia có thể thực hành ngay nhiều nội dung vừa thảo luận. Chúng tôi sẽ cung cấp điện thoại di động để các em sử dụng trong ba buổi đào tạo. Giải thích rằng có một số quy tắc đơn giản giúp quản lý hoạt động này.

Cung cấp cho mỗi người tham gia một điện thoại đào tạo và ghi lại số được chỉ định bên cạnh tên các em.

Giải thích quy tắc:

- Khi không sử dụng, vui lòng đặt điện thoại xuống sàn dưới ghế (để không bị phân tâm).
- Yêu cầu các em sử dụng công nghệ có trách nhiệm. Giải thích rằng bạn đã chỉ định cho mỗi người tham gia một chiếc điện thoại di động và lưu hồ sơ về điện thoại đó để theo dõi sự cố hoặc trong trường hợp các em sử dụng điện thoại sai cách. Tuy nhiên, hãy nhấn mạnh rằng bạn tin tưởng các em sẽ cư xử có trách nhiệm và không để xảy ra những vấn đề này.



Lập biểu đồ rủi ro để bảo vệ trẻ em trên mạng 15 PHÚT

- Trong một số hoạt động, người tham gia sẽ được yêu cầu đăng nhập vào tài khoản cá nhân. Nhắc nhở các em rằng cần phải đăng xuất sau khi kết thúc hoạt động.
1. Cho người tham gia biết rằng khóa đào tạo Swipe Safe – An toàn trên mạng sẽ tập trung tìm ra phương thức tối ưu để tham gia đời sống và tương tác trên Internet một cách an toàn.
2. Khi nhắc đến “Internet”, hầu hết mọi người ngày nay đều đã biết đó là gì. Định nghĩa chính thức thường dùng là:

“Một hệ thống thông tin liên lạc giúp kết nối nhiều máy tính và cơ sở dữ liệu trên toàn thế giới”
3. Giải thích cho người tham gia hiểu rằng cũng giống như ngoài đời thực, việc sử dụng Internet có cả lợi ích và rủi ro.
4. **Yêu cầu nhóm tham gia suy nghĩ về những lợi ích mà thế giới trực tuyến đem lại cho thanh thiếu niên.**
 - Tiếp cận lượng thông tin khổng lồ
 - Quan hệ xã hội với bạn bè, gia đình, những người chung sở thích
 - Vui chơi và giải trí
 - Kết bạn khắp thế giới
 - Cơ hội học tập và giáo dục
5. **Yêu cầu nhóm tham gia suy nghĩ về những rủi ro đang tồn tại đối với thanh thiếu niên.**
 - Bắt nạt qua mạng và mâu thuẫn bạn bè
 - Chặn dắt để xâm hại tình dục trẻ em trên mạng
 - Tổng tiền dưới sự đe dọa chia sẻ hình ảnh
 - Phát trực tiếp hành vi xâm hại tình dục
6. Giải thích rằng một số người tham gia có thể đã gặp phải những vấn đề này.
7. **Yêu cầu nhóm tham gia suy nghĩ về những việc có thể làm để cầu cứu khi gặp phải những rủi ro đã nêu.**
 - Kể với người lớn đáng tin cậy
 - Trao đổi với bạn và cùng nhau tìm ra giải pháp
 - Các tổ chức hỗ trợ xã hội
 - Tổng đài Quốc gia Bảo vệ Trẻ em 111
 - <https://vn-cop.vn/>
 - Sự giúp đỡ và lời khuyên từ bạn bè
 - Đường dây nóng của công an 113
 - Tìm kiếm sự giúp đỡ trên mạng
 - Sự hỗ trợ từ phía nhà trường
8. Nhắc người tham gia suy xét cẩn thận về những thông tin các em chọn chia sẻ trong nhóm. Trải nghiệm cá nhân có thể không phù hợp để thảo luận nhóm. Giải thích rằng các em có thể thảo luận riêng những lo ngại với chuyên viên đào tạo sau buổi đào tạo để xin trợ giúp và xin lời khuyên.



Giới thiệu các yếu tố quan trọng 5 PHÚT



Yếu tố "Công khai" 5 PHÚT



Tra cứu bản thân trên Google 10 PHÚT

9. Nhắc nhóm tham gia nên thông cảm cho nhau và xem xét vấn đề này một cách nghiêm túc.

Giải thích cho người tham gia rằng sáu khái niệm chính về Internet sẽ giúp các em hiểu rõ hơn về Internet. Đồng thời, đây cũng là cơ sở cho ba buổi đào tạo của chúng ta. Hướng sự chú ý của các em đến áp phích Các yếu tố quan trọng, đọc sáu khái niệm rồi giới thiệu video:

- **Công khai**
- **Vĩnh viễn**
- **Kết nối**
- **Ẩn danh**
- **Nguồn thông tin**
- **Tôn trọng**

Xem video: [VIDEO 2A – Các khái niệm chính về Internet](#)

Giải thích rằng tất cả mọi người đều có thể sử dụng Internet. Mọi việc chúng ta làm trên mạng đều có khả năng công khai. Bất cứ ai trên thế giới có điện thoại hoặc máy tính đều có thể truy cập Internet. Ai cũng có thể đăng, tải lên hoặc tải xuống mọi thứ. Chúng ta có thể thực hiện một số cách để bảo vệ quyền riêng tư của mình, nhưng nên nhớ rằng mọi thứ trên Internet đều mở và không bị hạn chế.

Giải thích rằng kể từ thời điểm chúng ta sử dụng Internet, chúng ta bắt đầu hiện diện trực tuyến, nơi người khác có thể tìm kiếm thông tin về chúng ta và những việc chúng ta đã làm trên mạng.

Minh họa thao tác tìm kiếm một người nổi tiếng bằng Google.

Hiển thị khối lượng thông tin có sẵn về người này. Giải thích rằng có thể tìm kiếm rất nhiều thông tin về đời sống cá nhân của chúng ta trên mạng nếu không thực hiện các biện pháp cẩn thận để bảo vệ thông tin đó.

Nếu thấy thoải mái, hãy thử tìm thông tin của chính mình trên Google và cho mọi người xem kết quả. Số lượng kết quả sẽ thấp hơn nhiều, nhưng vẫn sẽ có. Chỉ ra rằng một số hình ảnh và bình luận bạn từng đăng lên các nền tảng mạng xã hội như Twitter, TikTok và Facebook có thể sẽ hiện lên trong các tìm kiếm này.

1. Yêu cầu người tham gia lấy điện thoại và mở Google trên trình duyệt Chrome.
2. Chỉ cho các em cách tra cứu tên mình. Nhớ nhắc các em gõ dấu ngoặc kép trước và sau “Tên các em”, nếu không các từ tách biệt sẽ được tìm kiếm riêng chứ không tìm kiếm chung. Tìm kiếm sẽ không trả về nhiều kết quả trừ khi các em có hồ sơ công khai.
3. Sau khi các em tra cứu về bản thân, yêu cầu các em tìm kiếm một số người nổi tiếng hoặc thành viên trong cộng đồng.
4. **Các em tìm thấy những loại thông tin nào đáng ngạc nhiên?**
 - Bài đăng hoặc bình luận mà người nổi tiếng đã đăng.
 - Hình ảnh cũ từ nhiều năm trước.
 - Nội dung đáng xấu hổ hoặc riêng tư của người nổi tiếng.



Cài đặt Quyền riêng tư 5 PHÚT

- Giải thích rằng khái niệm **“công khai”** nghĩa là thông tin chúng ta chia sẻ hoặc đăng tải lên mạng luôn có thể hiển thị công khai, kể cả khi chỉ chia sẻ riêng tư.
- Hỏi các em xem một bức ảnh được chia sẻ riêng tư qua cuộc trò chuyện trên Messenger, Instagram hoặc WhatsApp có thể hiển thị công khai bằng cách nào.**
 - Mọi người có thể chia sẻ lại cho người khác. (Chẳng hạn như bằng cách chụp màn hình).
 - Tài khoản bị truy cập hoặc tấn công.
- Nếu không có câu trả lời nào như trên, hãy giải thích các câu trả lời đó với nhóm tham gia.

- Giải thích rằng việc dễ nhất có thể làm để giảm thiểu tình trạng thông tin của chúng ta trôi nổi tự do trên mạng là thay đổi cài đặt tài khoản trực tuyến từ chế độ công khai thành riêng tư.
- Giải thích rằng tài khoản thường mặc định đặt công khai, do các công ty công nghệ muốn các tài khoản mở để thu được nhiều tương tác (từ đó thu được nhiều lợi nhuận). Khi thiết lập tài khoản mới, người dùng trẻ nên nhớ luôn phải thay đổi các cài đặt này thành chế độ riêng tư để tăng tính bảo mật.
- Dùng điện thoại trình chiếu để minh họa thao tác thay đổi cài đặt Instagram từ chế độ công khai sang riêng tư:
 - Chọn Hồ sơ của bạn và nhấp vào Cài đặt (ba đường thẳng ở góc trên cùng).
 - Chọn Cài đặt.
 - Chọn Quyền riêng tư.
 - Ở phía trên cùng, bật “Tài khoản riêng tư” để chỉ người theo dõi mới xem được nội dung của bạn.
 - Như vậy, bài đăng của bạn sẽ chỉ hiển thị với những người đang theo dõi bạn.

Từ **Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng** có các chỉ dẫn chi tiết giúp chuyên viên đào tạo thực hiện thao tác này.

- Lưu ý cho người tham gia rằng dù rất hữu ích, các tính năng đảm bảo an toàn vẫn chưa hoàn toàn bảo vệ chúng ta. Nhiều sự cố xảy ra do thông tin của chúng ta bị chia sẻ theo cách ngoài dự đoán như có ai đó chụp ảnh màn hình mà không có sự cho phép của bạn. Việc bật cài đặt bảo mật không giúp ngăn chặn những loại rủi ro này.

Người tham gia có thể phản biện rằng một số nền tảng vô hiệu hóa tính năng chụp màn hình (như Snapchat), nhưng bạn có thể đáp lại rằng như vậy cũng không thể ngăn mọi người lấy điện thoại khác để chụp ảnh màn hình.

- Quan trọng là hãy nhớ rằng mọi thứ được đăng lên mạng đều có khả năng công khai. Như vậy sẽ giúp bạn giảm thiểu rủi ro.



Yếu tố "Vĩnh viễn" 5 PHÚT

Yếu tố **“Vĩnh viễn”** có liên quan mật thiết đến yếu tố **“Công khai”**. Giải thích rằng mọi thứ bạn đăng lên trên mạng đều có khả năng tồn tại mãi mãi. Kể cả khi bạn xóa nội dung khỏi hồ sơ để không hiển thị công khai, nội dung đó có thể vẫn còn trong các tệp của công ty. Những công ty điều hành nền tảng công nghệ sẽ lưu trữ mọi dữ liệu chúng ta tạo ra trong các “máy chủ” khổng lồ.



Tính năng “Ngày này năm xưa” trên Facebook 10 PHÚT

Các máy chủ giống như những thư viện to lớn, chứa tất cả dữ liệu chúng ta chia sẻ và đăng lên mạng. Các địa điểm đặt máy chủ trên khắp thế giới đều rất an toàn, nhưng nên nhớ rằng dữ liệu thuộc sở hữu của những công ty này và sẽ tiếp tục tồn tại trong hồ sơ của họ. Với tư cách là người dùng, bạn không có toàn quyền kiểm soát đối với những dữ liệu này.

Hãy nhớ rằng về cơ bản, các bình luận, hình ảnh và bài đăng có thể tiếp tục tồn tại trong các tệp của công ty, kể cả khi đã bị xóa khỏi chế độ xem công khai trên hồ sơ của bạn.

- Minh họa cách truy cập vào mục “Ngày này năm xưa” trên Facebook bằng điện thoại trình chiếu.
- Hiển thị qua một số bài đăng cũ bằng chức năng của tài khoản Facebook hư cấu hoặc tài khoản của riêng bạn.
- Yêu cầu người tham gia đăng nhập vào tài khoản Facebook cá nhân trên điện thoại đào tạo và kiểm tra “Ngày này năm xưa” trên Facebook của mình từ nhiều năm trước. Nếu các em không có tài khoản, hãy cung cấp thông tin đăng nhập vào tài khoản hư cấu.
- Cho thời gian 5 phút rồi yêu cầu các em bỏ điện thoại xuống để thảo luận.
- Hỏi nhóm tham gia xem các em có cảm nhận gì khi thấy những điều mình đã viết hồi xưa. Các em có ngạc nhiên không? Các em có nhớ mình từng đăng không? Các em có biết nội dung cũ này sẽ vẫn còn trên Internet không?**
 - Các em đã quên mất mình từng đăng một số nội dung.
- Minh họa cho người tham gia cách đăng xuất khỏi tài khoản Facebook cá nhân trên điện thoại đào tạo.
- Lưu ý cho người tham gia rằng đăng xuất là một kỹ năng đảm bảo an toàn trên mạng quan trọng mà các em phải nhớ. Giải thích rằng thực ra các công ty công nghệ muốn chúng ta duy trì trạng thái đăng nhập và khiến việc đăng xuất trở nên khó khăn hơn. Đôi khi, chúng ta rất khó tìm vị trí mục đăng xuất!
- Điều này có thể không sao vì ngày nay, chúng ta thường duy trì trạng thái đăng nhập trên thiết bị cá nhân. Tuy nhiên, các em vẫn cần ghi nhớ mật khẩu và thông tin đăng nhập của mình. Sẽ cần phản ứng nhanh nếu có vấn đề xảy ra, chẳng hạn như khi tài khoản bị tấn công. Việc không nhớ thông tin mật khẩu có thể gây ra rắc rối. Đề nghị người tham gia thỉnh thoảng đăng xuất khỏi tài khoản của mình cũng như cập nhật và theo dõi mật khẩu cẩn thận.

Yếu tố **“Kết nối”** đại diện cho cách Internet giúp chúng ta trò chuyện với rất nhiều người từ khắp nơi trên thế giới. Về cơ bản, bạn có thể liên lạc được với bất cứ ai có kết nối Internet.

Lưu ý rằng những kết nối có thể có này sẽ mang đến một số lợi ích tuyệt vời. Ví dụ: Bạn có thể kết nối với bạn bè hoặc gia đình sống ở làng, tỉnh khác hoặc bất cứ đâu trên thế giới.

Tuy nhiên, như vậy cũng có nghĩa là bạn có thể kết giao với tội phạm và những người có ý đồ xấu.



Yếu tố "Kết nối" 2 PHÚT



Trang web 10 PHÚT

1. Yêu cầu tất cả người tham gia đứng lên và tạo thành vòng tròn.
2. Tự mình đứng vào vòng tròn và cầm cuộn dây. Giải thích rằng cuộn dây này đại diện cho kết nối của chúng ta trên khắp thế giới.
3. Nói rằng bạn sẽ cầm một đầu của sợi dây và ném cuộn dây cho người khác. Sợi dây không được rời. Người tiếp theo phải bắt cuộn dây và hô tên một quốc gia (ví dụ: Việt Nam, Hoa Kỳ, Úc, Timor-Leste).
4. Sau đó, người này tiếp tục cầm một đoạn dây và ném cuộn dây cho người tiếp theo hô tên quốc gia mới. Tiếp tục cho đến khi hết cuộn dây hoặc tất cả mọi người đều đã nắm được sợi dây.
5. Hãy nhìn vào mạng lưới đã hình thành giữa mọi người, chỉ ra rằng cũng có một mạng lưới gồm các kết nối trên khắp thế giới khi chúng ta lên mạng.
6. Nói với người tham gia rằng Internet từng được gọi là "World Wide Web" (mạng lưới toàn cầu). Đây chính là cụm "WWW" ở đầu nhiều địa chỉ trang web. Yếu tố **"Kết nối"** là cơ sở cho cách thức hoạt động của Internet.

Giải lao 10 phút



Yếu tố "Ẩn danh" 15 PHÚT

Yếu tố **"Ẩn danh"** nghĩa là mọi người có thể che giấu danh tính thực sự của mình khi lên mạng.

Chỉ ra rằng chúng ta không thể hoàn toàn chắc chắn ai là người chúng ta nói chuyện trên mạng, hay ai là người đang xem nội dung của chúng ta. Việc trao đổi với nhau qua màn hình làm mất đi nét đặc trưng cá nhân của giao tiếp. Chúng ta không thể thấy được ai là người ở đầu bên kia như khi giao tiếp ngoài đời thực.

 Hiện thị ảnh chụp màn hình cuộc trò chuyện giữa hai người bạn:
[Hình ảnh cuộc trò chuyện chặn dặt, dụ dỗ](#)

 **Hỏi xem đây có giống như một cuộc trò chuyện thông thường giữa bạn bè hay không. Cuộc trò chuyện có tự nhiên không? Các em nghĩ hai người này đang cố đạt được điều gì?**

-  Cách diễn đạt có vẻ gượng ép, Daniel không sử dụng những từ ngữ hoặc cụm từ mà thanh thiếu niên sẽ dùng. Cậu ta rất thẳng thừng.
-  Daniel đang ép cô bé làm gì đó.
-  Cô bé có vẻ lưỡng lự và không thoải mái.

Giải thích rằng đây có thể là hai thanh thiếu niên. Có thể người này đang gây áp lực để người kia chia sẻ nội dung khiêu dâm. Nếu cô bé chia sẻ hình ảnh của mình, có nguy cơ hình ảnh đó sẽ được chia sẻ với những người chỉ trích và trêu chọc cô bé. Đây có thể là ví dụ điển hình của tình trạng "bắt nạt qua mạng".

 **Hỏi xem có ai có thể định nghĩa bắt nạt qua mạng hay không.**

-  Là loại hành vi không tử tế thường lặp đi lặp lại.
-  Là hành vi bắt nạt diễn ra trên mạng hoặc có sử dụng công nghệ.

Giải thích rằng chúng ta sẽ tìm hiểu thêm về bắt nạt trên mạng và cách ứng phó với hành vi này trong buổi đào tạo thứ ba. Tuy nhiên, hãy lưu ý rằng hành vi đó thường bao gồm cả yếu tố "Ẩn danh".

Trong ví dụ cuộc trò chuyện này, còn một khả năng khác là Daniel không phải người như hắn ta nói. Hắn ta có thể là một người lớn tuổi. Khi lên mạng, chúng ta không thể nhìn thấy những người mình đã kết nối. Đôi khi, mọi người đóng giả làm người khác vì nhiều lý do khác nhau. Một số người lớn làm vậy để lừa thanh thiếu niên chia sẻ nội dung khiêu dâm.

 **Hỏi xem nhóm tham gia đã nghe đến "chặn dặt tình dục" bao giờ chưa và có ai có thể định nghĩa thuật ngữ này hay không.**

-  Xây dựng mối quan hệ với nạn nhân nhằm mục đích bóc lột tình dục hoặc chụp ảnh hay ghi hình video khiêu dâm..

Cho biết rằng chúng ta cũng sẽ tìm hiểu thêm về hành vi chặn dặt tình dục và cách phòng tránh hoặc cầu cứu trong các buổi đào tạo sau.

Nên ghi nhớ yếu tố **"Ẩn danh"** để không quá dễ dàng tin tưởng những người gặp trên mạng. Không phải lúc nào cũng dễ dàng biết chắc chắn về danh tính thực của một người.

Đây là một số bí kíp giúp bạn xem xét mức độ tin tưởng một người trên mạng:

- Cách diễn đạt của họ có vẻ phù hợp hay khác lạ với một người trạc tuổi bạn?
- Bạn biết họ ngoài đời thực hay chỉ qua mạng?
- Có nội dung có mặt họ trong hồ sơ hay không? Nội dung đó có gần đây không?
- Người này có khiến bạn cảm thấy không thoải mái hay gây áp lực cho bạn không?

Một mẹo quan trọng chính là lắng nghe trực giác của mình. Thông thường, nếu bạn cảm thấy không ổn thì có thể thực sự có vấn đề. Tuy nhiên, kể cả khi cảm thấy thoải mái, hãy cố gắng ghi nhớ rằng chúng ta không thể hoàn toàn chắc chắn ai là người mình đang nói chuyện trên mạng và phải luôn hành xử có ý thức.



Yếu tố "Nguồn thông tin" 10 PHÚT

Yếu tố thứ năm là về lượng thông tin khổng lồ trên mạng. Internet cho phép chúng ta tiếp cận lượng thông tin rất lớn. Điều này mang lại vô vàn ảnh hưởng tích cực. Về cơ bản, Internet có sẵn đáp án cho hầu hết mọi câu hỏi.

Tuy nhiên, lượng thông tin lớn cũng gây ra nhiều vấn đề vì sẽ khó nhận biết thông tin đó có đúng, chính xác hoặc đáng tin cậy hay không. Việc tìm kiếm trên Internet đòi hỏi chúng ta suy xét cẩn thận về nguồn thông tin mà chúng ta tìm thấy.

Những thông tin xuất hiện khi chúng ta tìm kiếm chưa hẳn đã là thông tin đúng sự thật. Tính năng tìm kiếm sẽ trả về những kết quả phổ biến nhất. Không phải lúc nào chúng ta cũng nhận được kết quả chính xác nhất.

Bất cứ ai cũng có thể dễ dàng viết "tin giả" và đăng lên mạng. Nếu tin đó có nhiều lượt chia sẻ và trở nên phổ biến thì nhiều người sẽ dễ tin rằng đó là sự thật.

Con rắn đối bụng 15 PHÚT



1. Dùng điện thoại trình chiếu để mở: [Video 5 – Con rắn nuốt chứng xe ô tô](#)
2. Hỏi qua xem người tham gia có tin video đó là thật hay không. Sau đó, yêu cầu các em dành 5 phút sử dụng điện thoại đào tạo để xem có tìm hiểu được gì về chuyện này trên mạng hay không.
3. **Yêu cầu người tham gia cung cấp các mẹo giúp các em kiểm tra tính xác thực của vấn đề.**
 - A Địa chỉ web rất dài và phức tạp.
 - A Trong đó không có tên tác giả hoặc thông tin về người đăng tin (thường thấy ở cuối trang web đáng tin cậy).
 - A Bạn có thể tìm kiếm qua vụ việc trên Google để xem vụ việc đó đã được chứng minh là sai sự thật hay chưa.
 - A Việc có nhiều quảng cáo không liên quan (về cờ bạc hoặc khiêu dâm) trên trang có thể cho thấy đây là trang web không đáng tin cậy.
 - A Trang web có “https” ở đầu sẽ an toàn và đáng tin cậy hơn.
4. Tuy nhiên, hãy nhắc nhở người tham gia rằng tin giả ngày càng có sức thuyết phục. Chúng ta cần phải vận dụng kỹ năng tư duy phản biện để đánh giá thông tin chứ không vội vàng chấp nhận.
5. Suy nghĩ kỹ trước khi chia sẻ với người khác, nếu không sẽ thật ngớ ngẩn nếu bạn chia sẻ thông tin mà sau đó hóa ra là tin giả.

Yếu tố “Tôn trọng” 10 PHÚT

Yếu tố cuối cùng là **“Tôn trọng”**. Khi tương tác qua màn hình, chúng ta có thể sẽ quên mất rằng mình đang kết nối với người khác. Hoạt động giao tiếp có thể tạo cảm giác ít mang tính cá nhân hơn.

Có thể bạn không cố ý, nhưng khi không thể thấy phản ứng của người khác thì bạn sẽ không nhận được phản hồi về ảnh hưởng của lời bạn nói.

Đây là điều thường thấy khi phát trực tiếp – một dạng giao tiếp khá một chiều. Tình trạng này cũng thường xảy ra trong nhóm trò chuyện hoặc phòng phát sóng trực tiếp của game thủ, trong đó bạn sẽ không thể thấy phản ứng tức thì của người khác.

Nếu không chú ý, kiểu trò chuyện này có thể trở thành bắt nạt hoặc phát ngôn gây thù hận (như phân biệt chủng tộc, phân biệt giới tính, kỳ thị đồng tính). Những điều này chắc chắn có thể gây tác động tiêu cực đến nạn nhân, cũng như khiến thanh thiếu niên gặp rắc rối nghiêm trọng khi phát ngôn như vậy.

Nên nhớ rằng phải tôn trọng người khác và chính bản thân, từ đó hành động đúng đắn trên môi trường mạng. Hãy tự hỏi bản thân xem bạn có định nói thẳng điều đó trước mặt họ hay không.

1. Kẻ một đường thẳng trên bảng trắng/tập giấy lật, viết “trực tuyến” ở một bên và “trực tiếp” ở bên còn lại.
2. Gọi hai bạn xung phong. Đưa cho mỗi em một nửa số thẻ trong **Gói thẻ 1: Trực tuyến hay Trực tiếp**. Cho người tham gia biết rằng đây là những ví dụ lấy từ nhiều bình luận công khai về người nổi tiếng trên mạng.

Chơi game và các yếu tố quan trọng 20 PHÚT

3. Yêu cầu hai bạn xung phong đứng đối diện nhau và lần lượt đọc to các câu phát biểu cho nhau nghe.
4. Sau mỗi câu các em đọc, hỏi nhóm tham gia xem các em có nghĩ câu nói này thô lỗ hay không.
5. Hỏi cảm nhận của hai bạn xung phong khi trực tiếp nói những lời đó với người đối diện. Có câu nào các em không nói được không?
6. **Hỏi nhóm tham gia rằng: nếu đây là lời nói rất thô lỗ khi nói trực tiếp, vậy tại sao mọi người lại viết ra những câu đó trên mạng?**
 - A Lời nói trên mạng ít mang tính cá nhân hơn.
 - A Người nói ở chế độ ẩn danh.
 - A Người nói không thể thấy phản ứng của người khác.
7. Giải thích rằng lý do chính khiến chúng ta dễ tỏ ra thiếu tôn trọng trên mạng hơn là do không thể thấy ngôn ngữ cơ thể của người khác. Bạn có thể nhận được thông tin tức thì từ người khác khi nói chuyện trực tiếp. Còn trên mạng, người khác không thấy bạn và bạn cũng vậy. Trên thực tế, có thể phải mất đến vài giờ hoặc vài ngày sau đó thì người khác mới thấy bình luận của bạn.
8. Việc hành động làm tổn thương người khác trở nên dễ dàng hơn trong môi trường mạng. Tuy nhiên, điều này vẫn để lại hậu quả. Trong khi người nổi tiếng có thể không đọc những bình luận này, mọi người thường đọc hết những gì mọi người viết.
9. Người ta dễ dàng phát ngôn ác ý hơn. Hãy nhớ rằng phát ngôn như vậy sẽ để lại hậu quả và người khác có thể đánh giá bạn qua hành vi kém văn minh trên mạng. Bạn thậm chí có thể vướng vào rắc rối. Phải luôn ghi nhớ yếu tố “tôn trọng” để giao tiếp trên mạng cho đúng mực.

1. **Hỏi xem người tham gia thích chơi game trực tuyến nào.**
 - A Roblox, Fortnite, Minecraft, League of Legends, World of Warcraft, PUBG, Halo, FIFA, Animal Crossing, v.v.
2. Chia thành 4 nhóm, phát tập giấy lật và bút cho mỗi nhóm. Yêu cầu các em suy nghĩ về việc chơi game trực tuyến và viết ra liên hệ của hoạt động này với sáu khái niệm chính.
3. **Các yếu tố quan trọng áp dụng vào hoạt động chơi game trực tuyến như thế nào?**
 - A **Công khai** – Bất cứ ai chơi game trực tuyến đều có thể xem được thao tác, cuộc trò chuyện hoặc hồ sơ game thủ của chúng ta. Bạn phải đảm bảo không có phát ngôn hoặc hành động làm ảnh hưởng đến danh tiếng của mình trên mạng.
 - A **Vĩnh viễn** – Các máy chủ sẽ lưu trữ mọi thông tin trong quá trình chơi game. Chúng ta không thể xóa bỏ những thông tin này, kể cả khi đã xóa khỏi hồ sơ công khai. Bạn cũng cần lưu ý về những thông tin bạn cung cấp khi đăng ký tài khoản để chơi game. Ví dụ: Bạn không nên cung cấp tên thật trong ảnh đại diện hoặc cung cấp thông tin cá nhân như địa chỉ của mình cho game thủ khác. Bạn phải cực kỳ cẩn trọng khi cung cấp những thông tin như thông tin ngân hàng.



Biểu đồ rủi ro – Chơi game 5 PHÚT



Tóm tắt 5 PHÚT

- A Kết nối** – Internet cho phép chúng ta kết nối và chơi với bất cứ ai trên thế giới. Tuy nhiên, không phải ai chơi cùng cũng là người tốt và đáng tin cậy. Bạn phải có ý thức bảo vệ thông tin cá nhân và đảm bảo mình không dễ bị lừa đảo khi tương tác với người chơi khác.
- A Ẩn danh** – Bạn có thể không biết người đang chơi trực tuyến cùng mình thực sự là ai. Mọi người có thể che giấu danh tính của mình khi chơi game. Điều này mang lại lợi ích đối với quyền riêng tư của bạn. Tuy nhiên, một số người cũng có thể lợi dụng điểm này để che giấu ý đồ xấu.
- A Nguồn thông tin** – Bạn có thể nhận được thông tin sai lệch trong khi chơi game như cách vượt qua một cấp độ nhất định hoặc cách gian lận. Bạn nên cẩn thận khi làm theo bất kỳ chỉ dẫn nào. Hãy nghĩ xem lý do tại sao người ta lại cho bạn biết thông tin đó.
- A Tôn trọng** – Chúng ta cần chú ý cách chúng ta trò chuyện với các game thủ trực tuyến khác và nhận thức được những phát ngôn gây thù hận như phân biệt chủng tộc, phân biệt giới tính hoặc kỳ thị đồng tính.

1. **?** **Giải thích cho người tham gia rằng dù việc chơi game trực tuyến rất thú vị nhưng vẫn có một số rủi ro cần lưu ý. Yêu cầu các em đưa ra đề xuất. Trình bày những ý sau nếu chưa được nêu:**
 - A** Bạn có thể đang dành quá nhiều thời gian trên mạng nếu việc này ảnh hưởng đến các hoạt động khác trong đời sống.
 - A** Bạn có thể bắt gặp hình ảnh bạo lực, ngôn từ thô tục, phát ngôn gây thù hận hoặc các nội dung khác gây khó chịu khi chơi game trực tuyến (cả trong trò chơi và khi giao tiếp với những người chơi khác).
 - A** Người chơi khác có thể yêu cầu bạn cung cấp thông tin cá nhân khi chơi game trực tuyến.
 - A** Người chơi khác có thể cư xử tệ hại (bằng cách sử dụng ngôn từ thô tục hoặc tỏ ra thô lỗ) hay khiến bạn cảm thấy không thoải mái.
 - A** Các trò chơi có thể yêu cầu bạn trả tiền để truy cập thêm nhiều cấp độ hoặc tính năng khác.

Đưa ra tóm tắt ngắn gọn về các yếu tố quan trọng:

Công khai: Mọi thông tin bạn đăng hoặc chia sẻ lên mạng, kể cả ở chế độ riêng tư, đều có khả năng hiển thị công khai.

Vĩnh viễn: Mọi thứ chúng ta đăng lên Internet có thể tồn tại mãi mãi.

? **Hãy hỏi xem điều này xảy ra bằng cách nào.**

- A** Mọi nội dung được chia sẻ lên các nền tảng đều có thể còn trong máy chủ.

Kết nối: Internet cho phép chúng ta kết nối với mọi người trên khắp thế giới, nhưng không phải ai cũng đáng tin.

Ẩn danh: Mọi người có thể che giấu danh tính của mình trên mạng. Một số người có thể lợi dụng điểm này để lừa đảo hoặc làm hại chúng ta.

Nguồn thông tin: Chúng ta có thể tiếp cận một lượng thông tin khổng lồ, nhưng cần suy xét cẩn thận xem thông tin đó có đúng, chính xác và đáng tin cậy hay không.

Tôn trọng: Khi tương tác với mọi người qua màn hình, hoạt động giao tiếp có thể ít mang tính cá nhân và ít tử tế hơn. Nên nhớ rằng chúng ta đang nói chuyện với con người và cần phải tôn trọng người khác cũng như tôn trọng chính chúng ta.

Cho người tham gia biết rằng trong những buổi đào tạo tiếp theo, các em sẽ được tìm hiểu thêm về một số rủi ro liên quan đến việc sử dụng Internet và cách giữ an toàn trên không gian mạng.

Cảm ơn người tham gia vì đã đến dự.

Buổi 2: Lên mạng có trách nhiệm

Mục tiêu học tập

- o Người tham gia áp dụng các tính chất chính của Internet vào các ví dụ thực tế.
- o Người tham gia hiểu được cách thức hoạt động của tội phạm lừa đảo trên mạng và tin tặc.
- o Người tham gia tìm hiểu và thực hành các chiến lược bảo vệ cụ thể trên mạng.

Buổi đào tạo này cần có

- o Sổ tay hướng dẫn đào tạo
- o Điện thoại đào tạo và điện thoại trình chiếu
- o Máy chiếu
- o Loa
- o Áp phích Các yếu tố quan trọng
- o Tờ rơi 6 Viên đá thiêng
- o Gói thẻ 2: Danh tiếng của bạn
- o Bảng trắng hoặc tập giấy lật
- o Bút dạ
- o Tờ rơi: Bí kíp giữ an toàn trên mạng dành cho thanh thiếu niên (mỗi người một tờ)
- o Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng (có sẵn để chuyên viên đào tạo tham khảo)
- o Liên kết tới: [VIDEO 3 – Lừa đảo và Tấn công](#)
- o Liên kết tới: [VIDEO 2B – Các tính chất chính của Internet và Chiến lược bảo vệ](#)

Chuẩn bị

- o Sắp xếp 20 ghế theo hình bán nguyệt.
- o Treo áp phích Các yếu tố quan trọng lên.
- o Bật tất cả điện thoại đào tạo lên và đảm bảo điện thoại đã được sạc pin, cập nhật và có sẵn dữ liệu.
- o Kết nối máy chiếu và loa, đảm bảo mọi thiết bị đều hoạt động.
- o Kết nối điện thoại trình chiếu với máy chiếu và đảm bảo điện thoại hoạt động tốt.
- o Kiểm tra để đảm bảo liên kết video vẫn hoạt động hoặc sử dụng USB để mở video.
- o Đảm bảo bạn có thông tin chi tiết của tài khoản hư cấu trên các nền tảng.
- o Bạn cần có ví dụ về bài đăng không phù hợp cho một hoạt động trong buổi đào tạo này. Đảm bảo rằng bạn đã tạo một ví dụ có thể sử dụng trong tài khoản hư cấu.



Giới thiệu
5 PHÚT

Chào mừng người tham gia đến với buổi đào tạo thứ hai. Phát điện thoại đào tạo và ghi lại số được chỉ định. Nhắc các em đặt điện thoại xuống dưới ghế ngồi trong khoảng thời gian giữa các hoạt động.

Dành chút thời gian để ôn qua sáu yếu tố quan trọng trong buổi đào tạo trước. **Bỏ qua phần tóm lược nếu buổi đào tạo 2 được tổ chức cùng ngày với buổi đào tạo 1.**

Công khai: Mọi thông tin bạn đăng hoặc chia sẻ lên mạng, kể cả ở chế độ riêng tư, đều có khả năng hiển thị công khai.

Vĩnh viễn: Mọi thứ chúng ta đăng lên Internet có thể tồn tại mãi mãi.

Kết nối: **Internet** cho phép chúng ta kết nối với mọi người trên khắp thế giới, nhưng không phải ai cũng đáng tin.

Ẩn danh: Mọi người có thể che giấu danh tính của mình trên mạng. Một số người có thể lợi dụng điểm này để lừa đảo hoặc làm hại chúng ta.

Nguồn thông tin: Chúng ta có thể tiếp cận một lượng thông tin khổng lồ, nhưng cần suy xét cẩn thận xem thông tin đó có đúng, chính xác và đáng tin cậy hay không.

Tôn trọng: Khi tương tác với mọi người qua màn hình, hoạt động giao tiếp có thể ít mang tính cá nhân và ít tử tế hơn. Nên nhớ rằng chúng ta đang nói chuyện với con người và cần phải tôn trọng người khác cũng như tôn trọng chính chúng ta.



Bạn muốn làm gì?
5 PHÚT

1. Yêu cầu người tham gia di chuyển thành một nhóm ở giữa phòng.
2. Giải thích rằng bạn sẽ đưa ra hai sự lựa chọn và các em phải di chuyển sang trái hoặc sang phải để bày tỏ ý thích của mình. Các em phải chọn thật nhanh.
3. Trong khi đọc, dùng tay còn lại ra hiệu bên trái hoặc bên phải cho từng lựa chọn.
4. Giải thích rằng đây là trò chơi tốc độ và các em phải chọn thật nhanh. (Không có thời gian suy nghĩ hay nhìn người khác trước khi chọn!)
5. Đọc to các câu, cho các em thời gian về chỗ và sau đó nhanh chóng tiếp tục. Khiến các em phải di chuyển thật nhanh!
6. Bạn muốn:
 - Chỉ chơi game hay chỉ xem YouTube trong 24 giờ không ngừng nghỉ?
 - Được phép chỉ sử dụng TikTok hay chỉ sử dụng Instagram cả đời?
 - Có 1 triệu đô la hay 1 triệu người theo dõi?
 - Nổi tiếng trên Instagram hay trên Twitch?
 - Nhận iPhone miễn phí hay điện thoại Galaxy miễn phí?
 - Được Beyonce hay Jungkook (BTS) theo dõi trên mạng xã hội?
 - Gặp Beyonce hay Jungkook ngoài đời thực?
 - Công khai mọi cuộc trò chuyện hay mọi hình ảnh trong điện thoại?
 - Trở thành hiện tượng vì điệu nhảy hay giọng hát?
 - Là giám đốc điều hành của Meta (Facebook/Instagram) hay của TikTok trong một ngày?
7. Yêu cầu người tham gia trở về chỗ ngồi.



Lên mạng có trách nhiệm 5 PHÚT

Giải thích rằng giống như ngoài đời thực, cách chúng ta hành xử trên mạng cũng sẽ để lại hệ quả tích cực và tiêu cực. Những hành vi trong quá khứ có thể ảnh hưởng đến cách gia đình, bạn bè, cộng đồng và cả những nhà tuyển dụng nhìn nhận về chúng ta hiện tại, tương lai, cả trên mạng lẫn ngoài đời. Đây là “đanh tiếng”.

Hãy nhớ rằng yếu tố “**Vĩnh viễn**” nghĩa là mọi điều chúng ta làm trên mạng đều có thể tồn tại suốt cuộc đời.

Lên mạng có trách nhiệm là hành xử có đạo đức và tôn trọng khi tham gia vào đời sống trên mạng của cộng đồng. Nghĩa là:

- Hành xử đúng luật. Ví dụ: Việc tấn công, đánh cắp, tải xuống trái phép hoặc gây thiệt hại cho công việc, danh tính hoặc tài sản của người khác là trái pháp luật.
- Thực hiện các biện pháp để bảo vệ quyền riêng tư của chính bản thân và của người khác.
- Nhận thức rõ rằng bạn có cả quyền lẫn trách nhiệm trên không gian mạng.
- Hãy thử nghĩ xem hoạt động trên mạng của bạn có thể ảnh hưởng ra sao đến cách mọi người bạn biết và cộng đồng lớn hơn nhìn nhận bạn.

Đề cập đến yếu tố “**Công khai**” và nhắc nhở người tham gia rằng tất cả mọi người đều có thể nhìn thấy những điều chúng ta nói hoặc làm.

Đề cập đến yếu tố “**Nguồn thông tin**” và nhắc nhở người tham gia rằng những thông tin chúng ta chia sẻ cần đúng sự thực, chính xác và đáng tin cậy để không gây nhầm lẫn cho bạn bè và gia đình vì đăng thông tin giả mạo.



Đanh tiếng của bạn 15 PHÚT

1. Hoạt động này sẽ giúp người tham gia suy nghĩ về cách hành xử tôn trọng và lịch sự đối với bản thân và những người khác khi lên mạng.
2. Yêu cầu người tham gia sử dụng điện thoại đào tạo để **đăng nhập** vào một tài khoản cá nhân của mình (ví dụ: Facebook, Instagram hoặc TikTok). Nếu các em không có tài khoản, hãy cung cấp thông tin đăng nhập vào tài khoản hư cấu.
3. Yêu cầu người tham gia nhìn lại năm bài đăng, bình luận và lượt thích gần nhất của các em. Cho các em thời gian 5 phút để thực hiện.
4. Dán các câu hỏi trong **Gói thẻ 2: Danh tiếng của bạn** lên tường cho dễ thấy.
5. Đọc qua các câu hỏi trên thẻ và yêu cầu người tham gia cân nhắc trả lời dựa trên những bài đăng, bình luận và lượt thích mà các em đang xem.
6. **Yêu cầu người tham gia đưa ra ví dụ mà các em thấy có thể sẽ tạo hình tượng không tốt về mình.**
7. **Hỏi người tham gia xem sẽ có hậu quả gì nếu các nhóm được đề cập trong thẻ nhìn thấy nội dung này. Các em vẫn sẽ phát ngôn như vậy chứ?**
8. Giải thích rằng đôi khi lời nói của bạn có thể khiến người khác khó chịu, nhưng bạn vẫn quyết định nói ra. Việc bày tỏ quan điểm về một chủ đề là chuyện bình thường. Tuy nhiên, có thể có những lúc bạn chỉ đơn giản viết ra suy nghĩ mà chưa cân nhắc xem người khác sẽ thấy ra sao khi đọc được.
9. Nhắc nhở người tham gia rằng nội dung chúng ta đăng, bình luận hoặc thích có thể không xấu hay phạm pháp, nhưng việc tương tác với nội dung đó vẫn sẽ phản ánh về chúng ta.
10. **Hỏi về những bài đăng hoặc bình luận khiến người khác gặp rắc rối mà các em có thể đã thấy trên mạng.**
 - Chỉ trích những người nổi tiếng hoặc chính trị gia. Người bị nhắm đến có thể không đọc được, nhưng người khác lại thấy và khó chịu.



Bí kíp tương tác trên mạng 5 PHÚT

- Chỉ trích bạn bè hoặc những người trong cộng đồng để họ nhìn thấy và khó chịu.
 - Chỉ trích bất hợp pháp và phát ngôn gây thù hận.
11. Chỉ ra rằng cho dù không đăng bài hay bình luận, việc các em xem hoặc thích một số nội dung nguy hiểm vẫn có thể phản ánh xấu về các em (ví dụ: phân biệt chủng tộc, phân biệt giới tính, kỳ thị đồng tính).
 12. Lưu ý rằng trong nhiều trường hợp, những nội dung khiến mọi người vướng vào rắc rối đều mang tính chất tiêu cực. Nếu bạn định chỉ trích, hãy nghĩ kỹ xem điều đó có cần thiết hay không, sẽ đạt được kết quả gì và nhận hậu quả gì.
 13. Nhắc các em đăng xuất khỏi tài khoản cá nhân và đặt điện thoại xuống trước khi chuyển sang phần tiếp theo.

Thảo luận ngắn gọn về mỗi hành động sau:

- Suy nghĩ trước khi đăng, thích, bình luận, trò chuyện, tải lên hoặc tải xuống nội dung từ trên Internet. Nghĩ xem hành động của bạn sẽ ảnh hưởng ra sao đến danh tiếng của bạn và đến những người khác khi nhìn thấy.
- Tự hỏi bản thân xem những nội dung bạn đăng có làm tổn thương chính mình hay người khác không.
- Đối xử với người khác theo cách bạn muốn được đối xử trên mạng.
- Sử dụng biểu tượng cảm xúc để giúp mọi người hiểu cảm xúc phía sau những lời bạn nói trên mạng. (Ví dụ: biểu tượng mặt nháy mắt cho biết rằng bạn đang đùa).
- Nếu bạn không nói hoặc làm việc đó ngoài đời thực thì cũng đừng nói hay làm vậy trên mạng.
- Phát **Tờ rơi: Bí kíp giữ an toàn trên mạng dành cho thanh thiếu niên**. Lưu ý rằng chúng ta sẽ đề cập đến các phần khác ở buổi đào tạo sau.



Viết lại bài đăng 10 PHÚT

1. Chiếu ví dụ bài đăng không phù hợp trên tài khoản hư cấu của một nền tảng (Facebook, Instagram, v.v.) mà bạn đã chuẩn bị trước buổi đào tạo.
2. Yêu cầu người tham gia đọc bài đăng không phù hợp và nghĩ cách thay đổi bài đăng hoặc khiến bài đăng đó trở nên rõ ràng hơn. Ví dụ: Các em có thể dùng biểu tượng cảm xúc hoặc từ ngữ khác để làm rõ nghĩa.
3. Yêu cầu các em làm việc theo cặp trong vài phút để viết một phiên bản khác của bài đăng. Đây vẫn có thể là nội dung chỉ trích và tiêu cực, nhưng giọng văn không được ác ý hoặc mang tính cá nhân.
4. Yêu cầu một số người tham gia chia sẻ phiên bản của mình và đưa ra lời khuyên.



Biểu đồ rủi ro – Chia sẻ nội dung trên mạng 5 PHÚT

1. Đưa ra hai tình huống sau cho người tham gia, trong đó có những hành vi có thể khiến các em gặp rắc rối trên mạng:
 - **Tình huống A:** Một người gửi ảnh gợi cảm qua Messenger cho bạn trai/bạn gái dưới 18 tuổi.
 - **Tình huống B:** Một người chia sẻ video clip qua tin nhắn riêng tư, trong đó ghi lại cảnh một số bạn đột nhập vào công trường xây dựng và phá hoại tài sản.
2. Chia người tham gia thành bốn nhóm và phát tập giấy lật cho mỗi nhóm. Chỉ định một trong hai tình huống cho từng nhóm.
3. Yêu cầu các nhóm thực hiện hai việc sau:
 - Liệt kê tất cả các hệ quả có thể xảy ra trong tình huống đã cho.
 - Nhận biết các yếu tố quan trọng có thể liên quan đến tình huống này.

- Cho các em thời gian 10 phút.
- Tóm tắt nhanh các câu trả lời trên tập giấy lật. Câu trả lời dự kiến:

Tình huống A – Hệ quả:

-  Nếu ảnh bị chia sẻ công khai thì sẽ có thể ảnh hưởng tiêu cực đến cách người thân, bạn bè, nhà tuyển dụng hiện tại/tương lai nhìn nhận bạn và hủy hoại thanh danh của bạn trên mạng.
-  Công an có thể buộc tội bạn vì hành vi tạo và lưu hành nội dung khiêu dâm trẻ em.
-  Bạn có thể thấy xấu hổ hoặc ngượng ngùng nếu hình ảnh được chia sẻ với những người khác.
-  Việc này có thể dẫn đến tình trạng bắt nạt qua mạng hoặc hình ảnh bị tội phạm sử dụng để ép bạn gửi thêm ảnh hoặc liên hệ với xâm hại tình dục.
-  Hình ảnh có thể bị chia sẻ trên toàn thế giới và tội phạm trên mạng có thể tiếp cận với hình ảnh đó.

Tình huống A – Các yếu tố:

-  **Công khai** – Hình ảnh này có thể hiển thị công khai nếu được người khác chia sẻ, kể cả khi ban đầu bạn chỉ chia sẻ riêng tư.
-  **Vĩnh viễn** – Mọi thứ chúng ta chia sẻ lên mạng có thể tồn tại trên mạng mãi mãi, chỉ có công an và các cơ quan chính phủ mới có thể gỡ hình ảnh đó xuống.
-  **Kết nối** – Hình ảnh này có thể được chia sẻ trên toàn thế giới chỉ bằng vài cú nhấp chuột.
-  **Ấn danh** – Tội phạm có thể đóng giả người bạn biết hoặc xâm hại bạn bằng hình thức tống tiền dưới sự đe dọa chia sẻ hình ảnh.
-  **Tôn trọng** – Hình ảnh này có thể ảnh hưởng tiêu cực đến cách bạn bè và gia đình nhìn nhận bạn.

Tình huống B – Hệ quả:

-  Đoạn video có thể xác định những người liên quan và làm bằng chứng cho hậu quả pháp lý.
-  Thanh danh trên mạng và ngoài đời của bạn có thể bị ảnh hưởng trước người thân, bạn bè hoặc nhà tuyển dụng hiện tại/tương lai.
-  Bạn có thể gặp rắc rối với trang web mà bạn đăng video, chẳng hạn như Facebook có thể cấm tài khoản của bạn.
-  Bạn có thể làm ảnh hưởng đến người khác mà không biết, chẳng hạn như thanh thiếu niên khác có thể nghĩ hành động của bạn là bình thường và bắt chước theo.

Tình huống B – Các yếu tố:

-  **Công khai** – Hình ảnh này có thể hiển thị công khai nếu được người khác chia sẻ, kể cả khi ban đầu bạn chỉ chia sẻ trong tin nhắn riêng tư.
-  **Vĩnh viễn** – Mọi thứ chúng ta đăng lên mạng có thể tồn tại trên mạng mãi mãi và để lại hệ quả trong nhiều năm nếu bị người khác thấy.
-  **Kết nối** – Hình ảnh này có thể được chia sẻ với người khác, kể cả công an.
-  **Tôn trọng** – Hình ảnh này có thể ảnh hưởng tiêu cực đến bạn bè và gia đình bạn.

Tội phạm lừa đảo trên mạng, tin tặc và tống tiền dưới sự đe dọa chia sẻ hình ảnh 20 PHÚT



Giải thích cho người tham gia rằng không phải ai cũng sử dụng Internet vì những lý do chính đáng.

Hỏi xem người tham gia có biết “tội phạm lừa đảo” và “tin tặc” hay không. Giải thích những ý sau:

Tội phạm lừa đảo cố gắng lừa mọi người cấp quyền truy cập vào tài khoản mạng xã hội, tài khoản ngân hàng hoặc các thông tin cá nhân khác.

Tin tặc sử dụng Internet để bẻ khóa bảo mật và truy cập trái phép vào tài khoản, nội dung hoặc thông tin cá nhân của chúng ta.

Yêu cầu người tham gia đưa ra một số ví dụ về lừa đảo hoặc tấn công. Chia sẻ những ví dụ dưới đây nếu các em chưa nêu lên.

-  Truy cập vào tài khoản mạng xã hội của người khác rồi gửi tin nhắn cho bạn bè của tài khoản đó để yêu cầu chuyển tiền vào tài khoản của mình.
-  Gửi tin nhắn mời nhận việc, tiền bạc hoặc cơ hội có vẻ tốt đến mức khó tin. Ví dụ: Đề nghị mức lương cao cho người không có kinh nghiệm làm việc.
-  Đề nghị chuyển tiền nếu bạn cung cấp thông tin tài khoản ngân hàng.
-  Cuộc gọi hoặc tin nhắn thông báo rằng tài khoản của bạn đã bị tấn công và họ sẽ giúp bạn lấy lại quyền kiểm soát (nếu bạn cung cấp thông tin hoặc nhấp vào liên kết họ gửi).
-  Tin nhắn yêu cầu cung cấp thông tin cá nhân hoặc thông tin tài khoản.
-  Tin nhắn, email hoặc quảng cáo thông báo rằng bạn đã trúng thưởng hoặc đoạt giải trong cuộc thi mà bạn không tham gia.
-  Đề nghị giảm giá sập sàn cho các sản phẩm và mặt hàng xa xỉ.
-  Lừa mọi người chia sẻ nội dung khiêu dâm.

 Xem phần đầu của video: [VIDEO 3 – Lừa đảo và Tấn công](#) (tạm dừng lúc 1:30)

Hỏi xem động cơ của tội phạm lừa đảo và tin tặc là gì.

-  Lừa chúng ta cung cấp thông tin cá nhân.
-  Lấy được quyền truy cập vào thiết bị của chúng ta, bằng cách để chúng ta tải “phần mềm độc hại” hoặc “virus” khi nhấp vào các liên kết có thể cấp quyền truy cập.
-  Truy cập nội dung hoặc tiếp cận tiền bạc của chúng ta.

Hỏi xem nhóm tham gia đã nghe đến “tống tiền dưới sự đe dọa chia sẻ hình ảnh” bao giờ chưa và có ai có thể định nghĩa thuật ngữ này hay không.

-  Lấy hình ảnh hoặc video khiêu dâm của nạn nhân, thường bằng cách lừa gạt mà có hoặc đe dọa chia sẻ hình ảnh đã có với công chúng hoặc gia đình và bạn bè của nạn nhân nếu nạn nhân không gửi tiền hoặc gửi hêm ảnh. Lời đe dọa có thể là thật hoặc giả.



Bí kíp bảo vệ chống tội phạm lừa đảo và tin tặc 15 PHÚT



Giải thích rằng có nhiều cách để ngăn tin tặc và tội phạm lừa đảo lấy được quyền truy cập và gây rối.

Xem phần còn lại của video: [VIDEO 3 – Lừa đảo và Tấn công](#)
(phát từ lúc 1:30 đến hết)

Nhấn mạnh các thông điệp sau trong video:

- Sử dụng yếu tố **“Ẩn danh”** để nhớ rằng tội phạm có thể ẩn mình và lừa chúng ta chia sẻ thông tin cá nhân.
- Sử dụng yếu tố **“Nguồn thông tin”** để tự nhắc bản thân rằng không phải nội dung nào thấy trên mạng cũng là sự thật và đáng tin cậy.
- Không được cung cấp thông tin cá nhân qua công nghệ trực tuyến.
 - Không chia sẻ tên họ, ngày sinh, số điện thoại hoặc mật khẩu tài khoản.
 - Không chia sẻ vị trí, địa chỉ nhà hoặc trường học cho những người không quen biết ngoài đời thực.
 - Không chia sẻ hình ảnh mà bạn không muốn đến tay người khác.
- Sử dụng mật khẩu mạnh và giữ kín:
 - Chọn mật khẩu khó đoán đối với người khác. “12345” hoặc “matkhou” đều không ổn.
 - Đổi mật khẩu thường xuyên (6 tháng một lần).
 - Sử dụng mật khẩu khác nhau cho các tài khoản khác nhau để khi một tài khoản bị tấn công, tội phạm vẫn sẽ không truy cập được vào tất cả các tài khoản.
 - Không viết ra hay cung cấp mật khẩu cho bất cứ ai. Nếu bạn phải viết ra để không quên mất, hãy viết vào sổ tay/ghi chú và cất giữ cẩn thận. Không lưu mật khẩu trong bất kỳ ứng dụng Ghi chú nào trên điện thoại.

- Dùng điện thoại trình chiếu để minh họa cách vào mục **“Cài đặt bảo mật”** trên Instagram.
- Chạm vào hồ sơ của bạn.
 - Chạm vào ba đường kẻ ở góc trên cùng bên phải.
 - Chọn **“Cài đặt”**.
 - Chọn **“Bảo mật”**.
 - Chọn **“Kiểm tra bảo mật”**.

Cho người tham gia biết rằng Facebook cũng có một tùy chọn tương tự là **“Kiểm tra cài đặt bảo mật của bạn”**. TikTok không có tùy chọn **“Kiểm tra”**, nhưng có thể tìm thấy một số tính năng bảo mật trong mục **“Cài đặt và quyền riêng tư”** rồi chọn **“Bảo mật và đăng nhập”** trong hồ sơ.

Các quy trình này sẽ giúp xác nhận rằng có thể dễ dàng đặt lại tài khoản nếu tài khoản đó bị tấn công. Nếu còn thời gian trong buổi đào tạo, hãy để các em hoàn tất quá trình kiểm tra. Nếu chưa xong, khuyến khích các em thực hiện việc này sau buổi đào tạo.



Lời khuyên trong trường hợp bị lừa đảo 5 PHÚT



Tôi đang trò chuyện với ai qua mạng? 20 PHÚT

Nhắc người tham gia đăng xuất nếu các em sử dụng tài khoản của mình trên điện thoại đào tạo. Nhắc các em phải luôn nhớ làm vậy mỗi khi đăng nhập trên thiết bị công cộng.

Lặp lại những lời khuyên này trong video và hỏi xem các em có bất cứ thắc mắc hay điều gì cần làm rõ không.

- Báo cáo trên nền tảng, báo cho công an, ngân hàng hoặc các dịch vụ bảo vệ trẻ em
- Đăng xuất khỏi tất cả các tài khoản (đặc biệt là khi có mật khẩu giống nhau)
- Thay đổi tất cả các mật khẩu.
- Kể với người lớn và nhờ giúp đỡ.

Giải lao 10 phút

1. Cũng như tin tặc và tội phạm lừa đảo, một số người có ý định gây tổn hại nghiêm trọng cho thanh thiếu niên. Những tội phạm này cũng sẽ sử dụng tính năng ẩn danh để che giấu danh tính và có thể đóng giả làm một người hoàn toàn khác để xây dựng lòng tin.
2. Một số tội phạm giả danh bằng cách sử dụng tài khoản mạng xã hội giả để kết bạn với thanh thiếu niên.

PHẦN MỘT:

Bạn là một cô bé 15 tuổi sống trong thành phố. Bạn nhận được yêu cầu theo dõi trên Instagram từ một cậu bé mà bạn không quen. Ba người bạn nữ thân nhất của bạn cũng nhận được yêu cầu từ cậu bạn mới này.

Ảnh chụp của cậu bé trông rất quen nhưng bạn không nhớ là đã từng gặp. Từ hồ sơ, bạn có thể biết cậu bé này cũng là bạn với năm cậu bạn khác trong trường (bạn chung).

3. Đọc to phần đầu của tình huống:
4. **Hỏi người tham gia xem liệu các em có thêm cậu bé dựa vào những thông tin này hay không.**
 - Dựa vào tình huống, khả năng cao là có. Trừ khi người tham gia hạn chế tài khoản của mình rất chặt chẽ.

5. Đọc phần tiếp theo của tình huống:

PHẦN HAI:

Bạn quyết định thêm cậu bé vì:

- Bạn thân của bạn đã thêm
- Cậu bé có 5 bạn chung ở trường bạn
- Bạn tra tên cậu bé trên Google nhưng không tìm thấy thông tin gì

Cậu bé nhắn tin cho bạn và cả hai trò chuyện qua lại trong vài tuần. Cậu bé vừa chuyển đến sống ở thành phố của bạn nhưng lại học khác trường. Bạn để ý thấy cậu bé có kiểu trò chuyện hơi trang trọng và cậu bé không dùng nhiều từ lóng. Không có nhiều ảnh của cậu bé trong hồ sơ.

Cậu bé chia sẻ một bức ảnh cởi trần, hỏi xem bạn nghĩ sao và muốn bạn gửi vài tấm ảnh của bạn. Bạn do dự.

6.  Hỏi người tham gia xem liệu các em có nghĩ cậu bé này là thật hay không và lý do tại sao.

-  Cậu bé có cách diễn đạt rất lạ. Đây không phải là cách nói chuyện của trẻ em.
-  Cậu bé có rất ít ảnh cá nhân trong hồ sơ.
-  Cậu bé nói mình sống trong vùng này nhưng chưa có ai gặp cậu bé ngoài đời cả, điều này rất đáng ngờ.

7.  Hỏi người tham gia xem các em sẽ làm gì để biết được cậu bé có thật hay không.

-  Xem ảnh và thông tin hồ sơ của cậu bé để biết tuổi tác cậu bé.
-  Xem vị trí của cậu bé trên hồ sơ.
-  Hỏi bạn chung để biết thêm thông tin về cậu bé/bạn chung đã gặp mặt trực tiếp hay chưa.

Tìm kiếm cậu bé trên Google, đặc biệt là ảnh hoặc ảnh đại diện.

8. Giải thích cho người tham gia rằng bài học rút ra từ câu chuyện này là chúng ta cần thận trọng khi có người lạ liên hệ với chúng ta trên mạng. Chúng ta không thể phòng tránh mọi rủi ro, nhưng cần suy xét cẩn thận nhất có thể và đừng quá cả tin.



Bàn tay an toàn
5 PHÚT

1. Giải thích rằng chiến lược bảo vệ quan trọng chính là nhờ người lớn đủ tin tưởng giúp đỡ. Nhiều thanh thiếu niên cảm thấy không thoải mái khi làm vậy, điều này có thể khiến vấn đề nhỏ càng trở nên nghiêm trọng hơn.
2. Phát cho mỗi người tham gia một tờ giấy A4 và một cây bút dạ.
3. Yêu cầu từng thanh thiếu niên vẽ viền theo bàn tay lên giấy. Sau đó, yêu cầu người tham gia viết lên trên mỗi ngón tay tên của một người mà các em có thể trao đổi nếu các em lo lắng hay quan tâm về bất kỳ vấn đề nào trên mạng.
4. Khuyến khích người tham gia nghĩ về những người trong và ngoài gia đình mình.
5. Yêu cầu người tham gia viết “Công an” và “Tổng đài bảo vệ” lên vị trí cổ tay, đồng thời cung cấp số đường dây nóng của công an 113] và số tổng đài bảo vệ trẻ em [111.
6. Nói với người tham gia rằng các em có thể giữ lại “bàn tay an toàn” để mang về và không cần phải chia sẻ với nhóm vì đây là thông tin riêng tư.
7. Cho người tham gia biết rằng Internet cũng có thể giúp chúng ta tránh xa những người gây khó chịu bằng cách cho phép chúng ta rời khỏi cuộc trò chuyện, chặn ai đó hoặc báo cáo hành vi không phù hợp.
8. Giải thích rằng tính năng chặn và báo cáo có chút khác biệt và nên được sử dụng theo những cách sau:
 - **CHẶN:** Khi bạn bắt gặp nội dung hoặc tài khoản gây khó chịu hoặc quấy rối, bạn có thể chặn nội dung hoặc tài khoản đó. Sau khi chặn, nội dung hoặc tài khoản đó không còn hiển thị với bạn, nhưng nền tảng sẽ không thực hiện thêm bất kỳ hành động nào đối với nội dung hoặc tài khoản đó.
 - **BÁO CÁO:** Nếu bắt gặp nội dung hoặc tài khoản nguy hiểm hay bất hợp pháp, bạn nên thực hiện hành động nghiêm túc hơn là báo cáo. Nền tảng sẽ điều tra tài khoản hoặc nội dung bạn báo cáo. Nếu có hành vi nào phạm tội thì nền tảng sẽ báo công an.
9. Cho biết rằng bây giờ chúng ta sẽ thực hành chiến lược “Chặn” bằng Facebook, TikTok và Instagram. Chúng ta sẽ thực hành báo cáo vào buổi đào tạo thứ ba.



Chặn trên Facebook, Instagram và TikTok
20 PHÚT

1. Cách xử lý thao tác chặn của các nền tảng rất khác nhau. Ví dụ: Nếu bạn chặn một tài khoản trên Instagram hoặc Messenger, các cuộc trò chuyện sẽ không còn hiển thị với cả hai và các bài đăng riêng tư sẽ bị ẩn (vẫn hiển thị bài đăng công khai). Tuy nhiên, nếu bạn chặn ai đó trên Whatsapp hoặc Line, bạn sẽ không còn nhận được tin nhắn của người đó nữa, nhưng cả hai vẫn sẽ đọc được lịch sử trò chuyện.
2. Lưu ý rằng đôi khi người bị chặn sẽ tạo nhiều tài khoản mới để theo dõi lại bạn. Bạn có thể tiếp tục chặn và họ có thể sẽ dừng lại. Nhưng nếu vấn đề này vẫn tiếp diễn, bạn có thể báo cáo người đó với nền tảng hoặc báo cho công an về hành vi quấy rối này. Các nền tảng có thể cấm thiết bị của một người, không cho sử dụng nền tảng vĩnh viễn.
3.  Dùng điện thoại trình chiếu để minh họa cách chặn tài khoản trên Facebook:
 - Mở ứng dụng Facebook.
 - Nhấp vào hồ sơ của người cần chặn.
 - Nhấp vào ba chấm ở trên cùng trang của các em.
 - Chọn “Chặn”.
 - Xác nhận trên màn hình tiếp theo bằng cách nhấp vào “Chặn” một lần nữa.
4. Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách chặn một tài khoản trên Facebook. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.

Chiến lược bảo vệ
5 PHÚT



 Xem video: [VIDEO 2B – Các tính chất chính của Internet và Chiến lược bảo vệ](#) (Phần đầu video này giống với video 2A nhưng ở cuối sẽ có các chiến lược bảo vệ.)

1. Lắp lại ngắn gọn các chiến lược trong video:
 - **SUY NGHĨ:** Có ổn nếu để nội dung này công khai và tồn tại vĩnh viễn không?
 - **HỎI:** Mọi quan hệ này có tích cực và an toàn không?
 - **PHÂN TÍCH:** Thông tin này có chính xác và đáng tin cậy không? Nghiên cứu và tham khảo chéo nếu cần.
 - **ĐẶT NGHỊ VẤN:** Bạn có đủ quen biết với những người mà bạn đang kết nối không?
 - **TỰ PHÉ BÌNH:** Mình có cư xử trên mạng giống như cách mình cư xử ngoài đời không?

5.  Dùng điện thoại trình chiếu để minh họa cách chặn tài khoản trên Instagram:
 - Mở ứng dụng Instagram.
 - Nhấp vào hồ sơ của người cần chặn.
 - Nhấp vào ba chấm ở trên cùng trang của các em.
 - Chọn “Chặn”.
6. Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách chặn một tài khoản trên Instagram. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.
7.  Dùng điện thoại trình chiếu để minh họa cách chặn tài khoản trên TikTok:
 - Mở ứng dụng TikTok.
 - Nhấp vào hồ sơ của người cần chặn.
 - Nhấp vào ba chấm ở góc trên cùng bên phải màn hình (bên cạnh cái chuông).
 - Chọn “Chặn” trên menu bật lên ở dưới cùng màn hình.
8. Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách chặn một tài khoản trên TikTok. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.



Tóm tắt 5 PHÚT

Đưa ra tóm tắt nhanh về buổi đào tạo:

Mọi thứ chúng ta đăng lên mạng đều có thể gây ảnh hưởng đến suốt đời.

Lên mạng có trách nhiệm là hành xử tôn trọng và suy nghĩ đến những hệ quả xảy ra với người khác và chính bản thân khi chúng ta tương tác.

Không phải lúc nào chúng ta cũng có thể chắc chắn mình đang nói chuyện với trên mạng.

Tội phạm lừa đảo và tin tặc sử dụng nhiều phương thức khác nhau để lấy được quyền truy cập vào tài khoản, tài khoản ngân hàng hoặc các thông tin cá nhân khác.

Tóm lược ngắn gọn một lần nữa các chiến lược bảo vệ trong video:

SUY NGHĨ: Có ổn nếu để nội dung này công khai và tồn tại vĩnh viễn không?

HỎI: Mối quan hệ này có tích cực và an toàn không?

PHÂN TÍCH: Thông tin này có chính xác và đáng tin cậy không? Nghiên cứu và tham khảo chéo nếu cần.

ĐẶT NGHI VẤN: Bạn có đủ quen biết với những người mà bạn đang kết nối không?

TỰ PHÊ BÌNH: Mình có cư xử trên mạng giống như cách mình cư xử ngoài đời không?

CHIA SẺ: Trao đổi với người lớn đủ tin tưởng.

Buổi 3: Ngăn chặn và ứng phó với các vấn đề nghiêm trọng trên mạng

Mục tiêu học tập

- o Người tham gia nắm được khái niệm chặn dắt và xâm hại tình dục trẻ em trên mạng.
- o Người tham gia hiểu về hành vi bắt nạt qua mạng.
- o Người tham gia có thể nhận biết một số dấu hiệu cảnh báo sớm về các rủi ro nghiêm trọng trên mạng.
- o Người tham gia biết những biện pháp thiết thực để tìm kiếm sự giúp đỡ khi gặp các rủi ro nghiêm trọng trên mạng.

Buổi đào tạo này cần có

- o Sổ tay hướng dẫn đào tạo
- o Điện thoại đào tạo và điện thoại trình chiếu
- o Máy chiếu
- o Loa
- o Máy tính xách tay.
- o Áp phích Các yếu tố quan trọng
- o Bảng trắng hoặc tập giấy lật
- o Bút dạ
- o Giấy dán ghi chú
- o Hướng dẫn sử dụng các tính năng đảm bảo an toàn trên nền tảng (có sẵn để chuyên viên đào tạo tham khảo)
- o Liên kết tới: Khảo sát sau đào tạo
- o Liên kết tới: [VIDEO 4 – Dụ dỗ, Chặn dắt, Xâm hại tình dục trên mạng và Bắt nạt qua mạng](#)
- o Quét mã QR để tham gia khảo sát sau tập huấn (màu tím)

Chuẩn bị

- o Sắp xếp 20 ghế theo hình bán nguyệt.
- o Treo áp phích Các yếu tố quan trọng lên.
- o Bật tất cả điện thoại đào tạo lên và đảm bảo điện thoại đã được sạc pin, cập nhật và có sẵn dữ liệu.
- o Kết nối máy chiếu và loa, đảm bảo mọi thiết bị đều hoạt động.
- o Kết nối điện thoại trình chiếu với máy chiếu và đảm bảo điện thoại hoạt động tốt.
- o Kiểm tra để đảm bảo liên kết video vẫn hoạt động hoặc sử dụng USB để mở video.
- o Đảm bảo việc các em nắm được thông tin chi tiết các tài khoản giả của nền tảng.



Giới thiệu 2 PHÚT

Chào mừng người tham gia đến với buổi đào tạo thứ ba, cũng là buổi đào tạo cuối cùng.

Giải thích rằng trong buổi đào tạo này, chúng ta sẽ thảo luận về các chủ đề nhạy cảm, bao gồm cả xâm hại tình dục trẻ em.

Yêu cầu người tham gia tự lo cho bản thân và thông báo cho điều phối viên biết nếu có bất cứ điều gì khiến các em thấy buồn hoặc khó chịu hay các em muốn xin ra khỏi buổi đào tạo một lúc. Cho các em biết rằng các em có thể trao đổi với bạn sau buổi đào tạo nếu muốn.

Phát điện thoại đào tạo và ghi lại số được chỉ định. Nhắc các em đặt điện thoại xuống dưới ghế ngồi trong khoảng thời gian giữa các hoạt động.



Trò chơi nháy mắt 5 PHÚT

- Giải thích rằng trong trò chơi này, người tham gia cần phải thu hút sự chú ý của bạn khác trong vòng tròn mà không di chuyển hay tạo ra tiếng động. Các em chỉ có thể dùng giao tiếp bằng mắt.
- Hãy nháy mắt với một bạn và chờ bạn đó nháy mắt lại.
- Sau khi bạn đó nháy mắt lại, hai em có thể đứng lên và đổi chỗ cho nhau.
- Sau khi ngồi về chỗ, hãy thu hút sự chú ý của bạn khác và tiếp tục trò chơi. Không được đổi chỗ nhiều lần với cùng một người.
- Nhắc người tham gia rằng mục đích của trò chơi là đổi chỗ với càng nhiều người càng tốt và các em cần nhớ để ý xem ai đang nháy mắt với mình.
- Chơi trò chơi trong 3 phút.
- Yêu cầu các em giơ tay nếu đã đổi chỗ 3 lần, 4 lần, 5 lần, v.v.
- Giải thích rằng thông điệp chính của trò chơi này là nhận được sự đồng ý của người khác trước khi thực hiện hành động (đổi chỗ). Trong trò chơi này, bạn không thể đổi chỗ nếu không nhận được sự đồng ý.
- Khi lên mạng, chúng ta phải luôn nhớ rằng chỉ hành động khi có sự đồng thuận. Điều này tác động theo cả hai chiều. Người tham gia phải nhớ rằng người khác có quyền đồng ý hoặc không. Đổi lại, các em cũng vậy. Các em không nên chấp nhận sự ép buộc qua mạng. Nếu cảm thấy không thoải mái, hãy tin vào cảm giác đó và tránh khỏi tình huống đó.



Nội dung mang tính công kích trên mạng 5 PHÚT

Nhắc nhở người tham gia về các yếu tố “**Công khai**”, “**Kết nối**” và “**Ẩn danh**”. Các yếu tố này giúp chúng ta hiểu rõ lý do tại sao thế giới ảo lại có nhiều nội dung mang tính công kích mà thanh thiếu niên có thể gặp phải.

Bất cứ ai trên thế giới cũng đều có thể tải lên nội dung. Trong đó có cả những người có ý đồ xấu. Trên Internet thường có những nội dung thô lỗ, bạo lực hoặc đáng sợ, không an toàn để thanh thiếu niên xem.

- Yêu cầu người tham gia nghĩ ra ví dụ về những nội dung thô lỗ, bạo lực hoặc đáng sợ trên Internet. Đưa ra các ví dụ chưa được nêu:**
- Cảnh bạo lực (cả ngoài đời thực hay trên trò chơi điện tử).
 - Cảnh ăn cắp tiền hoặc làm việc bất hợp pháp.
 - Hình ảnh, video khiêu dâm.
 - Cảnh trẻ em hoặc thanh thiếu niên chịu tổn thương.
 - Cảnh tra tấn bạo lực cả động vật.
 - Hoạt động khủng bố.



Tìm kiếm an toàn 10 PHÚT

- Có thể sử dụng Google để chặn không cho nội dung không phù hợp như cảnh bạo lực hoặc khiêu dâm xuất hiện khi tìm kiếm.
- Dùng điện thoại trình chiếu để chỉ cách ẩn kết quả phản cảm bằng Google.
 - Mở Google trong trình duyệt Chrome.
 - Trước tiên, hãy tìm kiếm một nội dung nào đó.
 - Chạm vào biểu tượng bánh răng ở phía trên cùng màn hình Google (để hiển thị menu cài đặt).
 - Chọn tùy chọn “Ẩn kết quả phản cảm”.
 - Nhấn nút đảo chiều sang trạng thái “bật”.
- Yêu cầu người tham gia thao tác trên điện thoại đào tạo..



Báo cáo trên Face- book, Instagram và TikTok 15 PHÚT

- Như đã thảo luận trong buổi đào tạo trước, tính năng chặn và báo cáo có khác biệt và nên được sử dụng theo những cách sau:

CHẶN: Khi bạn bắt gặp nội dung hoặc tài khoản gây khó chịu hoặc quấy rối, bạn có thể chặn nội dung hoặc tài khoản đó. Sau khi chặn, nội dung hoặc tài khoản đó không còn hiển thị với bạn, nhưng nền tảng sẽ không thực hiện thêm bất kỳ hành động nào đối với nội dung hoặc tài khoản đó.

BÁO CÁO: Nếu bắt gặp nội dung hoặc tài khoản nguy hiểm hay bất hợp pháp, bạn nên thực hiện hành động nghiêm túc hơn là báo cáo.
- Dùng điện thoại trình chiếu để minh họa cách “báo cáo” tài khoản trên Face book:
 - Mở ứng dụng Facebook.
 - Nhấp vào hồ sơ của người cần chặn.
 - Nhấp vào ba chấm ở trên cùng trang của các em.
 - Chọn “Báo cáo”.
 - Xác nhận trên màn hình tiếp theo bằng cách nhấp vào “Báo cáo” một lần nữa và cung cấp thông tin theo yêu cầu.
- Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách báo cáo một tài khoản trên Facebook. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.
- Dùng điện thoại trình chiếu để minh họa cách báo cáo tài khoản trên Insta gram:
 - Mở ứng dụng Instagram.
 - Nhấp vào hồ sơ của người cần báo cáo.
 - Nhấp vào ba chấm ở trên cùng trang của các em.
 - Chọn “Báo cáo”.
 - Trong menu, chọn một lý do báo cáo (*Tuy nhiên, không chạm vào một mục trong danh sách, nếu không báo cáo sẽ được hoàn tất ngay lập tức*)

- Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách báo cáo một tài khoản trên Instagram. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.
-  Dùng điện thoại trình chiếu để minh họa cách báo cáo trên TikTok:
 - Mở ứng dụng TikTok.
 - Nhấp vào hồ sơ của người cần báo cáo.
 - Nhấp vào nút “báo cáo” ở dưới cùng màn hình.
 - Chọn “báo cáo tài khoản”.
 - Chọn một lý do trong danh sách.
 - Nhấp vào gửi trên màn hình tiếp theo.
- Yêu cầu người tham gia dùng điện thoại để đăng nhập và tìm cách báo cáo một tài khoản trên TikTok. Đi xung quanh và giúp các em xác định vị trí các tùy chọn.
- Cuối cùng, nhắc người tham gia **lắng nghe trực giác của mình**. Nếu các em thấy nội dung trên mạng thô lỗ, đáng sợ hoặc bạo lực hay có điều gì gây khó chịu cho các em, các em có thể hành động.

Giải lao 10 phút



Chặn dắt và xâm hại tình dục trẻ em trên mạng 25 PHÚT

Giải thích cho người tham gia rằng các nền tảng như Facebook, Instagram và TikTok đều là các phương thức giao tiếp tuyệt vời. Tuy nhiên, sẽ có rủi ro khi chúng ta có thể chia sẻ quá nhiều thông tin về bản thân với người khác ở trên mạng. Lưu ý cho người tham gia rằng điều này liên quan đến yếu tố **“Kết nối”**. Nhắc lại cho các em rằng yếu tố **“Ẩn danh”** nghĩa là mọi người có thể che giấu danh tính của chính mình, đặc biệt là khi họ có ý định gây hại.

Giải thích cho người tham gia rằng một khi bạn đã chia sẻ ảnh, video hoặc tin nhắn, kể cả là tự nguyện và riêng tư (còn gọi là “nhắn tin gợi dục”), bạn sẽ không thể kiểm soát các nội dung đó được gửi đi đâu. Người khác có thể chụp màn hình hoặc chỉ đơn giản là chia sẻ mà không xin phép bạn. Lưu ý cho người tham gia rằng điều này liên quan đến yếu tố **“Vĩnh viễn”**.

Nhắc nhở người tham gia luôn cẩn trọng với những nội dung các em thảo luận trong buổi đào tạo này. Các em không được làm lộ danh tính của người khác trong khi chia sẻ ví dụ. Lưu ý cho người tham gia rằng các em có thể xin ra khỏi lớp một lúc nếu không muốn nghe những câu chuyện như vậy.

Giải thích bóc lột và xâm hại tình dục trẻ em là:

“Quá trình trong đó người lớn (hoặc bạn đồng trang lứa) lợi dụng vị thế của mình để thực hiện các hoạt động tình dục với trẻ em.”

Xâm hại tình dục trẻ em trên mạng là khi quá trình đó có liên quan đến công nghệ kỹ thuật số, Internet và công nghệ truyền thông tại một thời điểm nào đó.

Cho biết rằng có các hình thức xâm hại và bóc lột tình dục trẻ em trên mạng khác nhau. Thường bao gồm:

Chặn dắt: Xây dựng mối quan hệ với nạn nhân nhằm mục đích bóc lột tình dục hoặc chụp ảnh hay ghi hình video khiêu dâm.

Nội dung xâm hại tình dục trẻ em: Sản xuất, chia sẻ hoặc xem ảnh hay video xâm hại tình dục trẻ em hoặc bộ phận sinh dục của trẻ em.

Tống tiền dưới sự đe dọa chia sẻ hình ảnh: Lấy hình ảnh hoặc video khiêu dâm của nạn nhân, thường bằng cách lừa gạt mà có hoặc đe dọa chia sẻ hình ảnh đã có với công chúng hoặc gia đình và bạn bè của nạn nhân nếu nạn nhân không gửi tiền hoặc gửi thêm ảnh. Lời đe dọa có thể là thật hoặc giả.

Phát trực tiếp hành vi xâm hại tình dục trẻ em: Khi hành vi xâm hại tình dục trẻ em được tiến hành và chiếu qua các công cụ video trên các nền tảng trò chuyện hoặc nền tảng khác trong thời gian thực.

 Xem phần đầu của video: [VIDEO 4 – Dụ dỗ, Chặn dắt, Xâm hại tình dục trên mạng và Bắt nạt qua mạng \(tạm dừng lúc 3:40\)](#)

 **Hỏi người tham gia xem các em thấy chuyện gì đang xảy ra trong video.**

-  Trước tiên, cậu bé đã bị Seagull chặn dắt trên kênh Twitch công khai rồi chuyển sang nhắn tin riêng tư.
-  Cậu bé chia sẻ một hình ảnh. Sau đó, Seagull thúc giục cậu bé chia sẻ thêm, còn nhắc rằng hẳn ta đã tặng quà để gây áp lực cho cậu bé – đây là một hình thức tống tiền dưới sự đe dọa chia sẻ hình ảnh.

 Tiếp tục video: [VIDEO 4 – Dụ dỗ, Chặn dắt, Xâm hại tình dục trên mạng và Bắt nạt qua mạng \(phát từ lúc 3:40 đến 7:38\)](#)

Nhắc lại cho người tham gia rằng chặn dắt tình dục là:

“Xây dựng mối quan hệ với nạn nhân nhằm mục đích bóc lột tình dục hoặc chụp ảnh hay ghi hình video khiêu dâm.”

Hành vi chặn dắt có thể bao gồm giao tiếp và/hoặc cố gắng kết bạn hoặc xây dựng một mối quan hệ hay kết nối tình cảm với ai đó.

Thanh thiếu niên thường bị “chặn dắt” trước khi bị xâm hại tình dục. Ban đầu, các em có thể bị lừa rằng mình đang ở trong một mối quan hệ an toàn và bình thường nên không biết hoặc có thể cảm thấy buộc phải làm theo yêu cầu.

 **Hỏi xem Seagull đã làm gì để lừa gạt cậu bé đang vừa phát trực tiếp vừa chơi game:**

-  Trước tiên, hẳn ta giả dạng là một cậu bé.
-  Hẳn ta nói rằng mình cũng thực hiện các hoạt động tương tự như cậu bé.
-  Hẳn ta đã tặng quà cho cậu bé để cậu bé cảm thấy phải “đền đáp”.

Giải thích rõ rằng việc bị chặn dắt và xâm hại trên mạng không bao giờ là lỗi của đứa trẻ bị xâm hại. Trẻ em không phải chịu trách nhiệm và không cần phải thấy xấu hổ.

Tội phạm mới là những kẻ đáng lên án. Thanh thiếu niên không làm bất cứ điều gì dẫn đến vụ việc.



Dấu hiệu cảnh báo hành vi xâm hại tình dục trẻ em trên mạng 10 PHÚT

Như đã xem trong video, hành vi chặn dắt có thể bắt đầu công khai với các mối quan hệ được thiết lập qua tài khoản mạng xã hội và trò chơi.

Sau đó, tội phạm thường sẽ cố gắng chuyển sang nhắn tin riêng tư. Chúng thường sẽ kết nối trên nhiều nền tảng cùng lúc để gây áp lực.

Tội phạm sử dụng cùng nền tảng, trò chơi và ứng dụng mà thanh thiếu niên thường dùng. Thông thường, chúng biết rất rõ cách sử dụng những nền tảng này.

Tội phạm rất thành thạo trong việc mình làm và có thể kết bạn với thanh thiếu niên bằng cách tỏ ra có cùng sở thích và mối quan tâm như các em.

Giống như Seagull, tội phạm thường sử dụng tài khoản giả và chia sẻ hình ảnh giả để trông có vẻ bằng tuổi với nạn nhân.

Thanh thiếu niên có thể cảm thấy phấn khích hoặc hãnh diện khi được quan tâm từ tế. Đặc biệt là khi tội phạm tặng quà cáp, tiền bạc, đưa ra lời khuyên hay thể hiện sự ủng hộ. Thông thường, tội phạm trông có vẻ như thực sự hiểu hoặc quan tâm đến nạn nhân.

Sau khi bắt đầu chiếm được lòng tin, tội phạm có thể yêu cầu nạn nhân cung cấp thêm thông tin cá nhân hoặc bí mật chia sẻ nội dung.

Hãy lắng nghe trực giác của mình. Nếu có người trên mạng bắt đầu tạo cảm giác khó chịu, suy xét kỹ trước khi tiếp tục tương tác với người đó. Bạn có thể trao đổi với bạn bè hoặc người lớn đủ tin tưởng về những điểm khác lạ để xin lời khuyên. Hãy nhớ rằng trong video, cậu bé có vẻ không thoải mái nhưng vẫn làm theo yêu cầu của Seagull.

Cũng như Seagull, tội phạm dùng thông tin đã thu thập được để thao túng, lừa gạt, hù dọa và kiểm soát. Tội phạm cũng sẽ cố gắng cô lập nạn nhân với bạn bè và gia đình để nạn nhân không xin trợ giúp và lời khuyên từ bất cứ ai.

1. **Yêu cầu người tham gia thảo luận tập thể về những biện pháp có thể thực hiện để phòng tránh tội phạm lợi dụng mình. Yêu cầu người tham gia liệt kê một số việc nên làm và không nên làm. Đảm bảo bao hàm các ý sau và đề cập đến nếu chưa được nêu:**

Việc bạn có thể làm:

- ☐ Đặt cài đặt quyền riêng tư thành “chỉ bạn bè” hoặc “riêng tư” cho các bài đăng để không hiển thị công khai.
- ☐ Dừng lại và suy nghĩ trước khi chia sẻ bất kỳ thông tin cá nhân nào.
- ☐ Nghiên cứu hoặc tham khảo chéo các thông tin về bạn bè mới bằng cách tìm kiếm hoặc kiểm tra bạn chung của họ.
- ☐ Bạn có thể sử dụng họ giả trên tài khoản thay vì họ thật.
- ☐ Tôn trọng quyền riêng tư của người khác. Luôn xin phép người khác trước khi đăng ảnh, gắn thẻ họ hoặc chia sẻ thông tin của họ.



Bí kíp phòng tránh tội phạm trên mạng 10 PHÚT

Việc bạn nên tránh:

- ☐ Không sử dụng tên đầy đủ.
 - ☐ Không đăng số điện thoại lên mạng một cách công khai.
 - ☐ Không đăng email lên mạng một cách công khai.
 - ☐ Không thêm ngày sinh vào hồ sơ công khai.
 - ☐ Không sử dụng tính năng “check in” hoặc gắn thẻ vị trí vào ảnh.
 - ☐ Đảm bảo ảnh không có các vị trí hoặc thông tin dễ nhận biết (ví dụ: tên trường học trên đồng phục).
 - ☐ Không sử dụng tên hoặc ngày/năm sinh trong tên người dùng.
 - ☐ Không chia sẻ địa chỉ nhà.
 - ☐ Không chia sẻ cho bất kỳ ai, kể cả người quen ngoài đời thực, những hình ảnh hay video cá nhân hoặc nhạy cảm.
2. Nhắc người tham gia rằng nếu nghi ngờ ai đó là tội phạm, các em nên xin lời khuyên từ một người lớn đáng tin cậy.

CHIA SẺ: Tìm đến người lớn đáng tin cậy để xin trợ giúp hoặc xin lời khuyên. Tham khảo bàn tay an toàn.

THU THẬP: Lưu và chụp màn hình các tin nhắn cũng như thông tin của người khiến bạn cảm thấy không thoải mái.

BÁO CÁO: Thông báo trực tiếp cho nền tảng hoặc công an về những vấn đề nghiêm trọng.



Bắt nạt qua mạng 15 PHÚT



Tiếp tục video: [VIDEO 4 – Dụ dỗ, Chặn dắt, Xâm hại tình dục trên mạng và Bắt nạt qua mạng \(phát từ lúc 7:38 đến hết\)](#)

Nhắc lại cho người tham gia rằng chúng ta đã thảo luận về định nghĩa của hành vi bắt nạt qua mạng trong buổi đào tạo đầu tiên. Hỏi xem có ai còn nhớ định nghĩa và lặp lại các ý dưới đây.

- ☐ Đây là hành vi lặp đi lặp lại, nhằm mục đích hù dọa, chọc giận hoặc nhạo báng người bị nhắm đến.
- Yêu cầu nhóm tham gia chia sẻ một số ví dụ về hành vi bắt nạt qua mạng.**
- ☐ Mọi người lan truyền những lời nói dối hoặc đăng các bức ảnh đáng xấu hổ của người khác lên mạng xã hội.
 - ☐ Mọi người gửi những tin nhắn gây tổn thương hoặc lời đe dọa qua các nền tảng nhắn tin như Facebook Messenger, Whatsapp hoặc Instagram, v.v.
 - ☐ Mọi người sử dụng tên của người khác để lập tài khoản giả mạo và chế nhạo họ.
 - ☐ Mọi người cố tình loại trừ ai đó khỏi một nhóm trên mạng.

Tóm lược lại rằng bắt nạt qua mạng là những hành vi không tử tế thường lặp đi lặp lại. Hành vi này có sử dụng công nghệ và thường diễn ra trên nền tảng mạng xã hội, nền tảng trò chuyện và trò chơi.

Giải thích rằng hành vi bắt nạt qua mạng thường do những người quen biết (chẳng hạn như bạn bè hoặc bạn cùng trường) thực hiện.

Đôi khi, mọi người có thể dễ “vào hùa” để bắt nạt nạn nhân. Càng nhiều người tham gia thì càng thoải mái. Bởi vì họ cảm thấy như mình sẽ không phải chịu hậu quả gì.

Giải thích rằng bắt nạt qua mạng khác với các hình thức bắt nạt khác ngoài đời, vì có rất nhiều người có thể chứng kiến hoặc tham gia vào vụ việc. Ví dụ: Khi có người đăng tin nhắn thô tục lên trang Facebook của bạn, tất cả bạn bè của bạn đều có thể xem nội dung đó.

Bắt nạt trực tiếp thường có thể xảy ra cùng lúc với bắt nạt qua mạng. Tuy nhiên, hành vi bắt nạt qua mạng sẽ được lưu hồ sơ vĩnh viễn trên nền tảng kỹ thuật số. Hồ sơ này có thể là bằng chứng giúp chấm dứt vụ việc. Người tham gia nên nhớ rằng hành vi bắt nạt trên mạng sẽ được lưu trữ lại và có thể ảnh hưởng xấu đến thanh danh của mình.

1. Chia người tham gia thành 2 nhóm.
2. Phân cho một nhóm tình huống đầu tiên và nhóm còn lại tình huống thứ hai được nêu bên dưới:
Tình huống A: Một nhóm bạn có phát ngôn ác ý với thanh thiếu niên khác trên hồ sơ Facebook của người đó
Tình huống B: Một nhóm thanh thiếu niên đăng ảnh cắt ghép/đã qua chỉnh sửa về thanh thiếu niên khác và chế nhạo người đó trong nhóm trò chuyện riêng tư
3. Giải thích rằng người tham gia cần đóng một vở kịch dài 2 phút để thể hiện tình huống và những điều các em sẽ làm để giải quyết vấn đề bắt nạt qua mạng.
4. Cho người tham gia thời gian 10 phút để dựng vở kịch.
5. Yêu cầu mỗi nhóm trình bày lại vai diễn của mình và dành thời gian nghe phản hồi (mỗi nhóm 10 phút).
6. Sau vở kịch diễn ra, yêu cầu người xem diễn giải những gì mình thấy và mô tả sự thay đổi cần thiết để giải quyết vấn đề bắt nạt qua mạng.

Lưu ý cho người tham gia rằng biện pháp ứng phó với những lo ngại thực sự nghiêm trọng này rất đơn giản. Mặc dù chúng ta đã thảo luận về những việc có thể làm để phòng tránh rủi ro, các em vẫn phải tìm kiếm sự giúp đỡ khi xảy ra vấn đề:

CHIA SẺ: Tìm đến người lớn đáng tin cậy để xin trợ giúp hoặc xin lời khuyên. Tham khảo bàn tay an toàn.

LƯU TRỮ: Lưu và chụp màn hình các tin nhắn cũng như thông tin của người khiến bạn cảm thấy không thoải mái.

CHẶN: Dừng ngăn ngại mà hãy chặn những người hoặc tài khoản khiến bạn cảm thấy không thoải mái.



Tóm tắt và khảo sát sau đào tạo 5 PHÚT

Đưa ra tóm tắt ngắn gọn về buổi đào tạo:

Nhắc người tham gia ghi nhớ sáu yếu tố để hành xử trên mạng cho đúng mực.

Trong buổi đào tạo này, các em đã tìm hiểu các cách phát hiện rủi ro và một số biện pháp tránh bị tổn hại (như tìm kiếm an toàn).

Các em có thể dễ dàng báo cáo những người gây khó chịu trên hầu hết các nền tảng.

Một số cá nhân sử dụng Internet để gây tổn hại nghiêm trọng cho thanh thiếu niên thông qua hành vi xâm hại trẻ em trên mạng. Yếu tố “Ẩn danh” và Yếu tố “Công khai” sẽ giúp chúng ta ghi nhớ điều này.

Bắt nạt qua mạng là một vấn đề nghiêm trọng mà rất nhiều thanh thiếu niên gặp phải. Yếu tố “**Tôn trọng**” có thể giúp định hướng hành động của chúng ta.

Ngoài ra, nhắc nhở rằng người tham gia có thể trao đổi với người có tên trên bàn tay an toàn nếu các em bị bắt nạt qua mạng hoặc lo lắng mình bị chặn dắt, xâm hại hoặc bóc lột.

Nhiệm vụ cuối cùng là yêu cầu người tham gia hoàn thành khảo sát ngắn sau đào tạo. Giải thích rằng cũng giống như khảo sát đã làm lúc mới bắt đầu, đây là bài khảo sát trắc nghiệm và chỉ mất 5 phút.

Đề nghị học viên quét mã QR tím để hoàn thành Khảo sát cuối kỳ.

Gửi lời cảm ơn đến tất cả những người tham gia và chúc mừng các em hoàn thành khóa đào tạo Swipe Safe – An toàn trên mạng.



Đóng kịch 30 PHÚT



Ứng phó với tình trạng bắt nạt qua mạng và xâm hại 10 PHÚT

