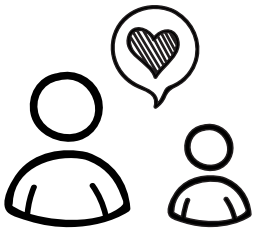
Cảnh Báo:

Dừng lại.
Suy nghĩ.
Kết nối.

VIETNAMESE

NHẤP CHUỘT



Để giúp các trẻ em trong cuộc sống của bạn được an toàn trực tuyến, *Cảnh Báo: Dừng lại. Suy nghĩ. Kết nối.* có một số ý tưởng để giúp bạn bắt đầu cuộc trò chuyện với trẻ. Chọn một phần và cùng đọc với trẻ để biết cách chia sẻ một cách thận trọng, cư xử tử tế trên mạng, chống lại hành vi bắt nạt trên mạng và bảo vệ thông tin cá nhân của trẻ (và của bạn) trực tuyến. Những công cụ này có thể giúp bạn chỉ dẫn cho trẻ cách đưa ra những lựa chọn đúng đắn và sử dụng công nghệ một cách có trách nhiệm. Và bằng cách nói chuyện với trẻ, bạn cho trẻ biết rằng chúng có một người lớn đáng tin cậy để giúp đỡ khi mắc lỗi.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Tham gia trực tuyến là một phần cuộc sống của bạn. Bạn xem thông tin và tạo nội dung, đăng ảnh và video, chơi trò chơi cũng như chia sẻ vị trí và việc mình đang làm với bạn bè và gia đình. Nhưng có những rủi ro khi bạn đăng bài, chơi trò chơi và kết nối trực tuyến. Một số người và tình huống bạn gặp phải không phải lúc nào cũng như những gì bạn thấy.

Bất kể các ngón tay của bạn lướt trên bàn phím, điện thoại hay máy tính bảng nhanh đến mức nào, công cụ tốt nhất bạn có để tránh rủi ro trực tuyến chính là bộ não và thời gian của bạn. Hãy dừng lại và suy nghĩ kỹ các tình huống để giúp bảo vệ bản thân, bạn bè và gia đình, tài khoản và thiết bị của bạn. Nếu không thì kết quả là bạn có thể chia sẻ thông tin quá mức, khiến bản thân hoặc người khác xấu hổ, làm hỏng máy tính của mình hoặc trò chuyện với những người không phải là người như họ nói.

- CHIA SẺ MỘT CÁCH THẬN TRỌNG
- HÃY CƯ XỬ TỬ TẾ
- CHỐNG LẠI HÀNH VI BẮT NẠT TRÊN MẠNG
- KẾT NỐI ĐƯỢC BẢO VỆ

CHIA SẺ MỘT CÁCH THẬN TRỌNG

Suy nghĩ trước khi bạn chia sẻ

Những gì bạn làm trên mạng đều có các hậu quả trong thế giới thực. Ảnh, video và tin nhắn bạn chia sẻ sẽ ảnh hưởng đến bạn, quyền riêng tư, danh tiếng của bạn và của những người xung quanh bạn — hiện tại và trong tương lai. Hãy dừng lại và suy nghĩ trước khi bạn đăng bài.

Những gì bạn đăng có thể có lượng "khán giả" nhiều hơn bạn nghĩ.

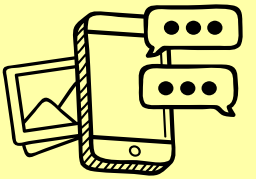
Không thể kiểm soát được hoàn toàn những ai xem hồ sơ, hình ảnh, video hoặc văn bản của bạn — ngay cả khi bạn sử dụng cài đặt quyền riêng tư hoặc ứng dụng xóa nội dung sau khi đã xem hay trong vòng 24 giờ. Bất kỳ ai nhìn thấy bài đăng của bạn đều có thể chụp ảnh màn hình hoặc ghi lại. Hãy tự hỏi bản thân: "Liệu tôi có muốn ai đó đứng dậy vào giữa giờ ăn trưa và chia sẻ bức ảnh hoặc video đó với toàn bộ căng tin không?"

Những gì bạn chia sẻ có thể ảnh hưởng đến người khác. Việc gửi hoặc đăng ảnh và video mà không được sự cho phép của những người trong đó có thể gây xấu hổ, bất công và thậm chí là không an toàn. Hãy xin sự đồng ý của mọi người trước. Trước khi đăng bài, hãy hỏi họ: "Bạn có đồng ý cho tôi đăng nội dung này lên mạng xã hội không?" Nếu họ trả lời là không thì đừng đăng.

Một khi đã đăng nội dung nào đó lên mạng, bạn không thể lấy lại được

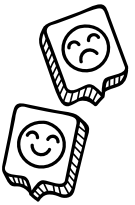
Ngay cả khi bạn xóa nội dung nào đó mình đã đăng — hoặc bài đăng hết hạn — thì ảnh hoặc nhận xét mà bạn không muốn mọi người xem nữa có thể được lưu lại, chia sẻ và tồn tại ở đâu đó trực tuyến — vĩnh viễn.

Nhắn tin tình dục: Đừng làm vậy



Bạn có thể đã nghe được những câu chuyện ở trường học hoặc trên tin tức về việc mọi người "nhắn tin tình dục" - gửi ảnh khỏa thân từ điện thoại của họ. Đừng làm vậy. Chấm hết. Việc tạo ra, chuyển tiếp hoặc thậm chí lưu ảnh, video hoặc tin nhắn khiêu dâm sẽ khiến tình bạn và danh tiếng của bạn gặp rủi ro. Tệ hơn là bạn có thể đang vi phạm pháp luật.

Một lưu ý về mạng xã hội



Theo Người cầm đầu Quân y Hoa Kỳ, việc sử dụng mạng xã hội có thể gây tổn hại cho bạn, tùy thuộc vào lượng thời gian bạn sử dụng các nền tảng, loại nội dung bạn xem và mức độ gây gián đoạn của nó đối với những thứ như giấc ngủ hoặc việc tập thể dục của bạn — những hoạt động cần thiết cho sức khỏe của bạn.

HÃY CƯ XỬ TỬ TẾ

Lịch sự là điều quan trọng

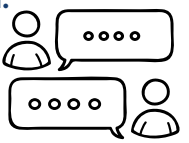
Khi bạn không thể nhìn thấy nét mặt, ngôn ngữ cơ thể hoặc các tín hiệu hình ảnh khác của ai đó trực tuyến, bạn có thể thấy thoải mái khi đăng hoặc nói những điều mà bạn sẽ không nói trực tiếp. Nhưng việc gửi tin nhắn, đăng bài, nhắn tin trực tiếp, chơi trò chơi điện tử và gửi email cũng giống như nói chuyện trực tiếp với ai đó. Hãy lưu tâm đến cách bạn giao tiếp và suy nghĩ trước khi nói hoặc đăng bài.

Chậm lại một chút. Rất dễ để xảy ra hiểu lầm trên mạng. Trước khi gửi tin nhắn, hãy tự hỏi: "Tin nhắn này sẽ khiến người khác cảm thấy thế nào?"

Luôn cân nhắc và tôn trọng quan điểm cũng như cảm xúc của người khác trên mạng — giống như điều bạn sẽ làm khi gặp trực tiếp. Hãy nhớ rằng: đằng sau ảnh đại diện và tên hồ sơ là những con người thật.

Giảm bớt giọng điệu. Đừng sử dụng toàn bộ chữ VIẾT HOA, hàng dấu chấm than dài hoặc phông chữ đậm và lớn. Điều này giống như là việc la hét.

Đừng đưa mọi thứ vào cuộc trò chuyện nhóm. Trước khi bạn gửi tin nhắn nhóm hoặc nhấn nút Reply All (Trả lời tất cả), hãy dừng lại và suy nghĩ: Ai cần xem tin nhắn này?



Đừng mạo danh

Việc tạo hồ sơ, nhận xét hoặc bài đăng mà dường như đến từ người khác, chẳng hạn như ai đó trong lớp hoặc giáo viên của bạn, là sai trái và có thể gây tổn hại.

Hãy lên tiếng

Nếu bạn thấy một người bạn đăng điều gì đó thiếu suy nghĩ hoặc không an toàn, hãy nói với họ. Bạn có thể giúp bạn bè của mình tránh khỏi rắc rối và tình huống đáng xấu hổ. Nếu bạn thấy điều gì đó không phù hợp trên mạng thì hãy báo cáo và nói với một người lớn đáng tin cậy. Hầu hết các ứng dụng và nền tảng đều có cách để báo cáo nếu hành vi của ai đó mang tính đe dọa hoặc không phù hợp.

CHỐNG LẠI HÀNH VI BẮT NẠT TRÊN MẠNG

Mọi người đều xứng đáng được cảm thấy an toàn trong các tương tác hàng ngày với người khác, cho dù là trên mạng hay trực tiếp.

Nếu ai đó đăng những bình luận ác ý, meme gây tổn thương, hình ảnh đáng xấu hổ hoặc gửi cuộc trò chuyện hay tin nhắn riêng tư về bạn thì đó là hành vi bắt nạt. Điều này là không chấp nhận được. Hãy trao đổi với một người lớn đáng tin cậy để được giúp đỡ về tình huống này và quyết định cách bạn nên phản ứng.

Nếu ai đó quấy rối bạn trên mạng thì dưới đây là những việc cần làm:

- **Phớt lờ** người đó hoặc chặn không cho họ liên lạc thêm với bạn.
- **Lưu lại bằng chứng** và yêu cầu sự giúp đỡ từ một người lớn đáng tin cậy.
- **Báo cáo việc này.** Nhiều ứng dụng và nền tảng có các công cụ để báo cáo nếu ai đó có hành vi đe dọa hoặc không phù hợp.

Việc bắt nạt thường khiến người bị quấy rối cảm thấy tồi tệ — và điều đó khiến kẻ bắt nạt có hình ảnh tồi tệ.

Hành vi bắt nạt cũng có thể khiến bạn gặp rắc rối với trường học hoặc cảnh sát.

Nếu bạn chứng kiến hành vi bắt nạt trên mạng thì hãy tìm cách trở thành người đứng lên bảo vệ - người mà can thiệp, chặn lại hoặc lên tiếng để ngăn chặn hành vi bắt nạt. Hành vi xấu thường chấm dứt khá nhanh khi ai đó đứng lên bảo vệ người bị bắt nạt.

KẾT NỐI ĐƯỢC BẢO VỆ

Bảo vệ quyền riêng tư của bạn

Khi bạn làm bất cứ điều gì trực tuyến, bạn đều để lại dấu vết. Hãy thực hiện các bước sau để đảm bảo rằng dấu vết đó không trở thành đường dẫn đến thông tin mà bạn không có ý định chia sẻ.

Sử dụng cài đặt quyền riêng tư. Tìm hiểu cách bật cài đặt quyền riêng tư cho thiết bị, ứng dụng và tài khoản mạng xã hội — sau đó thực hiện việc này. Điều này giúp bạn giới hạn những người có thể xem địa điểm của bạn, thông tin bạn đăng và những người có thể kết nối với bạn.

Kiểm tra cài đặt vị trí của bạn. Một số ứng dụng cho phép bạn biết bạn bè mình đang ở đâu. Các ứng dụng đó cũng chia sẻ địa điểm của bạn. Hãy nghĩ xem khi nào việc chia sẻ vị trí là hợp lý. Khi thấy không hợp lý thì hãy tắt tính năng

chia sẻ vị trí. Các tính năng trên thiết bị của bạn, như là máy ảnh, có thể có thông tin về vị trí của bạn khi chụp ảnh. Nếu bạn không muốn phát đi thông tin về địa điểm của mình trong mỗi lần chụp ảnh tự sướng thì hãy tắt vị trí của bạn trên camera điện thoại. Hãy luôn tự hỏi bản thân: "Ứng dụng này có cần phải biết tôi đang ở đâu không?"

Giới hạn bạn bè trực tuyến của bạn ở những người bạn thực sự biết. Việc kết nối với bạn bè qua tin nhắn, mạng xã hội hoặc trò chơi điện tử có thể rất thú vị — nhưng một số người không phải là người như họ nói khi ở trên mạng. Và nếu không cẩn thận thì bạn có thể chia sẻ thông tin cá nhân với người lạ.

Bảo vệ thông tin của bạn

Một khi bạn cung cấp thông tin cá nhân của mình — như là số An sinh Xã hội, mật khẩu hoặc thông tin tài khoản ngân hàng — cho người mà bạn không biết thì sẽ không có cách nào để lấy lại thông tin đó.

Dưới đây là cách bảo vệ thông tin của bạn trực tuyến:

Không trả lời những tin nhắn yêu cầu thông tin cá nhân. Ngay cả khi tin nhắn trông giống như được gửi từ một người bạn, thành viên gia đình hoặc một công ty mà bạn biết — hoặc nói rằng điều gì đó tồi tệ sẽ xảy ra nếu bạn không trả lời. Rất có thể, đó là tin nhắn giả mạo và được gửi để lấy cắp

thông tin của bạn. Hãy nhờ một người lớn đáng tin cậy giúp bạn báo cáo rằng tin nhắn đó là thư rác.

Kiểm tra xem thông tin nào một ứng dụng muốn truy cập — trước khi bạn tải ứng dụng xuống. Một số ứng dụng yêu cầu quyền truy cập vào thông tin hoặc tính năng mà chúng không cần đến, như là danh sách liên hệ, máy ảnh, bộ nhớ, vị trí và micrô. Hãy nhờ một người lớn đáng tin cậy trợ giúp đọc chính sách quyền riêng tư của ứng dụng để xem dữ liệu của bạn sẽ được sử dụng như thế nào và liệu dữ liệu đó có bị chia sẻ hay không. Sau đó, quyết định xem liệu trò chơi xếp chữ đó có thực sự cần truy cập vào kho ảnh của bạn hay không.

Trao đổi với một người lớn đáng tin cậy trước khi mua hàng trong ứng dụng — đặc biệt nếu họ trả tiền cho mặt hàng đó.

Bảo vệ tài khoản của bạn

Bạn lưu giữ nhiều thông tin cá nhân trong các tài khoản trực tuyến của mình. Dưới đây là một số bước cần thực hiện để ngăn người khác truy cập vào tài khoản của bạn.

Tạo các mật khẩu mạnh.
Mật khẩu của bạn càng dài thì càng khó bị bẻ khóa. Sử dụng ít nhất 12 ký tự kết hợp chữ hoa và chữ thường, con số và ký hiệu. Hãy cân nhắc việc sử dụng cụm mật khẩu gồm

các từ ngẫu nhiên để khiến nó dễ nhớ hơn. Nhưng đừng sử dụng các cụm từ thông dụng, lời bài hát hoặc trích dẫn từ phim ảnh mà người khác dễ đoán được.

Luôn chỉ có một. Hãy nghĩ ra các mật khẩu khác nhau cho các tài khoản khác nhau. Bằng cách đó, nếu ai đó lấy được mật khẩu của một tài khoản, họ sẽ không thể sử dụng mật khẩu đó để truy cập vào các tài khoản khác của bạn. Một cách để theo dõi tất cả các mật khẩu khác nhau của bạn là sử dụng trình quản lý mật khẩu.

Giữ làm thông tin riêng tư. Đừng chia sẻ mật khẩu với bất kỳ ai, kể cả bạn thân hoặc người bạn đang hẹn hò.

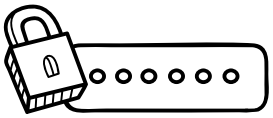
Hãy cẩn thận chọn các câu hỏi bảo mật. Cố gắng chọn

những câu hỏi bảo mật mà chỉ bạn mới có thể trả lời. Bỏ qua các câu hỏi có câu trả lời mà ai đó có thể tìm thấy trên mạng — như mã vùng, nơi sinh hoặc tên thời con gái của mẹ bạn. Nếu bạn không thể tránh được những câu hỏi đó thì hãy trở nên sáng tạo! Hãy coi chúng như là mật khẩu cũng như sử dụng các câu trả lời dài và ngẫu nhiên. Nhớ đảm bảo rằng bạn nhớ các câu trả lời của mình.

Sử dụng xác thực đa yếu tố. Nhiều tài khoản cung cấp khả năng bảo vệ bổ sung cho tài khoản của bạn bằng cách sử dụng “xác thực đa yếu tố” — yêu cầu thứ gì đó ngoài mật

khẩu. Xác thực đa yếu tố kết hợp thông tin bạn biết (như là mật khẩu) với thông tin bạn có (như là mật mã do ứng dụng tạo ra) hoặc thông tin gì đó về bạn (như là dấu vân tay).

Nhanh chóng đổi mật khẩu nếu có vi phạm.
Nếu một công ty cho bạn biết đã xảy ra sự cố vi phạm dữ liệu mà tin tặc có thể đã lấy được mật khẩu của bạn thì hãy thay đổi mật khẩu bạn sử dụng cho tài khoản đó ngay lập tức. Bạn cũng nên thay đổi mật khẩu cho bất kỳ tài khoản nào sử dụng mật khẩu tương tự.



Bảo vệ thiết bị của bạn

Cách tốt nhất để tận hưởng việc tham gia trực tuyến là gì? Đảm bảo rằng thiết bị của bạn được an toàn và bảo mật. Bắt đầu từ đây:

Đặt phần mềm bảo mật ở chế độ tự động cập nhật cho tất cả các thiết bị, trình duyệt internet và hệ điều hành của bạn. Điều này giúp bạn bảo vệ chống lại các mối đe dọa bảo mật mới.

Đừng bấm vào liên kết hoặc mở tệp đính kèm. Nếu bạn nhận được một văn bản, email hoặc tin nhắn trực tuyến bất ngờ mà yêu cầu bạn nhấp vào liên kết hoặc mở tệp đính kèm thì đừng làm vậy! Ngay cả khi đó là một lời đề nghị cung cấp những thứ miễn phí. Các liên kết và tệp đính kèm có thể ẩn chứa vi-rút hoặc phần mềm gián điệp mà có thể làm hỏng điện thoại, máy tính hoặc máy tính bảng của bạn.

Hãy bảo vệ thiết bị của bạn bằng mật khẩu. Điều này sẽ giúp giữ cho ảnh, tin nhắn và tài khoản của bạn không bị rơi vào tay kẻ xấu.

Để chúng ở nơi an toàn. Cho dù đó là điện thoại, máy tính xách tay hay máy tính bảng, đừng để nó ở nơi công cộng - dù chỉ là trong một phút.

Tìm hiểu thêm tại **ftc.gov/KidsOnline**

This booklet helps kids socialize safely online. There's help on how to share with care, be kind online, stand up to cyberbullying, and protect their personal information. Get free copies in English or Spanish at

ftc.gov/bulkorder

FEDERAL TRADE COMMISSION

Tháng 8 năm 2023