Tham gia trực tuyến an toàn và trách nhiệm

26 phút

Trong khoá học này, bạn sẽ được giới thiệu về những rủi ro an toàn mà bản thân có thể gặp phải khi sử dụng internet. Bạn sẽ tìm hiểu về những thủ đoạn gian lận và cách phòng tránh. Bạn cũng sẽ tìm hiểu về các biện pháp tốt nhất để chia sẻ thông tin trên mạng. Ngoài ra, bạn sẽ được giới thiệu về bắt nạt trên mạng.

Bảo mật và an toàn trực tuyến

17 phút | 8 bài

Trong học phần này, bạn sẽ tìm hiểu về một số rủi ro an toàn có thể ảnh hưởng đến bạn khi sử dụng internet, cũng như các mẹo để giữ an toàn và bí mật thông tin của bạn trên mạng.

Bảo vệ bạn khỏi lừa đảo trực tuyến

3 phút

Bảo vệ bạn khỏi lừa đảo trực tuyến

Mặc dù có nhiều điều tích cực chúng ta có thể làm trên mạng, ta cần luôn luôn cảnh giác với các rủi ro an toàn. Có rất nhiều trò gian lận mà những "kẻ săn mồi" sử dụng để truy cập thông tin trực tuyến của mọi người.

Bạn nên lưu ý về những trò gian lận này để cố gắng tránh chúng. **Lừa đảo trực tuyến** là một hình thức gian lận trực tuyến phổ biến mà bạn nên biết.

Xem video sau để tìm hiểu thêm về lừa đảo trực tuyến và cách tự bảo vệ mình khỏi trò gian lận trực tuyến này.

Video: Bảo vệ bạn khỏi lừa đảo trực tuyến

Internet mang lại cho chúng ta nhiều khả năng. Chúng ta có thể nói chuyện với người khác, mua hàng trực tuyến và thực hiện hoạt động kinh doanh cá nhân từ một nơi. Nhưng những tương tác trực tuyến này không phải lúc nào cũng an toàn. Hãy nói về một trò gian lận trực tuyến phổ biến mà bạn nên biết.

Một cách phổ biến để bắt cá là đặt thức ăn lên lưỡi câu để nhử cá. Một khi chúng cắn thức ăn, chúng sẽ bị mắc câu. Lừa đảo trực tuyến hoạt động theo cách thức tương tự. Những người muốn đánh cắp thông tin của bạn giống như ngư dân. Họ gửi cho bạn một email hoặc tin nhắn tức thời thông qua mạng xã hội hoặc một trò chơi trực tuyến. Họ thường giả vờ là một người và yêu cầu bạn cung cấp thông tin cá nhân hoặc họ bảo bạn nhấp vào một siêu liên kết để bạn có thể hoàn thành một nhiệm vụ quan trọng. Nếu bạn cung cấp cho họ thông tin hoặc nhấp vào siêu liên kết, bạn sẽ bị mắc bẫy. Nhưng đừng lo lắng. Bốn biện pháp này có thể giúp bảo vệ bạn khỏi lừa đảo trực tuyến.

Biện pháp số 1, hãy cẩn thận với các tin nhắn đáng ngờ. Những kẻ lừa đảo cố gắng làm cho tin nhắn của họ trông chính thức và quen thuộc, vì vậy bạn tin tưởng họ. Hãy cân nhắc kỹ khi bạn nhận được một tin nhắn đáng ngờ và tránh chia sẻ thông tin cá nhân qua tin nhắn hoặc email. Điều này bao gồm địa chỉ nhà của bạn, thông tin ngân hàng, mật khẩu v.v. Đừng nhấp vào liên kết hoặc tải xuống tệp nếu bạn không biết hoặc không tin tưởng người gửi.

Biện pháp số 2, hãy tìm kiếm các dấu hiệu cho thấy một trang web an toàn và bảo mật. Trước khi bạn cung cấp thông tin thẻ tín dụng, hãy nhập mật khẩu hoặc cung cấp thông tin cá nhân khác, xác minh rằng bạn đang ở trên một trang web an toàn đáng tin cậy. Hầu hết các trang web bảo mật đều có tiền tố https ở đầu URL trong thanh địa chỉ. Ngoài ra, hãy chắc chắn rằng bạn đang ở đúng trang web. Những kẻ lừa đảo thường cố gắng dẫn bạn đến các trang web có vẻ là chính thức và sử dụng sai chính tả tên công ty để lừa bạn. Ví dụ như www.microsoft.net không giống như trang web chính thức của Microsoft tại www.microsoft.com.

Luôn kiểm tra URL để đảm bảo bạn đang ở đúng trang web.

Biện pháp số 3, giữ cho trình duyệt web và hệ điều hành của bạn được cập nhật. Bạn có thể bật cập nhật tự động để đảm bảo các bản phát hành phần mềm mới nhất được tự động cài đặt trên máy tính của mình. Luôn cập nhật phần mềm trên thiết bị của bạn nghĩa là bạn sẽ nhận được các bản cập nhật bảo mật mới nhất giúp bảo vệ máy tính của mình

Biện pháp số 4, cài đặt phần mềm chống phần mềm độc hại được chứng nhận trên thiết bị của bạn. Đây là phần mềm đặc biệt được thiết kế để bảo vệ máy tính của bạn khỏi các phần mềm có hại và hacker. Đừng là con cá tiếp theo bị mắc câu. Khi bạn sử dụng internet, hãy nhớ suy nghĩ trước khi nhấp, tải xuống hoặc chia sẻ để bảo vệ bản thân khỏi các hành vi lừa đảo trực tuyến.

Giao tiếp trên mạng một cách an toàn

2 phút

Giao tiếp trên mạng một cách an toàn

Internet cho phép chúng ta giao tiếp với người khác theo những cách thức mới. Tuy nhiên, việc giao tiếp trên mạng không phải lúc nào cũng an toàn. Không phải lúc nào bạn cũng biết chắc chắn mình đang nói chuyện với ai khi bạn truy cập internet, vì vậy bạn phải cẩn thận để giữ an toàn.

Xem video sau để tìm hiểu cách giao tiếp trên mạng một cách an toàn.

Video: Giao tiếp trên mạng một cách an toàn

Với internet, chúng ta có thể giao tiếp với những người khác trên khắp thế giới theo những cách thức mới. Điều này có nhiều lợi ích, nhưng cũng có một số nguy hiểm. Có những kẻ săn mồi trực tuyến sử dụng internet mỗi ngày. Những kẻ mồi này thường giả vờ là những người khác. Vì vậy, rất khó để biết bạn đang nói chuyện với ai trên mạng. Dưới đây là ba mẹo bạn

có thể sử dụng để giữ an toàn cho bản thân khỏi những kẻ săn mồi trực tuyến khi giao tiếp trên mạng.

Mẹo số 1, sử dụng trực giác của bạn. Nếu ai đó khiến bạn cảm thấy lo lắng hoặc không thoải mái, hãy ngừng liên lạc với họ và nói với ai đó bạn tin tưởng ngay lập tức. Hầu hết các trang web và trang truyền thông xã hội đều có các công cụ mà bạn có thể sử dụng để báo cáo hoạt động đáng ngờ.

Mẹo số 2, hạn chế những gì bạn chia sẻ. Những kẻ săn mồi trực tuyến thường cố gắng dẫn dụ bạn chia sẻ thông tin cá nhân của mình thông qua email và tin nhắn. Tránh chia sẻ thông tin cá nhân với một người lạ trên mạng.

Mẹo số 3, giữ khoảng cách của bạn. Hãy suy nghĩ kỹ về việc gặp ai đó mà bạn chỉ nói chuyện qua mạng. Những kẻ săn mồi thường sử dụng mạng xã hội để đóng giả thành một người khác bằng cách thiết lập hồ sơ giả bằng hình ảnh của người khác. Ngay cả khi ai đó có vẻ thân thiện, thật khó để biết chắc chắn bạn đang nói chuyện với ai trên mạng. Luôn luôn nói với cha mẹ hoặc người mà bạn tin tưởng khi một người lạ trên mạng yêu cầu gặp bạn trực tiếp, để bạn không gặp phải tình huống nguy hiểm. Nhiều kẻ săn mồi trực tuyến sử dụng chiến thuật thông minh để dụ bạn vào tình huống nguy hiểm, nhưng bạn có thể thông minh hơn. Hãy ghi nhớ những rủi ro và lời khuyên này để bạn có thể an toàn khi nói chuyện với mọi người trên mạng.

Tạo mật khẩu mạnh

2 phút

Tạo mật khẩu mạnh

Một yếu tố quan trọng của việc giữ an toàn và bí mật thông tin của bạn trên mạng là bảo vệ thông tin, tài khoản và máy tính của bạn bằng mật khẩu mạnh.

Xem video sau để tìm hiểu cách tạo mật khẩu mạnh và hiệu quả để bảo vệ thông tin của bạn.

Video: Tạo mật khẩu mạnh

Mật khẩu giúp bảo vệ thông tin cá nhân và tài khoản của bạn khỏi những người khác. Mật khẩu cũng quan trọng như khóa cửa. Bạn muốn một chiếc khóa mạnh mẽ, khó phá và ngăn những người nguy hiểm xâm nhập vào bên trong. Bạn cũng không muốn bất cứ ai tìm thấy chìa khóa để mở khóa của bạn. Mật khẩu mạnh giống như một khóa mạnh cho tài khoản của bạn, bạn muốn người khác khó đoán, bạn cũng muốn nó an toàn và bảo mật để người khác không thể tìm thấy. Làm theo các mẹo sau đây để tạo mật khẩu mạnh và giữ chúng an toàn.

Mẹo số 1, sử dụng kết hợp các chữ cái, số và ký hiệu trong mật khẩu của bạn. Sử dụng kết hợp chữ hoa và chữ thường và ký tự và thêm số có thể tăng cường độ mạnh của mật khẩu của bạn.

Mẹo số 2, tránh sử dụng các từ phổ biến trong mật khẩu của bạn. Điều này bao gồm các từ và cụm từ phổ biến như mật khẩu hoặc trang web, cũng như các từ khóa cá nhân như sinh nhật, tên hoặc quê quán của bạn. Tin tặc có thể dễ dàng đoán những cụm từ này trong mật khẩu của bạn. Một sự kết hợp độc đáo của các ký tự và số tạo ra một mật khẩu mạnh hơn.

Mẹo số 3, sử dụng mật khẩu khác nhau cho các tài khoản khác nhau. Nếu ai đó đoán được mật khẩu email của bạn, sự an toàn và riêng tư của bạn có thể gặp rắc rối nếu bạn sử dụng cùng một mật khẩu cho tài khoản ngân hàng của mình. Thay vào đó sử dụng các mật khẩu khác nhau cho mỗi tài khoản trực tuyến của bạn.

Mẹo số 4, mật khẩu của bạn chỉ dành cho bạn. Khi bạn chia sẻ nó với những người khác thậm chí là bạn bè và gia đình, nhiều khả năng người khác sẽ sử dụng nó hoặc sẽ không giữ an toàn. Hãy giữ riêng mật khẩu của bạn. Khi bạn đăng nhập vào tài khoản, hãy đảm bảo bạn đăng xuất khi hoàn thành và không lưu thông tin đăng nhập của bạn trên máy tính công cộng.

Ngoài ra, tránh kinh doanh cá nhân trên máy tính công cộng và mạng công cộng, vì điều này giúp tin tặc truy cập thông tin của bạn dễ dàng hơn. Hãy nhớ rằng, sử dụng mật khẩu mạnh và giữ chúng an toàn là điều quan trọng đối với sự an toàn và bảo mật trực tuyến của bạn. Hãy ghi nhớ những lời khuyên này khi bạn tạo một mật khẩu mới.

Mô tả các biện pháp tốt nhất để chia sẻ thông tin trên mạng

2 phút

Hãy thông minh khi bạn chia sẻ

Khi chúng ta lên mạng, ta thường làm nhiều điều đe dọa đến sự an toàn của mình mà không suy nghĩ nhiều về nó. Điều quan trọng là phải suy nghĩ kỹ về những gì bạn chia sẻ trực tuyến và giữ an toàn cho bản thân.

Xem video sau để tìm hiểu thêm về những rủi ro của việc chia sẻ trên mạng quá nhiều.

Video: Chia sẻ trên mạng quá nhiều

Internet và web giúp chúng ta có thể kết nối với bạn bè và gia đình trên khắp thế giới. Chúng ta có thể sử dụng mạng xã hội và các nền tảng khác để xem những gì đang xảy ra trong cuộc sống của bạn bè, chia sẻ tin tức cá nhân và giữ liên lạc với những người khác, nhưng chia sẻ mọi thứ trên mạng không phải lúc nào cũng an toàn.

Xem xét kịch bản này, Harold có một chiếc xe mới và muốn bạn bè của mình nhìn thấy nó. Vì vậy, anh ấy đăng một bức ảnh của nó trên mạng xã hội. Điều này có vẻ ổn, nhưng bức ảnh bao gồm rất nhiều thông tin cá nhân về Harold. Bất cứ ai cũng có thể nhìn thấy biển số xe của anh ấy, loại xe anh ấy lái và nơi anh ấy sống từ một bức ảnh.

Điều này có thể ổn nếu bạn bè của anh ta xem nó, nhưng nó có thể nguy hiểm nếu người xấu tìm thấy thông tin này và muốn sử dụng nó cho các mục đích xấu. Điều quan trọng là chú ý đến an toàn và riêng tư khi bạn chia sẻ mọi thứ trên mạng.

Khi bạn thiết lập hồ sơ trên các trang web truyền thông xã hội, hãy nhớ xem lại cài đặt quyền riêng tư của tài khoản của mình. Nếu tài khoản của bạn được đặt thành công khai, bất kỳ ai cũng có thể xem thông tin của bạn và những gì bạn chia sẻ. Thay vào đó, hãy sử dụng cài đặt riêng tư trên các tài khoản để chỉ những kết nối cá nhân của bạn nhìn thấy những gì bạn chia sẻ.

Bạn cũng nên chọn lọc khi bạn chấp nhận lời mời kết nối với ai đó qua mạng xã hội. Hầu hết các nền tảng truyền thông xã hội đều có cách để bạn chấp nhận và từ chối các yêu cầu, để có ai đó là bạn của bạn hoặc người theo dõi trên trang web. Khi bạn chấp nhận ai đó, họ có quyền truy cập trực tiếp vào hồ sơ của bạn và những điều bạn chia sẻ. Hãy ghi nhớ điều này khi bạn nhận được yêu cầu và đảm bảo rằng bạn chỉ tương tác với những người bạn biết và tin tưởng.

Ngay cả khi bạn kiểm soát ai có quyền truy cập vào hồ sơ và tài khoản của mình, bạn cũng không thể kiểm soát những gì người khác làm với thông tin của mình. Khi bạn chia sẻ một cái gì đó trên mạng, bạn không thể xóa nó. Không bao giờ chia sẻ một cái gì đó trên mạng mà bạn sẽ không muốn người lạ và công chúng nhìn thấy. Luôn suy nghĩ kỹ trước khi chia sẻ. Lưu ý giữ an toàn và đưa ra lựa chọn thông minh khi bạn chia sẻ mọi thứ trên mạng.

Hãy thử trải nghiệm

Bạn đã học được gì từ video này? Viết ra 1 đến 3 điều bạn sẽ ghi nhớ khi chia sẻ thông tin cá nhân trên mạng.

Mô tả tầm quan trọng của việc quản lý dấu chân kỹ thuật số

3 phút

Dấu chân kỹ thuật số của bạn

Có rất nhiều thứ chúng ta có thể làm trên mạng, từ duyệt web, chia sẻ cập nhật trên mạng xã hội, đến mua hàng trực tuyến. Bạn nên nhớ rằng mọi thứ bạn làm trên mạng đều trở thành một phần của lịch sử trực tuyến hoặc **dấu chân kỹ thuật số** của bạn.

Bạn nên suy nghĩ về dấu chân kỹ thuật số của bạn khi bạn chia sẻ thông tin hoặc thực hiện mọi việc trên mạng, vì những việc xảy ra trên mạng rất khó xóa.

Xem video sau để tìm hiểu thêm về dấu chân kỹ thuật số của bạn và cách quản lý.

Video: Quản lý dấu chân kỹ thuật số của bạn

Nếu bạn sử dụng internet, bạn nên biết về dấu chân kỹ thuật số của bạn. Giống như dấu chân vật lý cho thấy ai đó bước trên một con đường đất, dấu chân kỹ thuật số của bạn là một lịch sử của tất cả các hoạt động bạn làm trên mạng. Bất kỳ bài đăng nào bạn viết, bất kỳ trang web nào bạn truy cập và bất kỳ thông tin nào bạn chia sẻ trên mạng đều góp phần vào dấu chân kỹ thuật số của bạn.

Khi bạn đăng một cái gì đó trên mạng, bạn không thể xóa nó. Vì vậy, dấu chân kỹ thuật số của bạn có thể tồn tại mãi mãi. Đây có thể là một điều tốt nếu dấu chân kỹ thuật số của bạn

bao gồm những thứ mang lại cho bạn một danh tiếng tích cực trên mạng. Điều này có thể giúp bạn xây dựng thương hiệu cá nhân của mình. Lịch sử trực tuyến của bạn cũng có thể giúp các ứng dụng bạn sử dụng biết nhiều hơn về bạn. Họ có thể sử dụng thông tin này để phục vụ bạn tốt hơn bằng cách điều chỉnh những thứ bạn thích và thói quen hàng ngày của bạn. Nhưng họ cũng có thể sử dụng thông tin này sai cách và chia sẻ nó với những người khác. Hãy ghi nhớ những lời khuyên sau đây khi bạn lên mạng để quản lý dấu chân kỹ thuật số của mình.

Mẹo số một, biết dấu chân của bạn nói gì về bạn. Người khác sử dụng dấu chân kỹ thuật số của bạn để đưa ra đánh giá về bạn trên mạng. Điều này có thể bao gồm các nhà tuyển dụng khi bạn nộp đơn xin việc hoặc nhà tuyển dụng khi bạn nộp đơn vào các chương trình học tập. Điều quan trọng là phải biết dấu chân kỹ thuật số của bạn nói gì về bạn và cách thức mà thông tin của bạn đang được sử dụng. Để xem thương hiệu cá nhân trên mạng của bạn là gì, bạn có thể tự tìm kiếm. Tìm kiếm tên của bạn trong công cụ tìm kiếm Bing và xem kết quả nào được hiển thị. Nếu những kết quả này không hiển thị những gì bạn muốn, hãy nghĩ về những gì bạn chia sẻ trên mạng và những thông tin bạn cho phép người khác xem.

Mẹo số 2, Quản lý cài đặt quyền riêng tư của bạn. Bạn có thể sửa đổi cài đặt quyền riêng tư của hầu hết các trang web và các ứng dụng mạng xã hội mà bạn sử dụng. Điều này có thể giúp bạn kiểm soát những người nhìn thấy những gì bạn chia sẻ và thông tin nào hiển thị khi ai đó tìm kiếm bạn trên mạng.

Mẹo số 3, Quản lý cookie của bạn. Cookies là những ghi chú được đưa ra cho trình duyệt web của bạn khi bạn duyệt web. Những cookie này giúp ứng dụng theo dõi thông tin mà họ cần trong khi bạn đang sử dụng ứng dụng. Điều này có thể giúp ứng dụng hoạt động tốt hơn cho bạn. Nhưng dữ liệu này cũng góp phần vào dấu chân kỹ thuật số của bạn. Bạn có thể sử dụng các cài đặt trong trình duyệt của mình để hạn chế hoặc chặn việc sử dụng cookie trên các trang web nhất định.

Mẹo số 2, suy nghĩ kỹ trước khi bạn chia sẻ. Khi bạn chia sẻ một cái gì đó trên mạng, bạn không thể lấy lại. Hãy chắc chắn rằng bạn đồng ý với việc nó trở thành một phần trong dấu chân kỹ thuật số công khai của mình trước khi bạn chia sẻ nó. Dấu chân kỹ thuật số của bạn có thể tồn tại mãi mãi. Hãy ghi nhớ những lời khuyên này để đảm bảo bạn hài lòng với dấu chân kỹ thuật số của mình và cách sử dụng nó.

Kiểm tra kiến thức

3 phút

1. Bạn nên tìm thành phần nào sau đây trong địa chỉ URL của trang web để đảm bảo bạn có thể sử dụng trang web an toàn?
    a) http
    b) an toàn
    c) https - Đúng! "https" có nghĩa là trang web được bảo mật.
    d) ssh

2. Mật khẩu nào mạnh nhất?
    a) John@453 - Đúng! Mật khẩu này chứa chữ hoa, chữ thường, ký tự đặc biệt và số.
    b) john500
    c) JoHn300
    d) 125893

3. Dấu chân kỹ thuật số của bạn là:
    a) Quy mô của thông tin trong tài khoản trực tuyến của bạn.
    b) Số lượng người bạn kết nối trực tuyến.
    c) Một bản ghi tất cả mọi thứ bạn làm và nói trên mạng. - Đúng! Dấu chân kỹ thuật số của bạn giúp dễ dàng theo dõi hành động của bạn trên mạng.
    d) Tên người dùng trực tuyến của bạn.

Tổng kết
1 phút

Chúc mừng bạn!
Bạn đã hoàn thành học phần Bảo mật và an toàn trực tuyến và bây giờ có thể tự trả lời các câu hỏi sau:

1. Một số nguy cơ của việc sử dụng internet và web là gì?
2. Một số dấu hiệu của rủi ro an toàn và lừa đảo trực tuyến là gì?
3. Những bước bạn có thể thực hiện để giữ an toàn trong khi sử dụng internet?
4. Bạn có thể quản lý dấu chân kỹ thuật số bằng cách nào?

Văn minh trực tuyến
9 phút | 5 bài

Trong học phần này, bạn sẽ tìm hiểu thêm về quyền và cách tốt nhất để sử dụng thông tin trên mạng. Bạn cũng sẽ tìm hiểu về bắt nạt trên mạng.

Giới thiệu
1 phút

Chúng ta có thể sử dụng internet để truy cập nhiều thông tin và liên lạc với người khác, nhưng chúng ta cũng phải đảm bảo rằng ta cư xử như những công dân số có trách nhiệm.

Trong bài học này, bạn sẽ học cách sử dụng internet và web một cách có trách nhiệm.

Kết thúc học phần này, bạn sẽ có thể:

1. Mô tả các quyền mà mọi người có đối với thông tin và nội dung được chia sẻ trên mạng.

2. Mô tả các biện pháp tốt nhất để sử dụng thông tin tìm thấy trên mạng.
3. Mô tả ý nghĩa của việc đối xử tệ với người khác trên mạng.

Mô tả các biện pháp tốt nhất để sử dụng thông tin tìm thấy trên mạng

2 phút

Sử dụng thông tin có trách nhiệm

Mặc dù việc truy cập thông tin rất dễ dàng trong thế giới số, nhưng có một số quy tắc cần lưu ý khi bạn muốn sử dụng thông tin bạn tìm thấy trên mạng.

Xem video sau để tìm hiểu một số hướng dẫn sử dụng thông tin mà bạn tìm thấy trên mạng.

Video: Sử dụng thông tin có trách nhiệm

Internet cung cấp cho chúng ta thông tin và khả năng không giới hạn. Chúng ta có thể tìm thấy bất cứ điều gì từ các video hài hước đến các bài hát yêu thích, hoặc thông tin về cách giải quyết vấn đề bài tập về nhà, nhưng chúng ta phải có trách nhiệm với thông tin mà chúng ta tìm thấy trên mạng.

Hãy xem xét một kịch bản. Harold muốn viết một cuốn sách nấu ăn và bán nó trên mạng. Anh ấy không giỏi chụp ảnh, vì vậy anh ấy tìm kiếm hình ảnh trên mạng. Anh ấy tải hình ảnh của các loại thực phẩm khác nhau và đưa chúng vào cuốn sách của mình. Điều này có vẻ ổn vì nó dễ thực hiện, nhưng đây không phải là cách sử dụng thông tin tìm thấy trên mạng một cách công bằng hoặc có trách nhiệm.

Khi ai đó đưa tác phẩm gốc của họ lên mạng bao gồm từ ngữ, hình ảnh, video, âm nhạc, v.v... họ trở thành chủ sở hữu của nội dung. Là chủ sở hữu, họ có một số quyền nhất định, thường được coi là bản quyền để quyết định cách sử dụng nội dung đó. Nếu bạn sử dụng câu từ hoặc tác phẩm của người khác như của riêng bạn, điều đó được coi là đạo văn. Điều này không công bằng với tác giả ban đầu và có thể khiến bạn gặp rắc rối. Nếu bạn muốn sử dụng nội dung của người khác trong tác phẩm của mình, hãy nhớ hỏi ý kiến của họ để trả phí cho tác phẩm của họ.

Khi bạn đang sử dụng tác phẩm của ai đó trong một sản phẩm mà bạn đang bán, trước tiên bạn nên xin phép tác giả. Có thể, bạn sẽ phải tiền cho giấy phép sử dụng tác phẩm của ai đó. Đôi khi, các tác giả của nội dung cung cấp sẵn tác phẩm của họ để sử dụng miễn phí.

Bạn có thể sử dụng các công cụ tìm kiếm như Bing để tìm hình ảnh, phương tiện và các loại nội dung khác có sẵn cho người khác sử dụng. Khi bạn sử dụng internet và tìm thông tin trên mạng, hãy đảm bảo bạn sử dụng nó một cách công bằng và có trách nhiệm.

Mô tả ý nghĩa của việc đối xử tệ với người khác trên mạng

3 phút

Bắt nạt trên mạng

Internet cho phép chúng ta kết nối với những người dùng trực tuyến từ khắp nơi trên thế giới. Nhưng, không may là mọi người không phải lúc nào cũng đối xử tốt với nhau trên mạng.

Bắt nạt trên mạng là một loại bắt nạt diễn ra trên internet. Việc gửi tin nhắn có nội dung xấu hoặc lan truyền tin đồn tiêu cực về người khác có thể rất dễ dàng, nhưng điều này gây nguy hiểm cho đối tượng được nhắm đến.

Xem video sau đây để tìm hiểu các mẹo để ngăn chặn bắt nạt trên mạng và là một công dân số.

Video: Tôn trọng người khác trên mạng

Internet và các nền tảng mạng xã hội kết nối chúng ta với bạn bè, gia đình và đồng nghiệp theo những cách thức mới. Đôi khi mọi người tận dụng các nền tảng này và sử dụng chúng để truyền bá thông điệp tiêu cực về người khác.

Bắt nạt trên mạng, hoặc bắt nạt diễn ra trên internet, có thể tệ như bắt nạt trực tiếp. Mọi người có thể sử dụng internet để gửi tin nhắn có ý nghĩa cho ai đó, lan truyền tin đồn giả mạo hoặc chia sẻ thông tin cá nhân của ai đó mà không được phép. Khi ai đó bị bắt nạt trên mạng, cảm xúc của họ có thể bị tổn thương và danh tiếng của họ có thể bị tổn hại. Bạn không thể luôn luôn ngăn chặn bắt nạt trên mạng, nhưng bạn có thể đóng góp một phần trong việc biến internet thành một nơi thân thiện hơn và an toàn hơn cho mọi người.

Dưới đây là một số hướng dẫn bạn có thể làm theo để thúc đẩy văn minh trực tuyến:

- Sống theo nguyên tắc vàng. Đối xử với người khác theo cách bạn muốn được đối xử, cho dù là trực tiếp hay trực tuyến.
- Tránh gửi tin nhắn tiêu cực và tham gia vào hành vi có thể làm tổn thương người khác.
- Tôn trọng sự khác biệt. Tất cả chúng ta đều khác biệt về nhiều mặt. Khi bạn tương tác với mọi người trên mạng, hãy tôn trọng sự khác biệt của họ về quan điểm, kinh nghiệm và văn hóa. Ngay cả khi bạn không đồng ý với điều gì đó mà người khác chia sẻ trên mạng, bạn vẫn nên tôn trọng họ và biến internet thành một không gian kết nối thân thiện.
- Tạm dừng trước khi trả lời. Trước khi bạn chia sẻ bất cứ điều gì trên mạng, luôn luôn tạm dừng và suy nghĩ về hậu quả. Tin nhắn của bạn sẽ làm tổn thương người khác? Nó sẽ làm tổn hại danh tiếng của bạn, hoặc sự an toàn hoặc danh tiếng của người khác?
- Hãy suy nghĩ kỹ trước khi chia sẻ trên mạng. Hãy hành động vì chính mình và những người khác. Nếu bạn cảm thấy không an toàn khi trực tuyến, bạn nên cảm thấy thoải mái khi loại bỏ bản thân khỏi một tình huống và báo cáo với người mà bạn tin tưởng.
- Khi bạn thấy hoạt động độc ác hoặc nguy hiểm trên mạng, hãy cung cấp hỗ trợ cho những người liên quan và báo cáo sự việc cho người mà bạn tin tưởng. Tất cả chúng ta có thể đóng vai trò trong việc biến internet thành một nơi an toàn và thân thiện cho mọi người.

- Hãy thực hiện vai trò của bạn và là một công dân số có trách nhiệm.

Kiểm tra kiến thức

2 phút

1. Hành động nào sau đây không vi phạm bản quyền?
    a) Sử dụng hình ảnh của ai đó trong một cuốn sách bạn xuất bản mà không có sự cho phép của họ.
    b) Trích dẫn một đoạn từ cuốn sách của ai đó và ghi nguồn từ họ - Đúng! Bạn phải tuân thủ bản quyền khi bạn trích dẫn lời của tác giả.
    c) Bán video của ai đó dưới tên của bạn.
    d) Bán sách của ai đó mà không có giấy phép.

2. Bắt nạt trên mạng có thể diễn ra:
    a) Chỉ trên các nền tảng truyền thông xã hội.
    b) Chỉ qua email.
    c) Chỉ trên tin nhắn SMS.
    d) Trên các nền tảng truyền thông xã hội và tin nhắn SMS, thông qua email. - Đúng! Bắt nạt trên mạng có thể diễn ra trong bất kỳ hình thức giao tiếp nào.

Tổng kết

1 phút

Chúc mừng bạn!

Bạn đã hoàn thành học phần Văn minh trực tuyến và bây giờ có thể tự trả lời các câu hỏi sau:

1. Bạn nên làm gì khi bạn muốn sử dụng thông tin mà bạn tìm thấy trên mạng?
2. Bạn có thể làm gì để ngăn chặn hoặc chấm dứt bắt nạt trên mạng?

Thực hiện khảo sát và nhận chứng chỉ hoàn thành

4 phút | 2 bài

Bạn phải hoàn thành tất cả các học phần trong khóa học này và thực hiện khảo sát để nhận được chứng chỉ.

Thực hiện khảo sát cuối khoá học

3 phút

Chúc mừng bạn đã hoàn thành khóa học Tham gia trực tuyến an toàn và trách nhiệm. Hãy bấm vào liên kết đến **bản khảo sát cuối khoá học** ở mục kế tiếp và điền các thông tin yêu cầu. Những ý kiến đóng góp của bạn sẽ giúp cho chương trình ngày càng hoàn thiện hơn.

Nhận chứng chỉ hoàn thành

1 phút

Nhận chứng chỉ

Sau khi hoàn thành bản khảo sát, bạn hãy trở lại trang này, chọn mục **Chứng chỉ** phía dưới và nhận chứng chỉ hoàn thành khoá học của mình. Họ và tên bạn cung cấp trong hồ sơ cá nhân của mình sẽ được tự đông in trên chứng chỉ cùng với ngày bạn hoàn thành khoá học.

Tải xuống chứng chỉ

Ở góc trên bên phải của mục Chứng chỉ, bạn hãy chọn **Tải xuống chứng chỉ** để lưu chứng chỉ của mình vào nơi an toàn. Nếu chưa muốn tải xuống, bạn có thể chọn **Đóng và thoát**. Chứng chỉ hoàn thành khoá học của bạn vẫn sẽ được lưu trên hệ thống, và bạn hoàn toàn có thể truy cập và tải xuống bất kỳ lúc nào.