CỤC AN TOÀN THÔNG TIN

BỘ CẨM NANG
VỀ BẢO VỆ TRẺ EM TRÊN KHÔNG GIAN MẠNG

Năm 2024

Sách thuộc:

Chương trình
"Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh,
sáng tạo trên môi trường mạng
giai đoạn 2021 - 2025"

Ban biên soạn:
Cục An toàn thông tin

Đơn vị tư vấn nội dung:
Viện Nghiên cứu Quản lý Phát triển bền vững
Tổ chức Cứu trợ trẻ em Quốc tế

LỜI GIỚI THIỆU

Không gian mạng, Internet đã và đang trở thành một phần không thể tách rời của cuộc sống, đặc biệt đối với trẻ em là những đối tượng đang sử dụng công nghệ vào trong học tập và sinh hoạt hàng ngày. Theo báo cáo của Tổng cục Thống kê, tới hết năm 2023, dân số Việt Nam đạt khoảng 100,3 triệu người, trẻ em chiếm gần 1/4 dân số, trong đó 2/3 trẻ em có thể tiếp cận thiết bị kết nối Internet. Cũng số liệu Trung tâm quốc gia về trẻ theo em mất tích và bị bóc lột (NCMEC), năm 2023 có khoảng 533.236 báo cáo về hình ảnh/video xâm hại tình dục trẻ em trên mạng liên quan tới Việt Nam - đứng thứ 3 trong ASEAN, sau Indonesia và Phillipine. Thực tế đó cho thấy, không gian mạng đang có ảnh hưởng quan trọng đối với sự phát triển của trẻ em.

Đối với trẻ em, đối tượng chưa có đầy đủ kiến thức, kỹ năng, kinh nghiệm khi tham gia hoạt động trên môi trường mạng sẽ đối mặt với rất nhiều rủi ro như: (1) Tiếp cận với những nội dung độc hại (bạo lực, khiêu dâm,…) làm lệch lạc suy nghĩ, lối sống, sự phát triển; (2) Bị phát tán thông tin riêng tư, thông tin cá nhân của trẻ; (3) Bị bắt nạt trực tuyến; (4) Sử dụng quá mức và nghiện Internet; (5) Bị lôi kéo, dụ dỗ, quấy rối, lừa đảo, dọa nạt, tống tiền, ép tham gia các hoạt động phi pháp, mại dâm, bị xâm hại tình dục,…

Ngày 01/6/2021, Thủ tướng Chính phủ đã ban hành Quyết định số 830/QĐ-TTg phê duyệt Chương trình "Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng giai đoạn 2021 – 2025". Chương trình có "mục tiêu kép" gồm: (1) Bảo vệ bí mật đời sống riêng tư và ngăn chặn, xử lý các hành vi lợi dụng môi trường mạng để xâm hại trẻ em, trong đó đặc biệt chú trọng đến việc trang bị cho trẻ em kiến thức, kỹ năng phù hợp theo từng lứa tuổi để trẻ em tự nhận biết và có khả năng tự bảo vệ mình trên môi trường mạng. (2) Duy trì một môi trường mạng lành mạnh, phát triển hệ sinh thái các sản phẩm, ứng dụng Việt cho trẻ em học tập, kết nối, giải trí một cách sáng tạo.

Cục An toàn thông tin đã phối hợp với các cơ quan, đơn vị và các chuyên gia trong công tác bảo vệ trẻ em biên soạn, xuất bản cuốn sách: "Bộ cẩm nang về bảo vệ trẻ em trên không gian mạng" nhằm mục đích cung cấp những kiến thức cơ bản, cốt lõi theo từng nhóm tuổi phù hợp để trẻ em tự bảo vệ bản thân và phụ huynh cùng tham

gia bảo vệ con em mình sinh hoạt trên môi trường mạng.

Bộ cẩm nang được biên soạn gồm có 5 phần:

➢ Phần I: Cẩm nang chung - Cung cấp các thông tin cơ bản về Internet, lợi ích, rủi ro trên môi trường mạng với trẻ em, một số khái niệm về bảo vệ trẻ em trên môi trường mạng; hướng dẫn cách thức phản ánh khi phát hiện nội dung độc hại, nội dung không phù hợp đối với trẻ em.

➢ Phần II: Cẩm nang cho trẻ dưới 6 tuổi - Giai đoạn ươm mầm: Đây là lứa tuổi trẻ em mới bắt đầu tiếp cận với Internet dưới sự hướng dẫn hỗ trợ của cha mẹ, thầy cô. Phần nội dung này chủ yếu để hướng dẫn cho cha mẹ, thầy cô cách để hướng dẫn ban đầu cho trẻ em tham gia môi trường mạng.

➢ Phần III: Cẩm nang cho trẻ từ 6 tới 11 tuổi - Giai đoạn phát triển: Đây là lứa tuổi trẻ em đã bắt đầu học tập và tìm hiểu tương tác trên môi trường mạng trong một giới hạn nhất định, bắt đầu hình thành các kỹ năng số. Phần nội dung này gồm các hướng dẫn dành cho trẻ em hình thành các kỹ năng ban đầu và hướng dẫn, lời khuyên dành cho phụ huynh để hỗ trợ con một cách hiệu quả.

➢ Phần IV: Cẩm nang cho trẻ từ 11 tới 16 tuổi - Giai đoạn tiền trưởng thành: Đây là lứa tuổi trẻ em đã bắt đầu sử dụng Internet một cách độc lập. Phần nội dung chính vì thế sẽ bao gồm các hướng dẫn cụ thể cho trẻ em trong hình thành các kỹ năng cụ thể sử dụng Internet an toàn, lành mạnh và có trách nhiệm.

➢ Phần V: Một số công cụ, phần mềm hỗ trợ bảo vệ trẻ em trên môi trường mạng.

Hy vọng rằng, với những kiến thức và kỹ năng cơ bản này sẽ giúp cho phụ huynh, người chăm sóc trẻ và trẻ em có thể tự tin tham gia môi trường mạng an toàn.

Trong quá trình biên soạn, nội dung có thể còn thiếu sót, chúng tôi rất mong nhận được sự đóng góp ý kiến của độc giả để cuốn sách được hoàn thiện hơn trong lần xuất bản sau. Mọi ý kiến góp ý xin gửi tới địa chỉ Cục An toàn thông tin (Trung tâm VNCERT/CC) - Tầng 5 - Tòa nhà Cục Tần số Vô tuyến điện, số 115 Trần Duy Hưng, quận Cầu Giấy, Hà Nội; website: vn-cop.vn; hotline: 0796863111; email: bvte@vncert.vn.

Xin trân trọng giới thiệu cuốn sách cùng bạn đọc!

PHẦN 1

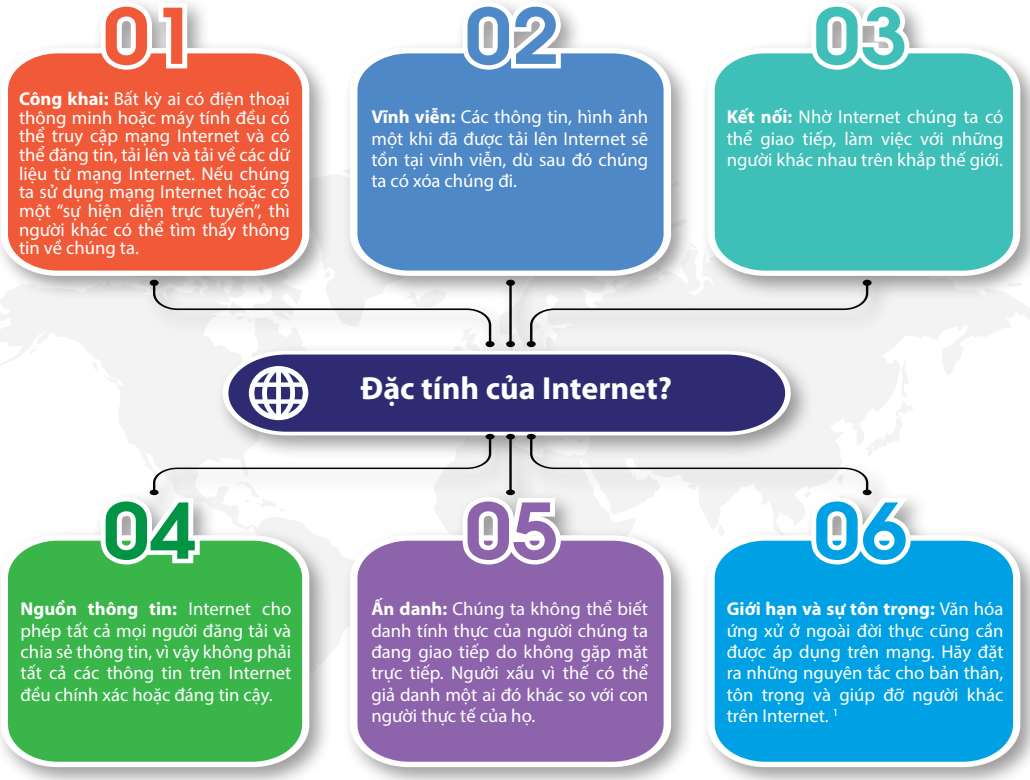
CẨM NANG CHUNG

1.1. TỔNG QUAN INTERNET

1.1.1. Internet và các đặc tính

Internet là gì?

Internet là một hệ thống thông tin toàn cầu có thể được truy cập công cộng gồm các mạng máy tính được liên kết với nhau. Internet có thể kết nối bởi máy tính, điện thoại thông minh, máy tính bảng, ...



Biểu đồ 1: 6 đặc tính của Internet

Chính vì 6 đặc tính này nên Internet có cả lợi ích và rủi ro.

[1] *Theo tài liệu dự án Swipe Safe – Tổ chức ChildFund tại Việt Nam*

1.1.2. Tình hình sử dụng Internet tại Việt Nam

Tình hình sử dụng Internet tại Việt Nam

Theo số liệu thống kê của We are Social, tính tới QI/2024, số lượng người dùng Internet ở Việt Nam là 78,44 triệu người, tăng 0,6% so với năm 2023 (chiếm 79,1% dân số); số người sử dụng mạng xã hội ở Việt Nam là gần 72.7 triệu người, tăng gần 6.5 triệu người trong vòng 1 năm (tương đương 73,3% dân số). Với con số này, Việt Nam là quốc gia có lượng người dùng Internet cao trên toàn thế giới. Người dùng Việt Nam dành trung bình 6 giờ 18 phút mỗi ngày để tham gia các hoạt động liên quan tới Internet và tỉ lệ người dùng Internet ở Việt Nam sử dụng Internet hàng ngày lên tới 94%, trong đó có trẻ em.

Tình hình sử dụng Internet của Trẻ em

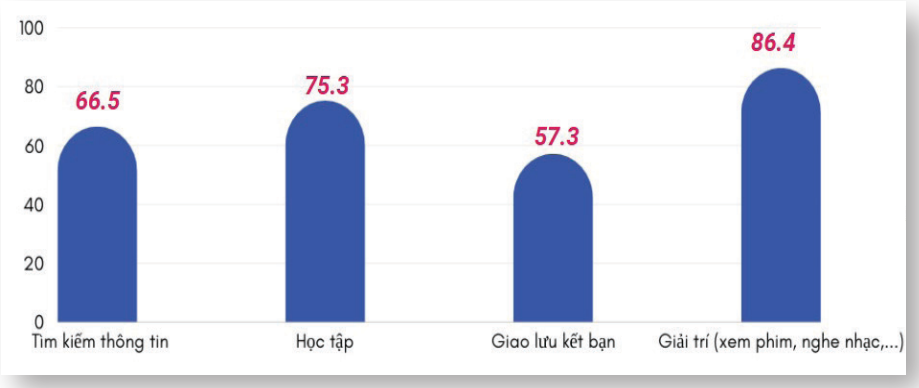
Nghiên cứu "Tiếng nói trẻ em Việt Nam" năm 2024 của Viện Nghiên cứu Quản lý phát triển bền vững (MSD) và Tổ chức Cứu trợ trẻ em quốc tế cho thấy bên cạnh các môi trường gia đình, trường học và cộng đồng, môi trường mạng đang ngày càng có vai trò quan trọng đối với trẻ em.

Cụ thể, theo kết quả khảo sát, có tới 83,9% trẻ em tham gia khảo sát có sử dụng điện thoại, và tỷ lệ sử dụng mạng xã hội là 86,1%.

97% trẻ em tham gia khảo sát sử dụng điện thoại từ 1 giờ/ ngày, trong đó gần 27% sử dụng tới 5 giờ/ngày. Mục đích sử dụng lớn nhất là giải trí, chiếm tới 86%; trong khi tỷ lệ sử dụng cho học tập, tìm kiếm thông tin, giao lưu kết bạn lần lượt là 75%, trên 66% và trên 57%.

Một điểm đáng mừng của kết quả khảo sát Tiếng nói trẻ em Việt Nam 2024 là tỷ lệ trẻ em đã được học những nội dung/kĩ năng để bảo vệ bản thân trên môi trường mạng là khá cao. Các nội dung quan trọng đều có tỷ lệ trên 70%. Nội dung về phòng ngừa bắt nạt qua mạng xã hội thấp nhất cũng đạt 63.4%.

Tuy nhiên, tỷ lệ trẻ em tự học các kiến thức này qua mạng xã hội lại có tỷ lệ cao nhất trong các kênh thông tin. Đây có thể vừa là một điều tích cực, nhưng cũng hàm chứa nhiều rủi ro xuất phát từ việc là điều hạn chế vì lúc này nhận thức của trẻ em còn chưa đầy đủ, cũng như những thông tin, kiến thức trên mạng xã hội luôn luôn cần kiểm chứng về độ chính xác. Do đó, cần tăng cường các kênh thông tin khác, nhất là các thông tin từ trường học, vì hiện còn khá thấp, chỉ đạt 56%. Ngoài ra, cha mẹ cũng cần nâng cao kĩ năng về an toàn mạng để có thể đồng hành và hỗ trợ con mình trong tiến trình này, vì hơn một nửa trẻ tham gia khảo sát tìm hiểu kiến thức qua cha mẹ.



Biểu đồ 2: Tỷ lệ mục đích sử dụng Internet của trẻ em
(Nguồn: MSD)

Mục đích trẻ sử dụng internet

a) Tiếp cận thông tin, kiến thức, học tập

Trẻ em sử dụng Internet để tiếp cận, tìm kiếm thông tin kiến thức phục vụ học tập. Thông qua các trang web tìm kiếm thông tin trên Internet như Google, Bing có thể cung cấp cho trẻ em bất kỳ một thông tin nào mà người học mong muốn.

b) Kết nối, giao tiếp và chia sẻ

Trẻ em có thể sử dụng Internet để gửi mail, trò chuyện, kết nối bạn bè trên các trang mạng xã hội hoặc tham gia các lớp học trực tuyến.

c) Phát triển bản thân

Internet hỗ trợ trẻ em sáng tạo với vô vàn kiến thức có thể học tập như: lập trình, chơi các loại nhạc cụ, làm đồ chơi, nhảy múa, học nấu ăn…, tìm kiếm thông tin cần thiết không bị giới hạn thời gian và không gian, khám phá và trải nghiệm nhiều kiến thức, lĩnh vực mới.

d) Giải trí

Thông qua Internet, trẻ em có thêm nhiều nội dung giải trí như: trò chơi điện tử trực tuyến, các trang tin tức giải trí, phim trực tuyến ...

1.2. Bảo vệ trẻ em trên môi trường mạng

1.2.1. Rủi ro trên môi trường mạng với trẻ em

Rủi ro đối với trẻ em trên môi trường mạng là những yếu tố, hành vi tiêu cực, những nguy cơ mà trẻ em có thể gặp phải khi tham gia hoạt động trên môi trường mạng có khả năng tác động, gây tổn hại về thể chất, tình cảm, tâm lý, danh dự, nhân phẩm, quyền riêng tư của trẻ em khi tham gia hoạt động trên môi trường mạng.

Tương ứng với 6 đặc tính của Internet, người dùng, bao gồm cả trẻ em có thể tận hưởng các lợi ích hoặc có thể phải gặp phải các rủi ro trên môi trường mạng.

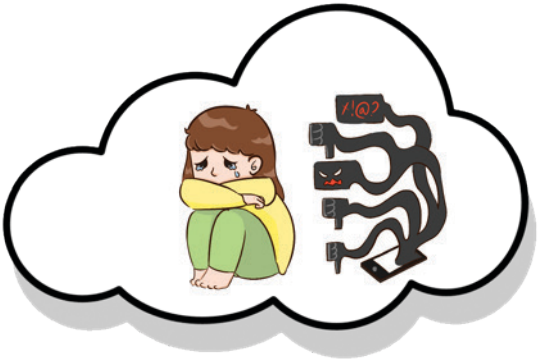
Ví dụ với đặc tính Ẩn danh của Internet, bất kỳ ai cũng có thể đăng ký tài khoản trên mạng và che giấu danh tính thật của mình. Chính vì thế, trẻ em có thể bị rủi ro kết bạn với người xấu mà không biết hoặc bị kẻ ẩn danh nói xấu, bắt nạt trực tuyến. Một ví dụ khác với đặc tính Nguồn thông tin, bất kỳ ai cũng có thể đăng tải và chia sẻ thông tin, chính vì thế, nguồn thông tin có thể không chính xác, hoặc tin giả khiến các người dùng trẻ tuổi của chúng ta chưa biết phân biệt. Ngoài ra, với đặc tính Vĩnh viễn, một khi các thông tin đã được đăng tải trên môi trường mạng, kể cả sau đó có bị xóa đi, các thông tin sẽ tồn tại vĩnh viễn. Chính vì thế, thông tin xấu về trẻ, sai lệch hoặc bị bắt nạt, hình ảnh nhạy cảm, ... một khi bị đưa lên mạng sẽ vẫn tồn tại dưới một dạng thức nào đó trên môi trường mạng.

Môi trường mạng có rất nhiều rủi ro tương ứng với các đặc tính của Internet, và luôn phát triển theo hướng nghiêm trọng và không lường hết được. Qua thống kê khảo sát và các kinh nghiệm, các rủi ro trẻ em thường gặp trên môi trường mạng bao gồm:

Tiếp cận thông tin không phù hợp, nội dung độc hại (bạo lực, thù địch, nội dung cực đoan, khiêu dâm, nội dung chưa xác thực từ các ứng dụng/công cụ AI…);

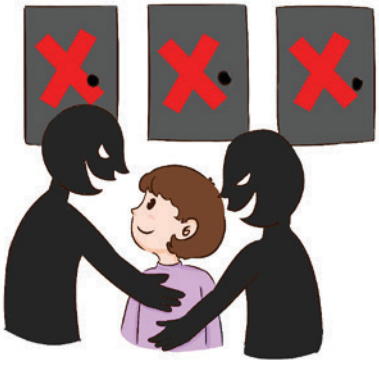
- Bị rò rỉ, lộ lọt thông tin bí mật đời sống riêng tư, bí mật cá nhân của trẻ em; đăng tải bí mật đời sống riêng tư, bí mật cá nhân của trẻ em mà chưa được sự đồng ý của cha, mẹ, người chăm sóc trẻ em và trẻ em theo quy định của pháp luật;

- Bắt nạt trực tuyến (hay còn gọi là "Bắt nạt trên mạng")



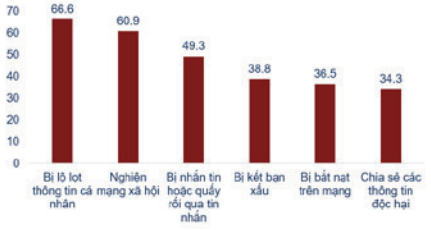
- Sử dụng quá mức gây nghiện (Nghiện Game, nghiện Internet, nghiện mạng xã hội)

- Bị lôi kéo, dụ dỗ, quấy rối, lừa đảo, dọa nạt, tống tiền, ép tham gia các hoạt động phi pháp, mại dâm, bị xâm hại tình dục:



Báo cáo Tiếng nói trẻ em Việt Nam của MSD chỉ ra các rủi ro mà trẻ em nhận thấy hay gặp nhất là các rủi ro liên quan đến bị lộ thông tin cá nhân, nghiện mạng xã hội, bị nhắn tin hoặc quấy rối qua tin nhắn, bị kết bạn xấu, ...

Biểu đồ 3. Tần suất cảm thấy an toàn khi sử dụng mạng

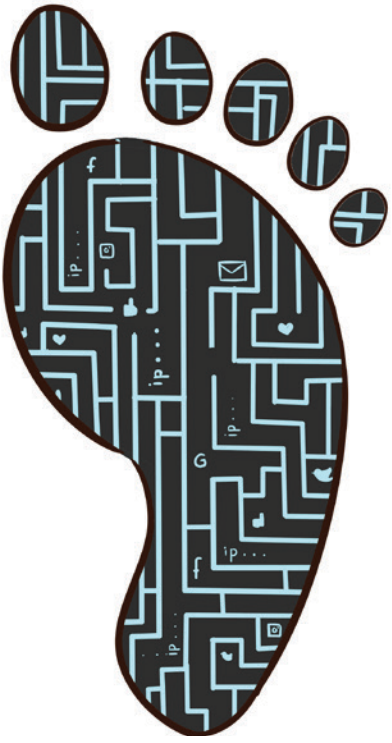


Biểu đồ 4. Trẻ đánh giá nguy cơ gặp phải khi sử dụng mạng

Ngoài ra, lưu ý rằng một khi trẻ em hay bất kỳ người dùng nào sử dụng Internet, tức là đã tham gia vào một xã hội, có danh tính số và dấu chân kỹ thuật số.

Danh tính số là những thứ cho người khác biết bạn là ai, là những thứ đặc biệt phân biệt bạn với những người khác, bao gồm:

- Thông tin cá nhân: Họ tên, ngày tháng năm sinh, số điện thoại, địa chỉ nhà, địa chỉ email,...
- Tính cách.
- Tín ngưỡng.
- Những thứ mà bạn theo đuổi.
- Sở thích riêng của bản thân.
- ...



Tất cả những thứ đó khi được đưa lên mạng Internet hoặc là đăng lên, chia sẻ lên mạng Internet, mạng xã hội,... tạo thành danh tính số.

Dấu chân kỹ thuật số là dấu vết người dùng để lại khi sử dụng Internet, như tin nhắn, email, hình ảnh và trò chuyện trực tuyến và hiện lên với mọi người dùng mạng. Giống như chúng ta đi để lại dấu chân, dấu chân kỹ thuật số khiến người khác có thể lần theo dấu vết của bạn.

Chính vì thế, việc danh tính số và dấu chân kỹ thuật số sẽ có thể quyết định trẻ em khi lên môi trường mạng sẽ có danh tính và dấu chân kỹ thuật số tích cực hay tiêu cực đồng thời có thể dễ gặp các rủi ro trên môi trường mạng hay không.

1.2.2. Biện pháp bảo vệ trẻ em trên môi trường mạng

Bảo vệ trẻ em trên môi trường mạng là thực hiện các biện pháp và hành động phù hợp để bảo đảm trẻ em được sử dụng môi trường mạng an toàn, lành mạnh, cụ thể:

- Phòng ngừa: Tuyên truyền, nâng cao nhận thức, trang bị kiến thức về bảo vệ trẻ em, xây dựng môi trường an toàn, giảm nguy cơ trẻ em bị xâm hại;

- Hỗ trợ: Kịp thời phát hiện, giảm, loại bỏ nguy cơ gây tổn hại cho trẻ em;

- Can thiệp: Ngăn chặn hành vi xâm hại, chăm sóc phục hồi, tái hòa nhập cộng đồng.

1.2.3. Mạng lưới ứng cứu, bảo vệ trẻ em trên môi trường mạng

Mạng lưới ứng cứu, bảo vệ trẻ em trên môi trường mạng (Viet Nam's Network for Child Online Protection (VN-COP)) là tổ chức phối hợp liên ngành giúp Bộ trưởng Bộ Thông tin và Truyền thông tăng cường hiệu lực, hiệu quả quản lý nhà nước và kết quả thực thi các nhiệm vụ phòng, chống xâm hại trẻ em trên môi trường mạng, góp phần nâng cao nhận thức xã hội và tạo lập một môi trường mạng an toàn, lành mạnh cho trẻ em.

Cục An toàn thông tin - Bộ Thông tin và Truyền thông là cơ quan điều phối Mạng lưới.

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) là cơ quan thường trực của Ban điều hành Mạng lưới.

Hotline: 0796863111.

Website: https://vn-cop.vn/

Mạng lưới có các chức năng, nhiệm vụ như sau:

① Đẩy mạnh truyền thông, góp phần nâng cao nhận thức xã hội về hoạt động bảo vệ trẻ em trên môi trường mạng.

② Tiếp nhận phản ánh, thu thập thông tin về các hành vi xâm hại trẻ em trên môi trường mạng.

3. Tổng hợp, phân loại và điều phối các thành viên Mạng lưới xử lý các phản ánh, thông tin về hành vi xâm hại trẻ em trên môi trường mạng.

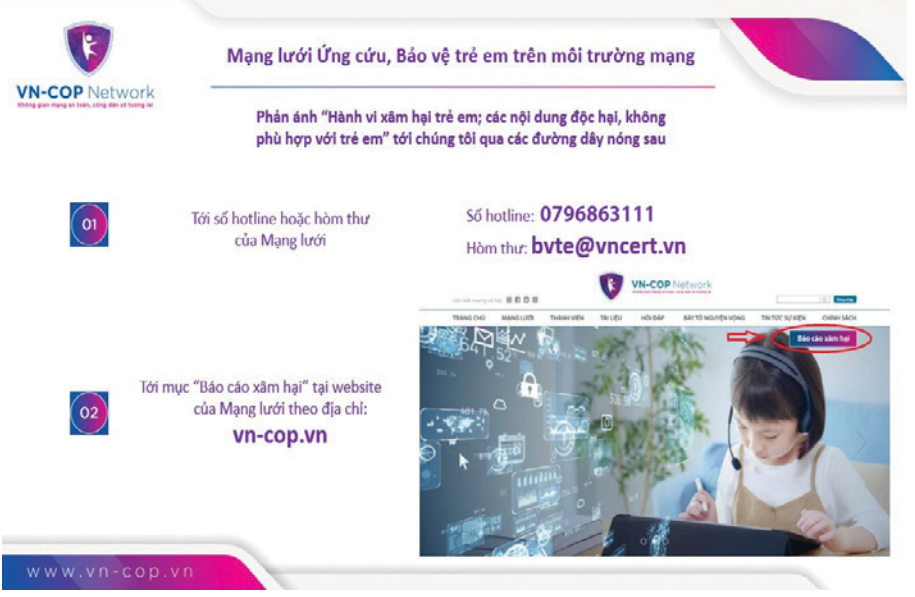
4. Thúc đẩy xây dựng hệ sinh thái các sản phẩm, nội dung lành mạnh, sáng tạo cho trẻ em trên môi trường mạng.

5. Tổ chức các hoạt động nâng cao năng lực, tập huấn, chia sẻ kinh nghiệm, hướng dẫn các biện pháp bảo vệ trẻ em trên môi trường mạng.

6. Ban hành, phổ biến và vận động thực hiện Bộ Quy tắc ứng xử, bảo vệ trẻ em trên môi trường mạng.

7. Kết nối với các mạng lưới bảo vệ trẻ em quốc tế nhằm nâng cao hình ảnh Việt Nam trong hoạt động bảo vệ trẻ em trên môi trường mạng.

8. Tư vấn, đề xuất chính sách, quy định về bảo vệ trẻ em trên môi trường mạng cho các cơ quan nhà nước có thẩm quyền.



1.2.4. Tổng đài điện thoại Quốc gia Bảo vệ Trẻ em (số 111)

Tổng đài điện thoại Quốc gia Bảo vệ Trẻ em là dịch vụ công đặc biệt thành lập theo quy định của Luật trẻ em năm 2016, chịu sự quản lý của Trung tâm Tư vấn và Dịch vụ Truyền Thông thuộc Cục Trẻ em - Bộ Lao động Thương binh và Xã hội, thực hiện các nhiệm vụ:

1. Bộ Lao động - Thương binh và Xã hội tiếp nhận thông báo, tố giác từ cơ quan, tổ chức, cơ sở giáo dục, gia đình, cá nhân qua điện thoại.

2. Liên hệ với các cá nhân, cơ quan, tổ chức có liên quan hoặc có thẩm quyền; khai thác thông tin trên phương tiện thông tin đại chúng, môi trường mạng về nguy cơ, hành vi xâm hại trẻ em để kiểm tra thông tin, thông báo, tố giác ban đầu.

3. Chuyển, cung cấp thông tin, thông báo, tố giác hoặc giới thiệu trẻ em có nguy cơ hoặc bị xâm hại, trẻ em có hoàn cảnh đặc biệt, cha, mẹ, người chăm sóc trẻ em tới các cơ quan, tổ chức, cá nhân có thẩm quyền, chức năng bảo vệ trẻ em.

4. Phối hợp với các cơ quan, tổ chức, cá nhân, cơ sở cung cấp dịch vụ bảo vệ trẻ em, cá nhân có thẩm quyền, chức năng bảo vệ trẻ em trong phạm vi toàn quốc để đáp ứng việc tiếp nhận, trao đổi, xác minh thông tin, thông báo, tố giác về trẻ em bị xâm hại hoặc có nguy cơ bị bạo lực, bóc lột, bỏ rơi.

5. Hỗ trợ người làm công tác bảo vệ trẻ em cấp xã trong việc xây dựng, thực hiện kế hoạch hỗ trợ, can thiệp đối với từng trường hợp trẻ em bị xâm hại hoặc có nguy cơ bị bạo lực, bóc lột, bỏ rơi; theo dõi, đánh giá việc xây dựng và thực hiện kế hoạch này.

6. Tư vấn tâm lý, pháp luật, chính sách cho trẻ em, cha, mẹ, thành viên gia đình, người chăm sóc trẻ em.

7. Lưu trữ, phân tích, tổng hợp thông tin để cung cấp, thông tin, thông báo, tố giác khi có yêu cầu của các cơ quan, tổ chức, cá nhân có thẩm quyền, đối với vụ việc xâm hại trẻ em và các cơ sở cung cấp dịch vụ bảo vệ trẻ em; thực hiện báo cáo định kỳ, đột xuất cho cơ quan quản lý nhà nước về trẻ em và các cơ quan khác có thẩm quyền, trách nhiệm về bảo vệ trẻ em.

1.2.5. Cách thức phản ánh nội dung độc hại, hành vi xâm hại trẻ em trên môi trường mạng

Ngay khi phát hiện nội dung độc hại, hành vi xâm hại đối với trẻ em trên kmôi trường mạng, người phát hiện cần thực hiện phản ánh ngay tới các đầu mối tiếp nhận cụ thể như sau:

1

Tổng đài Quốc gia Bảo vệ Trẻ em
Hotline: 111
Email: tongdaiquocgia111@gmail.com

2

Cơ quan Công an các cấp hoặc gọi
Hotline: 113

3

Mạng lưới ứng cứu bảo vệ trẻ em trên môi trường mạng
Hotline: 0796863111
Email: bvte@vncert.vn, website: vn-cop.vn, facebook.com/BVTE.VNCOP

1.2.6. Các quy tắc ứng xử cơ bản bảo vệ trẻ em trên môi trường mạng

Quy tắc ứng xử chung trên môi trường mạng:

1. Tuân thủ pháp luật Việt Nam về bảo vệ trẻ em, tôn trọng quyền và lợi ích hợp pháp của trẻ em, không gây tổn hại cho trẻ em trên nguyên tắc vì lợi ích tốt nhất của trẻ em.

2. Ứng xử lành mạnh, tích cực, phù hợp với văn hóa, thuần phong mỹ tục của Việt Nam và phù hợp với độ tuổi trẻ em trên môi trường mạng.

3. Không sử dụng các hình ảnh và bí mật đời sống riêng tư, bí mật cá nhân của trẻ em mà chưa được sự đồng ý của trẻ, cha, mẹ và người chăm sóc trẻ em; không sử dụng các hình ảnh và thông tin cá nhân của trẻ em cho các mục đích ảnh hưởng tới sự an toàn, phát triển lành mạnh của trẻ em.

4. Tích cực phối hợp với các cơ quan, tổ chức về bảo vệ trẻ em để ngăn chặn nội dung độc hại đối với trẻ em, xử lý các hành vi xâm hại trẻ em.

5. Khi nghi ngờ hoặc phát hiện các hành vi xâm hại trẻ em, nội dung độc hại đối với trẻ em cần khẩn trương phản ánh, tố giác tới một trong các cơ quan được đề cập tại mục 1.2.5 (trang 17,18).

Quy tắc ứng xử của trẻ em trên môi trường mạng:

Cẩn thận

Khi tham gia Internet, thận trọng trước khi chia sẻ các thông tin liên quan đến cá nhân của mình và người khác trên mạng xã hội.

Chia sẻ

Với bố mẹ, giáo viên, bạn bè, nhân viên bảo vệ trẻ em, những người tin tưởng khi có bất kỳ vấn đề nào cần đến sự hỗ trợ.

Quy tắc ứng xử của phụ huynh trên môi trường mạng:

Cùng

Đồng hành bảo vệ, lắng nghe che chở trẻ em khi trẻ gặp bất kỳ sự khó khăn nào, hướng dẫn trẻ em cách xử lý tình huống gặp phải phù hợp với độ tuổi.

Chú ý

Luôn chú ý, theo dõi, giám sát hoạt động của trẻ em khi trẻ tham gia môi trường mạng.

Câu hỏi thực hành

Câu hỏi thực hành 1: Bài tập nối từ: Hãy nối những mô tả sau về trò chơi điện tử gắn với các đặc tính của Internet

A. Công khai	1. Các máy chủ lưu trữ tất cả thông tin về việc chơi trò chơi trực tuyến của chúng ta
B. Vĩnh viễn	2. Chúng ta cần để ý tới cách chúng ta nói chuyện với những người chơi khác trên mạng và hãy tỏ ra lịch sự.
C. Kết nối	3. Chúng ta có thể không biết chúng ta đang chơi với ai trên mạng
D. Ẩn danh	4. Chúng ta có thể được nghe những thông tin không đúng sự thật trên mạng, như cách để vượt qua một cấp (level) nào đó, hacking vv.
E. Nguồn thông tin	5. Bất kỳ ai đều có thể chơi trò chơi và những người khác có thể nhìn thấy hành động của họ
F. Tôn trọng người khác	6. Chúng ta có thể kết nối và chơi với bất kỳ ai trên thế giới thông qua webcam hay tai nghe

Câu hỏi thực hành 2: Hãy kẻ bảng thực hành chia sẻ ít nhất 3 điều bạn thấy Internet có lợi và 5 điều Internet có hại đối với trẻ em

Lợi ích của Internet đối với trẻ em	***Rủi ro của Internet đối với trẻ em***

Câu hỏi thực hành 3: Con bạn đang ở độ tuổi nào? Hãy ghi chú vào đây những điều bạn mong muốn con mình sẽ ứng xử với mình như thế nào trong việc sử dụng Internet nhé!

Tên trẻ:.....

Độ tuổi:.....

Giai đoạn: A. 0 Internet B. Ươm mầm C. Phát triển D. Tiền trưởng thành

Mong muốn của bản thân:.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

PHẦN 2

GIAI ĐOẠN ƯƠM MẦM
(Trẻ em từ 0 - 6 tuổi)

2.1. Tâm sinh lý của trẻ ở độ tuổi 0 - dưới 6 tuổi

2.1.1. Giai đoạn 0 – dưới 3 tuổi

Ở giai đoạn này, trẻ em không cần và không nên tiếp xúc với các thiết bị kỹ thuật số dù với bất kỳ lý do gì. Đây là giai đoạn trẻ cần được sự quan tâm, yêu thương, tương tác thực tế, để phát triển ngôn ngữ, giao tiếp, vận động. Việc tiếp xúc thiết bị công nghệ giai đoạn này có thể gây ra hiện tượng mất cân bằng trong quá trình phát triển trí não của trẻ nhỏ. Trẻ tiếp cận nhiều thiết bị điện tử, tiếp xúc mạng quá sớm trong giai đoạn này có thể bị chậm phát triển ngôn ngữ, có các vấn đề về khả năng tập trung và phản xạ khi lớn lên.

2.1.2. Giai đoạn 3 – dưới 6 tuổi

Trong giai đoạn 3 – dưới 6 tuổi, trẻ khám phá thế giới xung quanh một cách nhanh chóng, tiếp xúc với xung quanh bằng các giác quan khác nhau, phát triển ngôn ngữ. Trẻ thích thú trong các hoạt động trò chơi, khám phá thế giới xung quanh và đặt các câu hỏi tại sao và bắt đầu đưa ra các ý kiến. Giai đoạn này cái tôi của trẻ được hình thành, trong quan hệ tình cảm trẻ tiến tới nhận ra vị trí của mình với mọi người. Đây được coi là độ tuổi vàng để phát triển trí tuệ, kỹ năng cho trẻ. Vì vậy, để trẻ phát triển toàn diện và vượt bậc trong giai đoạn này, người lớn cần nhiều thời gian tổ chức các hoạt động vui chơi, khám phá môi trường xung quanh thay vì việc dành thời gian cho trẻ tiếp xúc quá nhiều với các thiết bị công nghệ.

2.2. Những lưu ý dành cho trẻ khi gặp rủi ro

Trẻ em mẫu giáo thường gặp 2 loại rủi ro chính:

1. Tiếp cận thông tin không phù hợp, nội dung độc hại Những rủi ro này bao gồm:

- Những nội dung khiến trẻ cảm thấy bất an, sợ hãi, hoang mang. Ví dụ: phim hoạt hình có nội dung ma quái, chém giết hay khiêu dâm, hình ảnh tàn ác với động vật hoặc các nội dung chỉ thích hợp cho trẻ lớn hơn.

- Trẻ em bắt chước theo các hướng dẫn tiêu cực gây tổn hại cho bản thân và/hoặc làm tổn thương người khác. Ví dụ: bắt chước các trò chơi, thử thách nguy hiểm như trốn vào tủ lạnh, máy giặt, treo cổ, ... hay phá hủy trò chơi, ứng dụng của người khác tạo nên, ...

2. Rò rỉ, lộ, mất thông tin

Trẻ bị rò rỉ, lộ thông tin cá nhân do thói quen của bố mẹ hoặc người thân vô tình đăng tải thông tin bí mật riêng tư, bí mật đời sống cá nhân của trẻ mà chưa được phép; hoặc trẻ chấp nhận một cách vô thức vào các giao dịch hợp đồng trên mạng một cách không công bằng, hoặc chấp nhận các điều kiện mà trẻ không biết hoặc không hiểu. Ví dụ: trẻ có thể click (nhấp) vào đồng ý cho phép doanh nghiệp hay chủ các trang mạng truy cập vào dữ liệu của thiết bị trẻ đang sử dụng, hoặc gửi tới trẻ, gia đình các tài liệu không phù hợp.

2.3. Kỹ năng trẻ cần có

Kỹ năng lắng nghe và làm theo hướng dẫn – Kỹ năng báo cáo

Ở giai đoạn này, trẻ nên nghe theo mọi sự chỉ dẫn của cha mẹ và người chăm sóc trẻ. Tuyệt đối không được tự ý sử dụng, tham gia vào môi trường Internet một cách độc lập. Vì ở giai đoạn này trẻ chưa có nhiều nhận thức về các mối nguy hiểm đang rình rập trên môi trường mạng, do đó phụ huynh và người chăm sóc trẻ sẽ là người hướng dẫn và đồng hành cùng con để khám phá môi trường mạng trong giai đoạn này.

2.4. Những lưu ý dành cho phụ huynh và người chăm sóc trẻ để giáo dục trẻ ở độ tuổi dưới 6 tuổi

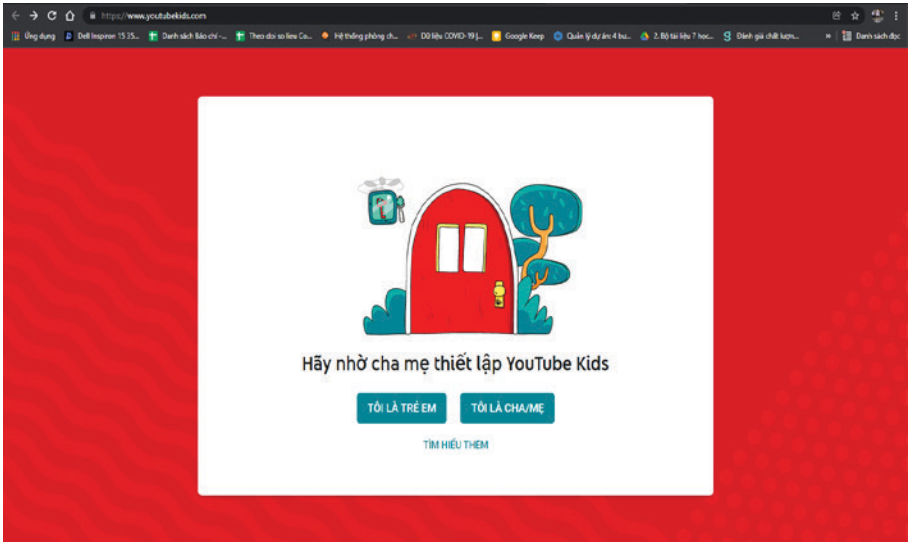
Ở độ tuổi này, trẻ chưa nên sử dụng Internet một cách độc lập. Chúng tôi khuyến cáo trong giai đoạn này, cha mẹ nên cùng trẻ xem các chương trình hoặc đảm bảo rằng những tương tác trên mạng và các chương trình trẻ xem đều nằm trong tầm mắt của bố mẹ, tránh tình trạng trẻ thoát khỏi tài khoản hoặc chẳng may các chương trình chặn, lọc của ứng dụng không đảm bảo, trẻ gặp phải các chương trình không phù hợp.

Chúng tôi khuyến nghị các kỹ năng sau cho trẻ nhỏ và phụ huynh cần được quan tâm:

a. Thiết lập tài khoản cho trẻ và xác định danh tính số của trẻ

- Trẻ em giai đoạn này bố mẹ có thể giúp lập các tài khoản trên mạng và kết nối với tài khoản của bố mẹ qua các chức năng kết nối theo dõi của phụ huynh. Việc lập tài khoản và khai báo độ tuổi của trẻ sẽ giúp các ứng dụng này phân loại và cung cấp nội dung phù hợp cho trẻ, cha mẹ cũng có thể thảo luận và cùng con xác định danh sách các chương trình mà con có thể xem phù hợp với

sở thích của trẻ. Cha mẹ hãy giúp trẻ nhận thức rằng đây là tài khoản của con để tăng tính sở hữu của trẻ, đảm bảo trẻ sẽ truy cập khi sử dụng Internet.



- Thiết lập một thư mục có dấu trang cho các ứng dụng hoặc trang web yêu thích của con để con có thể dễ dàng tìm thấy chúng. Phụ huynh có thể thiết lập các thư mục và dấu trang trên tất cả các thiết bị mà con bạn sử dụng. Nếu con có thêm chương trình nào muốn xem, hãy cùng thảo luận với cha mẹ. Phụ huynh cũng có thể kiểm tra xem các trò chơi, trang web và chương trình Tivi có phù hợp với trẻ em hay không thông qua các bài đánh giá trên Common Sense Media.

Cha mẹ tuyệt đối không lập cho con các tài khoản trên các ứng dụng khi con chưa đủ tuổi bằng cách khai báo sai tuổi hoặc sử dụng các thiết bị/tài khoản của bố mẹ để truy cập

b. Quản lý thời gian tiếp xúc với màn hình

Trẻ em độ tuổi 0-3 không nên tiếp xúc với màn hình dù là Tivi hay xem/chơi các chương trình trên Internet, trẻ từ 3-6 tuổi không nên tiếp xúc với màn hình dù là Tivi hay xem/chơi các chương trình trên Internet quá 1 giờ/ngày. Cha mẹ có thể cài đặt các ứng dụng để đảm bảo thời gian con xem không quá 1 giờ. Lưu ý rằng khi cài đặt thời gian, cha mẹ cũng nên giải thích trước với con để con hiểu rằng chỉ nên xem các chương trình này dưới 1 giờ/ngày để đảm bảo sức khoẻ cho con, kết thúc hoạt động này còn rất nhiều các hoạt động thú vị khác mà con có thể tham gia. Để tránh trẻ mè nheo, đòi hỏi và có thể khóc, sốc, khi kết thúc chương trình một cách đột ngột khi hết thời gian, cha mẹ có thể thông báo cho trẻ trước khi kết thúc chương trình từ 15 phút, 10 phút hoặc 5 phút để trẻ chuẩn bị chuyển trạng thái. Việc giúp trẻ tự giác trong việc thành lập thói quen giờ giấc, nền nếp sẽ giúp ích rất nhiều khi trẻ sử dụng Internet độc lập hơn ở các độ tuổi lớn hơn.

c. Quản lý an toàn thông tin và quyền riêng tư

Tài khoản của trẻ cần được cài đặt ở chế độ riêng tư, có thể hạn chế các nội dung và tương tác từ người lạ. Ngoài ra, phụ huynh có thể cài đặt về thời gian cũng như theo dõi dấu chân kỹ thuật số của trẻ, những hoạt động của trẻ trên môi trường mạng.

Kiểm tra cài đặt quyền riêng tư, sử dụng kiểm soát của phụ huynh, chặn mua hàng trong ứng dụng, tắt tùy chọn thanh toán bằng một cú nhấp chuột và dịch vụ định vị trên thiết bị và đồ chơi có kết nối Internet của bạn. Hạn chế các chức năng của máy ảnh và video quảng cáo - hãy thận trọng với các ứng dụng có các nhân vật trong phim hoặc các sản phẩm nổi tiếng, vì các ứng dụng này thường quảng cáo tiêu dùng và các sản phẩm cụ thể. Ngoài ra, hãy đọc và kiểm tra các điều khoản và điều kiện xem liệu các ứng dụng có thu thập dữ liệu không.

Tìm hiểu cách thức để báo cáo, chặn, ...

d. Quản lý hành vi rủi ro

Phụ huynh có thể bắt đầu giải thích cho con mình rằng có nội dung tốt và xấu trên Internet, bao gồm cả nội dung không đúng sự thật. Khuyến khích con nói chuyện với cha mẹ nếu chúng thấy điều gì đó khiến các con khó chịu, sợ hãi hoặc lo lắng. Ví dụ, cha mẹ có thể nói: "Một số video trên Internet có thể gây khó chịu hoặc đáng sợ. Hãy nói cho bố/mẹ biết nếu con thấy điều gì đó khiến con sợ hãi hoặc khiến con không vui nhé!".

e. Định hướng cho trẻ các nội dung phù hợp

Hãy chú ý tới độ tuổi của trẻ để định hướng cho con xem/chơi các chương trình có nội dung tốt, phù hợp với độ tuổi, sở thích, sự phát triển tâm sinh lý của trẻ, ngoài tránh rủi ro, cũng có thể quan tâm cả đến việc trẻ có thể xem các chương trình vô ích, mất thời gian như quảng cáo – tuy có thể không có hại một cách rõ ràng nhưng cũng không có lợi cho sự phát triển của trẻ.

Đây là các nội dung giúp cho trẻ học hỏi và phát triển, các ứng dụng hoặc trò chơi có chất lượng tốt cho trẻ có thể:

- **Khuyến khích trẻ phát triển ngôn ngữ.** Ví dụ: học thêm ngoại ngữ là tiếng Anh qua các chương trình, ứng dụng tiếng Anh dành cho trẻ mẫu giáo; học các bài hát; luyện cách phát âm, ...

- **Khuyến khích trẻ sáng tạo, giải quyết vấn đề.** Ví dụ: hướng dẫn trẻ vẽ tranh, xây dựng các cốt truyện, câu đố, phân biệt cách xử lý tình huống khi gặp các vấn đề như tai nạn thương tích trẻ nhỏ, phòng tránh xâm hại trẻ em, ...

- **Khám phá:** Khám phá các sở thích của trẻ như vẽ tranh, thiết kế thời trang, chơi một nhạc cụ, lập trình, lắp ráp, các môn STEM hoặc thí nghiệm an toàn với trẻ nhỏ, ...

f. Những lưu ý khác với cha mẹ khi đồng hành cùng con độ tuổi dưới 6 tuổi

- Hãy hướng dẫn trẻ không nên click/nhấp chuột vào các quảng cáo hay các thông báo lạ trên mạng mà hãy cho bố mẹ biết khi có bất kỳ bất thường nào xảy ra. Hãy cho trẻ biết rằng có nhiều trò chơi và ứng dụng có tính năng mua hàng trong ứng dụng cho những thứ như trang phục nhân vật và cấp độ mới, hãy nói với con "Trò chơi có thể đòi hỏi con mua thứ này thứ kia, nhưng chúng mình chưa có tiền, cũng chưa biết tiêu tiền, nên chúng ta không click chuột vào các đề nghị con mua váy công chúa hay robot hay gì đó nhé! Nếu con thấy nó hiện lên màn hình, hãy tới nói với bố mẹ".

- Noi gương: đảm bảo rằng cả cha mẹ và các thành viên khác trong gia đình – ví dụ anh chị lớn hơn cũng đều tuân theo các quy tắc an toàn Internet ở trong gia đình, ví dụ về quy tắc giờ giấc sử dụng hoặc hành vi, chương trình xem theo độ tuổi.

- Cha mẹ nên lập 1 kế hoạch giáo dục trẻ em về các kiến thức an toàn trên mạng Internet bao gồm các nội dung chính như: phân biệt nội dung tốt xấu, không click chuột vào các đường link lạ, xử lý tình huống khi con xem phải các nội dung khiến con lo sợ, bối rối, ... Hãy cùng lên mạng với con, chơi với con, bình luận và chia sẻ về các nội dung và cảm xúc về các chương trình con đã xem, đặt ra các tình huống, yêu cầu con chỉ cho bạn cách chơi 1 trò chơi mà con yêu thích, ... để con cảm thấy có không gian chia sẻ thoải mái. Hãy chắc chắn rằng con sẽ nói lại ngay với bố mẹ những cảm xúc của con khi xem/chơi trên Internet. Nếu con xem phải các chương trình không phù hợp, hãy an ủi con và hướng dẫn con, đừng đổ lỗi và mắng trẻ khiến trẻ chưa hiểu được vấn đề và sẽ không dám tìm kiếm sự trợ giúp của bố mẹ khi cần.

Câu hỏi thực hành

Câu hỏi thực hành 4: Trẻ từ 0 - dưới 3 tuổi được khuyến cáo sử dụng Internet như thế nào:

A. Dưới 1giờ/ngày
C. Không có giới hạn
B. Dưới 2 giờ/ngày
D. Không nên sử dụng

Câu hỏi thực hành 5: Trẻ em dưới 6 tuổi thường gặp các loại rủi ro gì? (Có thể chọn nhiều đáp án)

A. Xem các nội dung không phù hợp

B. Bị tiếp xúc, kết bạn bởi những người không quen biết

C. Sử dụng tài khoản của người lớn

D. Click chuột vào các đường link làm mất thông tin cá nhân

E. Bắt chước theo các trò chơi trên mạng, có cả các trò rất nguy hiểm như nấp trong máy giặt, uống nước xà phòng, treo cổ, nhảy từ trên cao xuống, v.v.

Câu hỏi thực hành 6: Một số các biện pháp Cha mẹ nên làm để đồng hành cùng con giai đoạn Ươm mầm (Có thể chọn nhiều đáp án)

A. Cùng con xem các chương trình.

B. Lập chung danh mục phim bố mẹ và con cùng thích bao gồm cả phim trẻ con và phim người lớn cho bố mẹ.

C. Bắt con tắt ngay chương trình khi hết thời gian xem (1 giờ đồng hồ).

D. Hỏi han con xem cảm xúc của con khi xem mỗi chương trình như thế nào.

E. Cho con tuỳ ý xem Youtube.

F. Lập tài khoản của con theo tuổi bố mẹ cho dễ sử dụng.

G. Tịch thu thiết bị công nghệ khi con xem chương trình không phù hợp.

H. Đặt ra một số tình huống và hỏi con tình huống an toàn hay không an toàn để con có tư duy phản biện phân tích.

PHẦN 3

GIAI ĐOẠN PHÁT TRIỂN
(Trẻ em từ 6 - dưới 11 tuổi)

3.1. Tâm sinh lý của trẻ ở độ tuổi 6 - dưới 11 tuổi

Hoạt động chủ yếu của trẻ ở giai đoạn này là học tập, bắt đầu có tư duy, trẻ phát triển ngôn ngữ vượt trội. Đây cũng là độ tuổi hình thành nếp sống, thói quen, những hành vi có ý thức, tuân thủ theo các quy định tại gia đình, nhà trường, xã hội. Từ quan hệ ruột thịt, trẻ đã bắt đầu dần dần chuyển sang các mối quan hệ xã hội. Trẻ có sự thay đổi môi trường sống, không phải chỉ là môi trường gia đình quen thuộc như trước đây mà còn tiếp xúc với thầy cô, bạn bè.

Ở độ tuổi này, trẻ cũng có nhu cầu độc lập lớn hơn trong việc sử dụng Internet, bắt đầu nhận định về sự riêng tư, có khả năng để học tập và nhận định phân biệt đúng và sai, an toàn và không an toàn. Trẻ vẫn có nhu cầu hỗ trợ và hướng dẫn, nhận lời khuyên từ cha mẹ về các vấn đề mà trẻ gặp phải trong cuộc sống hay trên môi trường mạng.

3.2. Những lưu ý dành cho trẻ khi gặp rủi ro và cách phòng tránh

Ở độ tuổi này trẻ có thể gặp một hoặc một số rủi ro sau khi tham gia môi trường mạng. Khi gặp các rủi ro này, hãy áp dụng một số biện pháp phòng tránh được gợi ý dưới dây:

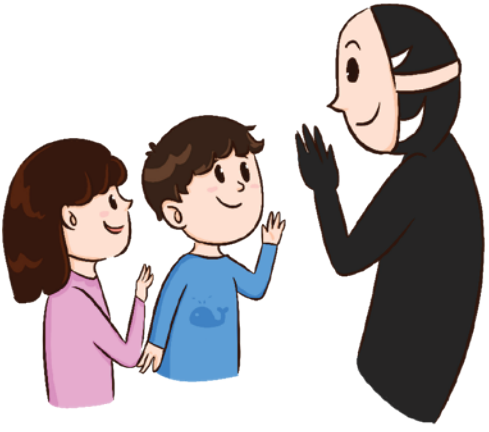
a. Rò rỉ, lộ lọt thông tin cá nhân

Nguyên nhân	Cách phòng tránh, xử lý, ngăn chặn
- Bị lộ mật khẩu hoặc mật khẩu quá dễ đoán; - Sử dụng phần mềm/ứng dụng không có bản quyền; - Chia sẻ ảnh/thông tin cá nhân công khai trên mạng; - Kết bạn với cả những người mình không quen biết, không đáng tin cậy; - Bị mất hoặc bị ăn cắp thiết bị, bị hack (lấy cắp) hoặc nhiễm phần mềm độc hại; - Do bạn bè, người thân sơ ý cung cấp. 	- Đặt mật khẩu mạnh: Sử dụng mật khẩu khó đoán, có ít nhất 8 ký tự, kết hợp số, chữ in hoa và cả in thường, và ký tự đặc biệt; - Thiết lập cảnh báo đăng nhập và bảo vệ 2 lớp; - Đăng nhập an toàn: Không nên đăng nhập vào tài khoản của mình ở các thiết bị công cộng, không nên lưu mật khẩu khi đăng nhập các thiết bị/trình duyệt công cộng; - Cài đặt riêng tư: Kích hoạt các tính năng giới hạn việc gợi ý, bật tính năng chặn lọc theo độ tuổi (nếu có) trên cài đặt của ứng dụng, nền tảng xã hội để hạn chế việc kết bạn, gắn thẻ, nhắn tin, chế độ người xem, ... - Kích hoạt tính năng kết nối với cha mẹ (nếu có) để cha mẹ có thể hỗ trợ mình ngay khi cần thiết; - Quản lý cookie thông qua phần cài đặt của trình duyệt web - như Firefox, Chrome, Safari hoặc Internet Explorer. Tùy thuộc vào trình duyệt, có thể xóa các cookie và chặn một số hoặc tất cả chúng; - Sử dụng các phần mềm có bản quyền và bảo mật; - Kết nối có chọn lọc: Nếu ai đó kết bạn với bạn mà bạn không rõ là ai hoặc nghi ngờ mình không quen, hãy từ chối và chặn người đó, hoặc hỏi ý kiến bố mẹ; - Tuyệt đối không chia sẻ thông tin và hình ảnh riêng tư trên mạng.

b. Tiếp cận các thông tin không phù hợp, nội dung độc hại

Dấu hiệu nhận biết thông tin không phù hợp, nội dung độc hại	Cách phòng tránh, xử lý, ngăn chặn
- Không phù hợp với lứa tuổi, dành cho trẻ em trên 11 tuổi; - Có thể có hình ảnh khiêu dâm, bạo lực, phát ngôn thù ghét, chửi rủa; - Hình ảnh, video, trò chơi bạo lực; - Hình ảnh hay nội dung, quảng cáo cờ bạc, cá cược; - Lôi kéo bạn thực hiện các thử thách không an toàn hoặc nguy hiểm, gây hại. 	- Nhanh chóng đóng trang lại hoặc thoát khỏi ứng dụng; - Tuyệt đối không bắt chước ngay các thử thách, nội dung trên môi trường mạng trước khi hỏi ý kiến bố mẹ, thầy cô hoặc người lớn mà bạn tin tưởng; - Chặn những người chia sẻ hoặc những trang có nội dung không phù hợp; - Trao đổi ngay với cha mẹ, thầy cô hoặc một người lớn mà các bạn tin tưởng về chuyên đã xảy ra, cảm giác của bạn và lắng nghe lời khuyên của người lớn; - Cùng người lớn báo cáo nội dung không phù hợp với các nhà cung cấp dịch vụ. Ví dụ như YouTube có ngay nút "cảnh báo/flags", "báo cáo/ report" ngay bên cạnh nội dung. Hoặc liên hệ tới các kênh phản ánh nội dung độc hại, thông tin không phù hợp được đề cập tại mục 1.2.5 (trang 17, 18)

c. Bị kết bạn xấu

Kết bạn xấu	Cách phòng tránh, xử lý, ngăn chặn
- Các bạn có thể kết bạn và liên lạc với các người bạn này thông qua email, tài khoản chơi trò chơi điện tử, mạng xã hội, ... Do tính chất ẩn danh của Internet, bạn có thể trót kết bạn với bạn xấu mà bạn không biết; -Đôi khi bạn tưởng kết bạn với người quen nhưng có thể đó là những tài khoản giả mạo mà bạn không nhận ra. Trên mạng, hãy nhớ chúng ta rất khó xác định được danh tính thật xem có đúng người kết bạn trên mạng với bạn có đúng là người em đã quen thân ngoài đời hay không. Kẻ xấu có thể sẽ đánh cắp thông tin, hình ảnh cá nhân của bạn, lừa đảo, bắt nạt, nói xấu, đe dọa hay lôi kéo bạn, thậm chí có thể tìm cách quấy rối, xâm hại bạn.	- Vô hiệu hoá tính năng đề xuất kết bạn của người mà bạn không có liên hệ; - Hãy chia sẻ với bố mẹ về danh sách bạn bè của mình và kể chuyện những bạn bè này để bố mẹ biết hoặc kiểm tra thông tin; - Trong khi tương tác, nói chuyện với bạn bè trên mạng, dù quen hay chưa quen lắm, nếu cảm thấy có sự kỳ lạ, làm bạn khó chịu hoặc sợ hãi, hãy chuyển chủ đề, dừng nói chuyện, hủy kết bạn và nói ngay với cha mẹ, thầy cô hoặc người lớn. 

d. Bắt nạt trực tuyến

"Bắt nạt trực tuyến" là hành vi quấy rối, đe dọa hoặc làm nhục người khác diễn ra trên môi trường mạng. Bắt nạt trực tuyến có thể xảy ra thông qua tin nhắn, các ứng dụng trên mạng, mạng xã hội, diễn đàn hoặc các trò chơi trực tuyến nơi mọi người có thể xem, tham gia hoặc chia sẻ nội dung.

Hình thức bắt nạt trực tuyến	Cách phòng tránh, xử lý, ngăn chặn
Bắt nạt trên môi trường mạng bao gồm các hành vi như: chê bai, loại trừ, quấy rối, rình rập, lừa tình, mạo danh, trêu chọc,... Những nơi thường xảy ra bắt nạt trực tuyến là: - Mạng xã hội như Facebook, Instagram, Snapchat và Tik Tok. - Ứng dụng nhắn tin và nhắn tin văn bản trên thiết bị di động hoặc máy tính bảng. - Nhắn tin trực tiếp và trò chuyện trực tuyến qua internet. - Diễn đàn, phòng trò chuyện và bảng tin trực tuyến, chẳng hạn như Reddit. - Email. - Cộng đồng chơi game trực tuyến	- Cài đặt lại quyền riêng tư nếu cần để không phải bạn nào cũng liên lạc được với bạn; - Chặn/báo cáo tài khoản người bắt nạt mình nếu tình trạng đó tiếp tục diễn ra; - Trao đổi với cha mẹ, thầy cô hoặc người lớn để được hỗ trợ nếu bản thân hoặc chứng kiến hành động bắt nạt; - Tuyệt đối không tham gia các hoạt động bắt nạt trực tuyến.

e. Bị xâm hại tình dục trên không gian mạng (môi trường mạng)

Các hành vi xâm hại tình dục trên môi trường mạng	Cách phòng tránh, xử lý, ngăn chặn
- Gửi cho trẻ em các nội dung phim, ảnh, trang web, nghe âm thanh, câu chuyện khiêu dâm hoặc liên quan tới tình dục qua điện thoại hoặc tin nhắn, email, mạng xã hội, ...; - Dụ dỗ, lôi kéo, ép buộc trẻ em khỏa thân và phát trực tiếp âm thanh, hình ảnh qua môi trường mạng; - Trẻ em bị sử dụng hình ảnh quay cơ thể phát tán trên mạng xã hội, các diễn đàn, các trang web khác nhau; - Bị bắt hoặc cho trẻ xem các hoạt động trình diễn khiêu dâm trực tuyến. 	- Giới hạn quyền riêng tư, đặt hạn chế người lạ xem danh sách bạn bè; - Tuyệt đối đừng bao giờ chia sẻ thông tin cá nhân hay hình ảnh, video bộ phận riêng tư của mình trên môi trường mạng; - Nếu ai đó yêu cầu bạn gửi thông tin cá nhân hay, hình ảnh hay clip bộ phận riêng tư hoặc thực hiện các hành vi xâm hại tình dục trẻ em như ô bên cạnh, hãy ngay lập tức hủy kết bạn, chặn, báo cáo tài khoản của người này và báo ngay với cha mẹ, thầy cô hoặc phản ánh nội dung độc hại tới các kênh phản ánh được đề cập tại mục 1.2.5 (trang 17,18).

3.3. Kỹ năng trẻ cần có

1	2	3	4
Quản lý danh tính số	**Quản lý quyền riêng tư**	**Quản lý thời gian tiếp xúc màn hình**	**Quản lý rủi ro**
Nhận biết danh tính số an toàn.	Biết quản lý thông tin mật khẩu: đặt mật khẩu mạnh; không chia sẻ với người ngoài.	Tuân thủ thời gian tiếp xúc màn hình theo kế hoạch được lập.	Nhận biết được các rủi ro có thể xảy ra khi tham gia môi trường mạng như: rò rỉ, lộ lọt thông tin cá nhân; tiếp cận các thông tin không phù hợp, nội dung độc hại; bị kết bạn xấu; bắt nạt trực tuyến; bị xâm hại tình dục trên môi trường mạng. Biết cách báo cáo hoặc nhờ sự hỗ trợ của người thân xử lý khi có rủi ro.

3.4. Những lưu ý dành cho phụ huynh cần nắm để giáo dục trẻ ở độ tuổi từ 6 - dưới 11 tuổi

☞ **Nói về việc sử dụng Internet và các rủi ro trực tuyến với con:**

Trẻ em ở độ tuổi này đã bắt đầu có khả năng học tập, ghi nhớ và dần hình thành các kỹ năng tư duy, kỹ năng xử lý tình huống rồi nên cha mẹ hãy sẵn sàng nói chuyện cởi mở với con cái về việc sử dụng Internet.

Đồng hành trên Internet với con từ sớm, bạn có cơ hội cùng giáo viên hướng dẫn con cách sử dụng Internet cũng như các rủi ro con có thể gặp phải, hướng dẫn, giải thích cho con. Đối với các bạn nhỏ trên 9 tuổi, cha mẹ có thể giao cho con các bài tập tìm hiểu về rủi ro trên mạng Internet và cách phòng tránh để thuyết trình, chia sẻ/dạy lại cha mẹ, như vậy các con có thể tự tìm hiểu, và làm chủ kiến thức của mình.

Cha mẹ hãy kể với con cách bạn sử dụng Internet, lợi ích và rủi ro, các trải nghiệm vui và cả không vui để giúp con cảm thấy rằng con có thể chia sẻ với cha mẹ về những gì con trải nghiệm không tốt trên mạng.

Hãy cho con biết không phải tất cả các thông tin trực tuyến đều đúng và hữu ích, khuyến khích con đặt câu hỏi, cùng con đặt ra các tình huống và cùng bố mẹ tìm cách giải quyết giúp tăng cường tư duy phản biện, và kỹ năng xử lý tình huống của con khi có các rủi ro xảy ra.

☞ **Hướng dẫn và áp dụng các phương pháp phòng tránh rủi ro Internet cho trẻ em được mô tả trong mục 3.2**

☞ **Xây dựng một kế hoạch sử dụng Internet an toàn trong gia đình**

Đó có thể là bản thỏa thuận để mọi thành viên trong gia đình tuân thủ về các điều khoản như:

- Không tiết lộ các thông tin cá nhân của mình cũng như của bố mẹ cho bất kỳ ai;

- Không chia sẻ ảnh, video clip của bản thân và gia đình cho bất cứ ai nếu chưa có sự cho phép của bố mẹ. Bố mẹ cũng không được chia sẻ hình ảnh, thông tin của con, dù là khoe bảng thành tích của con nếu không có sự cho phép của con;

- Con sẽ nói với bố mẹ ngay lập tức nếu có điều gì khiến con cảm thấy kỳ lạ, lo lắng, khó chịu. Bố mẹ sẽ không trách mắng, đổ lỗi cho con mà sẽ nghiêm túc cùng con tìm hiểu chuyện gì đã xảy ra, nguyên nhân và giải pháp;

- Con sẽ chia sẻ với bố mẹ danh mục các chương trình con muốn xem, danh sách bạn bè con muốn kết bạn. Bố mẹ hãy đảm bảo sẽ tôn trọng bạn bè và các sở thích của con, hỗ trợ tư vấn cho con về các chương trình phù hợp với con;

- Quy định thời gian sử dụng Internet của con và bố mẹ là: Sử dụng bao lâu? Vào lúc nào?

- Không sử dụng Internet khi đang ăn hoặc trong phòng ngủ, khi đang nói chuyện và chơi với nhau;

- Các điều khoản khác có sự thảo luận và nhất trí của tất cả các thành viên trong gia đình.

Bản kế hoạch/cam kết này nên được cả trẻ và bố mẹ ký nhận, dán tại nơi sử dụng Internet của gia đình và được theo dõi việc thực hiện. Cha mẹ hãy đảm bảo làm gương cho trẻ nếu muốn trẻ có thể xây dựng các thói quen sử dụng Internet hợp lý, an toàn.

☞ Cài một số ứng dụng để hạn chế, theo dõi, giám sát trẻ

Phụ huynh có thể cài đặt một số ứng dụng để hạn chế, theo dõi, giám sát trẻ (tham khảo các ứng dụng được đề cập tại Phần 5) nhưng tốt nhất không nên bí mật theo dõi trẻ - điều này sẽ khiến con nghĩ rằng bạn không tin tưởng con.

Tốt hơn hết nên nói chuyện cởi mở về việc sử dụng Internet của riêng bạn và khuyến khích con bạn làm điều tương tự, nếu cài đặt các ứng dụng, hãy cho con biết và nhận được sự đồng ý của con. Hãy cho con biết nếu cần cài đặt, đó là vì bạn đang nỗ lực giúp

con an toàn. Tuy nhiên, đối với trẻ trên 9 tuổi, cha mẹ thay vì cài đặt, giám sát nên hướng dẫn trẻ tự bảo vệ bản thân, bởi nếu trẻ muốn tránh sự giám sát của cha mẹ, trẻ có thể học cách gỡ hoặc vô hiệu hóa các ứng dụng cha mẹ cài đặt hoặc không sử dụng máy tính, tài khoản bố mẹ cài đặt mà lập tài khoản mới, sử dụng thiết bị công nghệ khác ở trường hoặc của bạn bè mà không cho cha mẹ biết.

- Hãy cho trẻ em hiểu rằng: Cha mẹ sẽ không đổ lỗi cho con nếu con gặp phải các rủi ro trên môi trường mạng, luôn có thể có giải pháp nếu con cho cha mẹ biết. Nếu cần thiết, trẻ và gia đình có thể liên hệ phản ánh nội dung độc hại, hành vi xâm hại tới các kênh phản ánh tại mục 1.2.5 (trang 17,18).

Câu hỏi thực hành

Câu hỏi thực hành 7: Trong các mật khẩu sau đây, đâu là mật khẩu mạnh?

A. 123456

B. VanBin1808

C. @Antoan_8456#

D. @ThiBong_2209

Câu hỏi thực hành 8: Một số các biện pháp cha mẹ nên làm để đồng hành cùng con giai đoạn Phát triển (Có thể chọn nhiều đáp án)

A. Hướng dẫn con lập tài khoản và các mật khẩu mạnh

B. Cho con vào tài khoản của bố mẹ để dùng chung cho nhanh và bố mẹ dễ kiểm soát

C. Lập thời gian biểu sử dụng Internet của cả gia đình và nghiêm túc thực hiện

D. Hỏi han con xem cảm xúc của con khi xem mỗi chương trình như thế nào

E. Mắng mỏ con vì để bạn bè đăng hình nói xấu con và gia đình trong tin nhắn của lớp

F. Tịch thu thiết bị công nghệ khi con xem chương trình không phù hợp

G. Đặt ra một số tình huống và hỏi con tình huống an toàn hay không an toàn để con có tư duy phản biện phân tích

Câu hỏi thực hành 9: Buổi tối, quan sát thấy con đang rất buồn và lo lắng, ăn ít cơm, cha mẹ mới hỏi Bông: Bông sao thế? Ở trường có chuyện gì buồn hả con? Bông trả lời: "Ở trong lớp con (lớp 3B), có 1 nhóm bạn ABC bảo con là béo ú xấu nhất lớp, các bạn gửi tin nhắn cho các bạn trong lớp hình con heo và ghi chú "Đây là Bông", con rất

buồn". Nếu bạn là cha mẹ của Bông, bạn sẽ làm thế nào?

PHẦN 4

GIAI ĐOẠN TIỀN TRƯỞNG THÀNH (Trẻ em từ 11 - dưới 16 tuổi)

4.1. Tâm sinh lý của trẻ ở độ tuổi 11 - dưới 16 tuổi

Trẻ ở độ tuổi thiếu niên (teen) có nhu cầu khẳng định bản thân, nhạy cảm với những đánh giá của mọi người xung quanh. Quan hệ xã hội của trẻ em giai đoạn này chuyển mạnh từ mối quan hệ gia đình sang nối quan hệ bạn bè, có nhu cầu độc lập. Chính vì thế, trước các vấn đề các em có thể tự nghĩ cách đối diện, giải quyết hoặc tham khảo ý kiến bạn bè trước khi tìm kiếm sự trợ giúp của người lớn bao gồm cha mẹ và thầy cô. Các em cũng mong muốn người lớn tôn trọng ý kiến của mình.

Ở độ tuổi này, các em thường chưa thực sự nhận thức được hết mặt tốt xấu ngoài xã hội, nhưng cũng không muốn thừa nhận việc thiếu sót trong kỹ năng, và có thể thể hiện việc che giấu hoặc chống đối. Tuy nhiên, ở độ tuổi này, trẻ vẫn sẵn sàng dành thời gian cho cha mẹ, thầy cô dù hạn chế hơn. Chính vì thế, các em cần sự quan tâm hỗ trợ, đồng hành một cách có trách nhiệm, nhạy cảm và tôn trọng các em từ cha mẹ và thầy cô để định hướng các em tự đánh giá, tìm giải pháp xác định hình thành nhân cách và quan điểm thái độ phù hợp khi trưởng thành. Chính vì thế, thiếu niên thường muốn độc lập, muốn thể hiện bản thân nhưng chưa đủ nhận thức đầy đủ để phân biệt tốt xấu.

Đối với việc sử dụng Internet, đây là giai đoạn thiếu niên có thể phát triển kỹ năng vượt trội khi sử dụng Internet, tự hình thành các kỹ năng số của bản thân. Trẻ bắt đầu độc lập khỏi cha mẹ và tự có các hành vi, ứng xử trên môi trường mạng, trước khi bước sang giai đoạn hình thành các kỹ năng trưởng thành.

4.2. Những lưu ý dành cho trẻ khi gặp rủi ro và cách phòng tránh

Ở độ tuổi này trẻ có thể gặp một hoặc một số rủi ro sau khi tham

gia môi trường mạng. Khi gặp các rủi ro này, hãy áp dụng một số biện pháp phòng tránh được gợi ý dưới dây:

a. Rò rỉ, lộ lọt thông tin cá nhân

Nguyên nhân	Cách phòng tránh, xử lý, ngăn chặn
- Bị lộ mật khẩu hoặc mật khẩu quá dễ đoán; - Sử dụng phần mềm/ứng dụng không có bản quyền; - Chia sẻ ảnh/thông tin cá nhân công khai trên mạng; - Kết bạn với cả những người mình không quen biết, không đáng tin cậy ; - Bị mất hoặc bị ăn cắp thiết bị, bị hack (lấy cắp) hoặc nhiễm phần mềm độc hại; - Do bạn bè, người thân sơ ý cung cấp. 	- Đặt mật khẩu mạnh: Sử dụng mật khẩu khó đoán, có ít nhất 8 ký tự, kết hợp số, chữ in hoa và cả in thường, và ký tự đặc biệt; - Thiết lập cảnh báo đăng nhập và bảo vệ 2 lớp; - Đăng nhập an toàn: Không nên đăng nhập vào tài khoản của mình ở các thiết bị công cộng, và "lưu mật khẩu" khi đăng nhập; - Cài đặt riêng tư: Kích hoạt các tính năng giới hạn việc gợi ý, bật tính năng chặn lọc theo độ tuổi (nếu có) trên cài đặt của ứng dụng, nền tảng xã hội để hạn chế việc kết bạn, gắn thẻ, nhắn tin, chế độ người xem, danh sách bạn bè...; - Kích hoạt tính năng kết nối với cha mẹ (nếu có) để cha mẹ có thể hỗ trợ mình ngay khi cần thiết; - Quản lý cookie thông qua phần cài đặt của trình duyệt web - như Firefox, Chrome, Safari hoặc Internet Explorer. Tùy thuộc vào trình duyệt, có thể xóa các cookie và chặn một số hoặc tất cả chúng; - Sử dụng các phần mềm có bản quyền và bảo mật; - Kết nối có chọn lọc: Nếu ai đó kết bạn với bạn mà bạn không rõ là ai hoặc nghi ngờ mình không quen, hãy từ chối và chặn người đó, hoặc hỏi ý kiến bố mẹ; - Tuyệt đối không chia sẻ thông tin và hình ảnh riêng tư trên mạng.

b. Lừa đảo trên mạng

Lừa đảo trên mạng là những hành vi kẻ có ý đồ xấu cố tình dùng các cách thức khác nhau để người dùng, bao gồm cả trẻ em trên môi trường mạng tin và thực hiện theo để đạt được ý đồ của kẻ lừa đảo.

Các hành vi lừa đảo	Cách phòng tránh, xử lý, ngăn chặn
- Hành vi lừa đảo hay tấn công giả mạo: Lừa đảo hoặc dụ dỗ bạn chia sẻ thông tin đăng nhập hoặc các thông tin cá nhân khác trên mạng. Hành vi lừa đảo được thực hiện qua email, mạng xã hội, tin nhắn, quảng cáo hoặc các trang web trông giống những trang web thật từng được sử dụng nhưng lại là giả; - Lừa đảo tiền hoặc thông tin: Lừa người khác chia sẻ thông tin đăng nhập, thông tin cá nhân, thông tin liên hệ, ... hoặc lừa người khác chuyển tiền hoặc tài sản kỹ thuật số của họ; - Giả mạo danh tính: Giả danh hoặc tạo tài khoản giả trên mạng để lừa người khác kết bạn hoặc chia sẻ thông tin cá nhân; - Tin giả: Tin tức lừa đảo hoặc bóp méo sự thật (hiện còn được gọi là "fake news"– "tin tức giả mạo").	- Luôn bảo đảm bí mật thông tin cá nhân không bị rò rỉ, lộ lọt, đánh cắp; - Luôn kiểm tra website cũng như thông tin, uy tín của nhà cung cấp trước khi làm theo hướng dẫn, thực hiện các giao dịch trực tuyến; - Kiểm chứng thông tin; - Thông báo chia sẻ với người thân, bạn bè hoặc thầy cô để được tư vấn, giúp đỡ; - Báo cáo, gọi điện thoại phản ánh theo một trong các hình thức tại 1.2.5 (trang 17,18). 

c. Nghiện Internet

Nghiện Internet là hành vi sử dụng Internet quá mức (sử dụng hơn 38 giờ/tuần và có 5/8 dấu hiệu bị lệ thuộc hành vi và cảm xúc vào Internet). Nghiện Internet hay sử dụng Internet quá mức rất có hại tới trẻ em, khiến cho trẻ: tâm trạng bất ổn; không thể tập trung; ảnh hưởng não bộ và trí nhớ bị giảm sút; ảnh hưởng sức khỏe thể chất và rối loạn giấc ngủ; trầm cảm, rối loạn hành vi.

Dấu hiệu nghiện Internet	Cách phòng tránh, xử lý, ngăn chặn
- Bận tâm với Internet khi luôn nghĩ về hoạt động online của mình ở lần trước hay các lần sắp tới; - Nhu cầu gia tăng thời gian sử dụng Internet; - Nhiều lần thất bại khi cố gắng kiểm soát, giảm bớt hoặc ngưng sử dụng Internet; - Bồn chồn, ủ rũ, buồn phiền hoặc dễ cáu kỉnh khi cố gắng giảm hoặc ngưng sử dụng Internet; - Online trên mạng trong thời gian nhiều hơn so với dự định ban đầu; - Hủy hoại hoặc nguy cơ mất mối quan hệ quan trọng, cơ hội học tập vì Internet; - Nói dối những người trong gia đình, nhà trị liệu hoặc người khác để che giấu mức độ bị cuốn hút vào Internet; - Sử dụng Internet như cách thức để tạm tránh đối diện với những vấn đề khó khăn trong cuộc sống hay cảm xúc khó chịu như lo lắng, thất vọng, mặc cảm.	- Trò chuyện, thảo luận với bố mẹ về kế hoạch sử dụng Internet phù hợp; - Tham gia các hoạt động thể thao, đi du lịch, cùng nấu ăn, ...; thiết lập các thói quen mới; - Tìm kiếm sự giúp đỡ của các chuyên gia tâm lý, các cán bộ xã hội, các bác sỹ điều trị cai nghiện (nếu cần thiết). 

d. Nghiện trò chơi điện tử (hay còn gọi là "nghiện game")

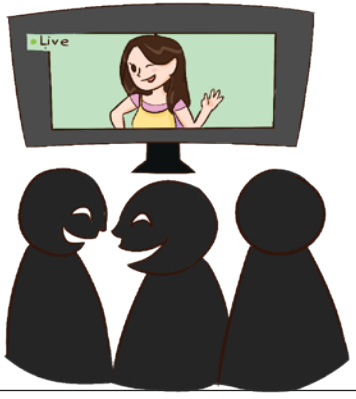
Là tình trạng trẻ em không thể kiểm soát cảm giác thèm chơi game, chơi liên tục và ưu tiên việc chơi game hàng đầu đến mức lệ thuộc vào game và ngày càng cô lập bản thân với gia đình, bạn bè và xã hội.

Trẻ em nghiện game ngày càng đòi hỏi để được chơi game nhiều hơn nhằm mục đích giữ được tình trạng tâm lý hiện tại của mình, nếu không đạt được mục đích này, trẻ emnghiện game online sẽ cáu giận và có thể gây ra những hành vi bạo lực gây nguy hiểm.

Dấu hiệu nghiện game	Cách phòng tránh, xử lý, ngăn chặn
Nếu có từ hai triệu chứng trở lên trong số các triệu chứng sau đây thì được xem là mắc bệnh nghiện game: - Thèm chơi game: quan tâm quá mức đến game online, luôn trò chuyện về game, không hứng thú với những việc khác. - Chơi game liên tục không nghỉ: chơi liên tục và không có thời gian nghỉ. - Không kiểm soát được việc chơi game và thời gian chơi của mình. Dù muốn chơi game với khoảng thời gian ít hơn, nhưng trẻ vẫn không thể hành động theo suy nghĩ ban đầu của mình. - Không quan tâm đến những công việc khác: trẻ nghiện game thường không quan tâm đến việc nào khác ngoài game, trẻ bỏ bê những mối quan hệ xung quanh như gia đình và bạn bè. Việc học tập, làm việc trì trệ, không được tiến hành. Kể cả việc ăn uống và vệ sinh cá nhân cũng không được thực hiện.	- Tham gia vào các hoạt động thay thế cho việc chơi game, tương tác nhiều hơn với mọi người xung quanh để quên đi cảm giác thèm muốn chơi game trước đây. Ví dụ: tham gia các hoạt động ngoài trời lành mạnh (đi bộ, đạp xe, chơi các môn thể thao); đi tham quan, du lịch hoặc tham gia vào các hoạt động xã hội; - Trò chuyện, trao đổi nhờ sự giúp đỡ của bố mẹ; - Tìm kiếm sự giúp đỡ của các chuyên gia tâm lý, các cán bộ xã hội, các bác sỹ điều trị cai nghiện (nếu cần thiết).

Dấu hiệu nghiện game	Cách phòng tránh, xử lý, ngăn chặn
- Che giấu cảm xúc: khi có một cảm xúc khó chịu hoặc tình huống không hay, người nghiện game thường chơi game để che giấu đi những cảm xúc này. Trẻ dùng thế giới ảo trong game để không phải đối diện với những vấn đề nảy sinh trong cuộc sống. - Nói dối về thời gian chơi game: trẻ nghiện game thường có xu hướng nói dối gia đình về thời gian chơi game. - Tiêu tốn nhiều tiền cho việc chơi game: người nghiện game thường đầu tư nhiều tiền vào chơi game và mua các thiết bị chơi game. - Cảm xúc bất ổn: khi chơi game, trẻ nghiện game sẽ có trạng thái kích thích, hưng phấn khi chơi và cũng có thể thất vọng. Cảm xúc này có thể vẫn tồn tại sau khi chơi. 	- Tham gia vào các hoạt động thay thế cho việc chơi game, tương tác nhiều hơn với mọi người xung quanh để quên đi cảm giác thèm muốn chơi game trước đây. Ví dụ: tham gia các hoạt động ngoài trời lành mạnh (đi bộ, đạp xe, chơi các môn thể thao); đi tham quan, du lịch hoặc tham gia vào các hoạt động xã hội; - Trò chuyện, trao đổi nhờ sự giúp đỡ của bố mẹ; - Tìm kiếm sự giúp đỡ của các chuyên gia tâm lý, các cán bộ xã hội, các bác sỹ điều trị cai nghiện (nếu cần thiết).

e. Selfie và Livestream không an toàn

Dấu hiệu nhận biết bức ảnh selfie hay clip livestream không an toàn	Cách phòng tránh, xử lý, ngăn chặn
- Bức ảnh/clip để lộ các thông tin cá nhân như lớp, trường học, địa chỉ nhà, hay vô tình để lộ các thông tin cá nhân khác; - Bức selfie/clip cho thấy những phần cơ thể riêng tư; - Bức selfie/clip có thể làm ô uế danh tiếng của bạn (ví dụ như một bức selfie/clip cho thấy bạn đang say xỉn hay đang hút thuốc); - Kể cả những phần cơ thể riêng tư không bị để lộ, nó vẫn có thể không an toàn (ví dụ như bức selfie cho thấy phần khe ngực, hay những bức selfie sử dụng kí hiệu tay.) 	Khi chụp selfie hoặc livestream, các bạn hãy nhớ những điều sau: - Liệu bạn có thoải mái nếu bức selfie/livestream được bố mẹ hoặc những người lớn khác nhìn thấy không? Nếu không, thì đó có thể không phải là một bức selfie/livestream an toàn và đừng đăng lên; - Những gì bạn đăng tải hay chia sẻ trên mạng không thể dễ dàng thu hồi, kể cả khi bạn đã xóa nó. Quá dễ dàng để người khác có thể sao chép, tải xuống và gửi cho những người khác; - Điều chỉnh Cài đặt Quyền riêng tư ở các mạng xã hội mà bạn dùng, chỉ chia sẻ cho nhóm người mà bạn thân quen, không nên chia sẻ rộng rãi.

f. Tham gia các thử thách nguy hiểm hoặc các trò chơi khăm trên mạng

Thử thách nguy hiểm	Cách phòng tránh, xử lý, ngăn chặn
Thử thách/thách thức trực tuyến liên quan đến việc mọi người thực hiện lại các thử thách/thách thức được truyền nhau trên Internet. Thử thách có thể thú vị và an toàn, nhưng cũng có thể rủi ro hoặc nguy hiểm, có thể dẫn đến tổn thương về thể chất hoặc tinh thần. Thử thách chơi khăm để chỉ một danh mục gồm các thử thách nguy hiểm trong đó yếu tố thử thách là giả nhưng nội dung được thiết kế để gây sợ hãi và gây đau đớn. Ví dụ điển hình là các trò chơi khăm thử thách dụ dỗ trẻ tham gia một loạt các hành vi gây hoảng sợ, tự làm hại bản thân hoặc tự tử như Momo hay Cá voi xanh.  	- Hãy thực hành tư duy phản biện trước khi quyết định có thực hành thử thách hay tin và làm theo các trò chơi khăm không. Trước hết bạn hãy kiểm tra lại các động cơ của mình, tại sao bạn lại muốn tham gia các thử thách, chơi khăm này: + Thử sức mình với một thử thách nguy hiểm hấp dẫn? + Làm theo bạn bè? Mọi người làm thế nên bản thân phải làm theo? + Tăng mức độ nổi tiếng trên môi trường mạng – thu hút sự chú ý. + Hãy kiểm tra xem các động cơ này có đủ mạnh để bạn bất chấp tham gia các thử thách hay không, đánh giá lại độ an toàn và tính chính xác của thử thách, chơi khăm để đưa ra quyết định phù hợp. - Nếu bạn cảm thấy có điều gì đó không ổn, hãy dừng lại. Bạn có thể chia sẻ với cha mẹ, thầy cô để tham khảo ý kiến và nhận được những lời khuyên hữu ích. - Cảnh báo bạn bè nếu thấy bạn bè tham gia các thử thách nguy hiểm. - Nếu bạn phát hiện các thử thách nguy hiểm hay trò bịp bợm, hãy báo cáo tới đơn vị cung cấp dịch vụ, nền tảng và báo cáo tới các cơ quan chức năng tại mục 1.2.5 (trang 17,18).

g. Nội dung độc hại, thông tin không phù hợp trên môi trường mạng

Thông tin gây hại cho trẻ em trên môi trường mạng là thông tin gây tổn hại trực tiếp hoặc tiềm tàng nguy cơ gây tổn tại tới thể chất, tình cảm, tâm lý, danh dự, nhân phẩm, sự riêng tư, hay sự phát triển của trẻ em được lưu hành trên mạng máy tính, mạng viễn thông phương tiện điện tử kết nối mạng.

Nội dung độc hại cho trẻ em là những thông tin xấu độc trái với quy định của pháp luật và đạo đức xã hội; những nội dung vượt quá giới hạn độ tuổi 18, có yếu tố bạo lực, tình dục; những nội dung lừa đảo, vi phạm thuần phong mỹ tục văn hóa của Việt Nam; và các nội dung gây hại khác ảnh hưởng tới thể chất, tinh thần của trẻ em.

Dấu hiệu nhận biết thông tin không phù hợp, nội dung độc hại	Cách phòng tránh, xử lý, ngăn chặn
- Không phù hợp với lứa tuổi, dành cho trẻ em trên 16 tuổi; - Có thể có hình ảnh khiêu dâm, bạo lực, phát ngôn thù ghét, chửi rủa; - Hình ảnh, video, trò chơi bạo lực; - Hình ảnh hay nội dung, quảng cáo cờ bạc, cá cược; - Lôi kéo bạn thực hiện các thử thách không an toàn hoặc nguy hiểm, gây hại. 	- Tuyệt đối không bắt chước ngay các thử thách, nội dung trên môi trường mạng trước khi hỏi ý kiến bố mẹ, thầy cô hoặc người lớn mà bạn tin tưởng; - Nhanh chóng đóng trang lại hoặc thoát khỏi ứng dụng; - Chặn những người chia sẻ hoặc những trang có nội dung không phù hợp; - Trao đổi ngay với cha mẹ, thầy cô hoặc một người lớn mà các bạn tin tưởng về chuyện đã xảy ra, cảm giác của bạn và lắng nghe lời khuyên của người lớn; - Cùng người lớn báo cáo nội dung không phù hợp với các nhà cung cấp dịch vụ. Ví dụ như YouTube có ngay nút "cảnh báo/flags", "báo cáo/report" ngay bên cạnh nội dung. Hoặc liên hệ tới các kênh phản ánh nội dung độc hại, thông tin không phù hợp được đề cập tại mục 1.2.5 (trang 17,18).

h. Tin giả, tin sai sự thật

Tin giả, tin sai sự thật	Cách phòng tránh, xử lý, ngăn chặn
- Tin giả: Tin không có thật, tin bịa đặt, vu không được lan truyền trong xã hội và trên môi trường mạng; - Tin sai sự thật: Tin có một phần sự thật nhưng không hoàn toàn chính xác, tin xuyên tạc, bóp méo sự thật; tin không có sở cứ được lan truyền trong xã hội và trên môi trường mạng. 	Kiểm tra nguồn thông tin một cách có hệ thống và đánh giá độ tin cậy. Cách thẩm định các nguồn thông tin khác nhau: + Nếu thấy nghi ngờ thông tin dạng văn bản, bạn hãy sao chép tiêu đề hoặc một phần cụm từ bạn đọc được và dán nó vào công cụ tìm kiếm, sử dụng dấu ngoặc kép ở hai đầu cụm từ/tiêu đề, thế là bạn đã kiểm tra ra một loạt các nguồn thông tin liên quan khác đấy. Sau đó hãy quay lại bước đánh giá nguồn thông tin ở trên; + Đối với hình ảnh, bạn có thể sử dụng tính năng Tìm kiếm hình ảnh của Google (images.google.com) để tìm hiểu thêm về hình ảnh. Cũng có thể sử dụng dịch vụ web TinEye (www.tineye.com) để tìm ra nơi ảnh có thể được sử dụng; + Đối với tài liệu video hay âm thanh, việc kiểm tra sẽ khó hơn: bạn hãy chú ý đến chất lượng của đoạn clip và ai là người chịu trách nhiệm tải đoạn clip lên. Những ý kiến bên dưới đoạn clip cũng có thể là bên cung cấp manh mối.

i. Bị kết bạn xấu

Kết bạn xấu	Cách phòng tránh, xử lý, ngăn chặn
- Các bạn có thể kết bạn và liên lạc với các người bạn này thông qua email, tài khoản chơi trò chơi điện tử, mạng xã hội, ... Do tính chất ẩn danh của Internet, các em có thể trót kết bạn với bạn xấu mà em không biết; - Đôi khi bạn tưởng kết bạn với người quen nhưng có thể đó là những tài khoản giả mạo mà bạn không nhận ra. Trên mạng, hãy nhớ chúng ta rất khó xác định được danh tính thật xem có đúng người kết bạn trên mạng với bạn có đúng là người em đã quen thân ngoài đời hay không. Kẻ xấu có thể sẽ đánh cắp thông tin, hình ảnh cá nhân của bạn, lừa đảo, bắt nạt, nói xấu, đe dọa hay lôi kéo em, thậm chí có thể tìm cách quấy rối, xâm hại bạn. 	- Vô hiệu hoá tính năng đề xuất kết bạn của người mà bạn không có liên hệ; - Đặt ra một số tiêu chí để kết bạn: + Kiểm tra xem đó có phải là người chúng ta đã gặp chưa? + Kiểm tra hình ảnh có phải là hình ảnh thực không? + Kiểm tra danh sách bạn chung? + Kiểm tra địa điểm, nơi ở của người ta kết bạn? + Kiểm tra các hoạt động, chia sẻ trên trang của người đó. Đây là những tiêu chí mang tính chất tham khảo. Mỗi chúng ta nên xây dựng tiêu chí kết bạn của riêng mình và vẫn cần cẩn trọng cả đối với những người đã kết bạn.

j. Bắt nạt trực tuyến (hay còn gọi là "bắt nạt trên mạng")

Là hành vi quấy rối, đe dọa hoặc làm nhục người khác diễn ra trên môi trường mạng. Bắt nạt trên môi trường mạng có thể xảy ra thông qua tin nhắn, các ứng dụng trên mạng, mạng xã hội, diễn đàn hoặc các trò chơi trực tuyến nơi mọi người có thể xem, tham gia hoặc chia sẻ nội dung. Trẻ bị bắt nạt trực tuyến có thể bị gửi, đăng hoặc chia sẻ thông tin cá nhân, thông tin riêng hoặc các nội dung tiêu cực, có hại, sai sự thật gây ra sự xấu hổ hoặc gây mất uy tín đối với trẻ em

Các hình thức bắt nạt trực tuyến phổ biến	Cách phòng tránh
- Đặt điều (đưa ra những thông tin làm hủy hoại danh dự, mối quan hệ của một ai đó); - Cô lập (cô lập hoặc loại trừ một ai đó ra khỏi nhóm trên mạng); - Giả danh (đột nhập vào email của người nào đó và gửi đi những thông tin, hình ảnh có thể làm mất đi danh dự, mối quan hệ của người đó); quấy rối (liên tục gửi email, tin nhắn thô lỗ, quấy rối tới ai đó); - Tấn công mạng (liên tục gửi những email, tin nhắn đe dọa cho một ai đó); - Lừa/Cài bẫy (lừa ai đó chia sẻ những bí mật hoặc những thông tin đáng xấu hổ để chia sẻ rộng rãi trên mạng); đe dọa trực tuyến (có những phát ngôn hoặc hành động bạo lực, đưa ra những xu hướng đe dọa, thậm chí giết người).	- Thực hành kỹ năng quản lý riêng tư và tư duy phản biện, phân biệt đâu là những thông tin nên chia sẻ, đâu là những thông tin không nên chia sẻ; - Đảm bảo việc chia sẻ thông tin không ảnh hưởng đến sự an toàn của bạn và người quen; - Đảm bảo việc chia sẻ thông tin không ảnh hướng tới hình ảnh/văn hóa/giá trị mà bạn và người quen đang thể hiện; - Cư xử văn minh trên môi trường mạng.

k. Bị xâm hại tình dục trẻ em qua mạng

Xâm hại tình dục trẻ em qua mạng là việc đe dọa, ép buộc, lôi kéo, dụ dỗ trẻ em tham gia vào các hành vi liên quan đến tình dục thông qua việc sử dụng không gian số, Internet và các phương tiện truyền thông khác.

Hành vi xâm hại tình dục trẻ em qua mạng có thể xảy ra hoàn toàn trên môi trường mạng hoặc có cả sự tương tác trực tiếp giữa người thực hiện hành vi với trẻ em ngoài đời thực.

Các hành vi xâm hại tình dục trẻ em qua mạng	Cách phòng tránh, xử lý, ngăn chặn
- Gửi cho trẻ em các nội dung phim, ảnh, trang web, nghe âm thanh, câu chuyện khiêu dâm hoặc liên quan tới tình dục qua điện thoại hoặc tin nhắn, email, mạng xã hội, ...; - Dụ dỗ, lôi kéo, ép buộc trẻ em khỏa thân và phát trực tiếp âm thanh, hình ảnh qua môi trường mạng; - Trẻ em bị sử dụng hình ảnh quay cơ thể phát tán trên mạng xã hội, các diễn đàn, các trang web khác nhau; - Bị bắt hoặc cho trẻ xem các hoạt động trình diễn khiêu dâm trực tuyến. 	- Giới hạn quyền riêng tư; - Tuyệt đối đừng bao giờ chia sẻ thông tin cá nhân hay hình ảnh, video bộ phận riêng tư của mình trên môi trường mạng; - Nếu ai đó yêu cầu bạn gửi thông tin cá nhân hay ảnh, hình ảnh hay clip bộ phận riêng tư hoặc thực hiện các hành vi xâm hại tình dục trẻ em như ô bên cạnh, hãy ngay lập tức hủy kết bạn, chặn, báo cáo tài khoản của người này và báo ngay với cha mẹ, thầy cô hoặc phản ánh nội dung độc hại tới các kênh phản ánh được đề cập tại mục 1.2.5 (trang 17,18).

4.3. Kỹ năng trẻ cần có

1	2	3	4
Quản lý danh tính số	**Quản lý quyền riêng tư**	**Quản lý thời gian tiếp xúc màn hình**	**Quản lý rủi ro**
Biết sử dụng danh tính số an toàn, có trách nhiệm. Phân biệt sống ảo và sống thật.	Biết quản lý thông tin mật khẩu: đặt mật khẩu mạnh; không chia sẻ với người ngoài. Biết cách xử lý việc chia sẻ thông tin cá nhân để bảo vệ quyền riêng tư của bản thân và những người khác.	Tự thiết lập thời gian biểu sử dụng Internet an toàn và hiệu quả phù hợp với độ tuổi, có sự đồng ý của phụ huynh.	Nhận biết rủi ro, biết cách phòng tránh, xử lý rủi ro. Có tư duy phản biện (biết cách kiểm chứng thông tin, kết quả do người khác đưa ra) và tư duy thấu cảm (cảm nhận cảm xúc của người khác.

4.4. Những lưu ý dành cho phụ huynh cần nắm để giáo dục trẻ ở độ tuổi từ 11 - dưới 16 tuổi

Ngoài việc nhận thức các rủi ro và hướng dẫn trẻ em cách phòng tránh theo mục 4.3, phụ huynh cần lưu ý thêm các điều sau:

❖ Tôn trọng việc con sử dụng Internet như các công dân số độc lập đang sắp trưởng thành;

❖ Nói về việc sử dụng Internet và các rủi ro trực tuyến với con.

Con bạn ở độ tuổi này đã có tư tưởng cá nhân độc lập, muốn chứng minh cái tôi. Do đó, cha mẹ hãy nói chuyện với con theo

cách tin tưởng và tôn trọng con, khuyến khích con tự tìm hiểu và học hỏi về các kỹ năng số, rủi ro trên Internet để có trách nhiệm bảo vệ bản thân và cả gia đình.

5 điều nói với con để đồng hành cùng con sử dụng Internet an toàn[2]:

1. "Hôm nay ở trên mạng có gì hay không con?" - Khởi đầu câu chuyện và xây dựng mối quan hệ giao tiếp gần gũi với con

Thời gian nghỉ ở nhà chính là thời gian thích hợp nhất để xây dựng mối quan hệ giao tiếp trong gia đình cởi mở và gần gũi. Cha mẹ hãy tận dụng cơ hội này để chia sẻ và trao đổi với con về việc sử dụng Internet. Để có thể nói cùng ngôn ngữ với con, hãy tìm hiểu các trang mạng, ứng dụng mà con hay dùng, tìm hiểu ngôn ngữ mà giới trẻ hay sử dụng trên mạng. Hãy nói chuyện với con về Internet tự nhiên như hỏi chuyện con về các việc xảy ra trong ngày và cùng con tìm hiểu về cách sử dụng Internet an toàn.

2. "Bố mẹ không phải là cảnh sát hay quan tòa, bố mẹ ở đây để đồng hành và hỗ trợ con"

Khi trẻ đang trong thời gian không tiếp xúc được với bạn bè, liệu cha mẹ có thể tận dụng thời gian này để làm bạn cùng con không? Làm bạn với con rất khó, riêng việc để được con chấp nhận kết bạn trên mạng xã hội đã là thách thức với nhiều cha mẹ. Nếu chưa thể xây dựng được mối quan hệ giống như "làm bạn" cùng con, ít nhất cha mẹ hãy thể hiện sự tôn trọng, lắng nghe, khích lệ và hỗ trợ trẻ. Đừng đóng vai "cảnh sát" truy hỏi trẻ, hay "quan toà" phán xét các hành vi của trẻ. Đấy chỉ là cách làm con sẽ xa cách cha mẹ và không tìm cha mẹ để được hỗ trợ, giúp đỡ khi cần thiết. Hãy cho con biết, cha mẹ ở đây để hỗ trợ, giúp đỡ con bất cứ khi nào con cần.

[2] *Nguyễn Phương Linh, 5 điều nói với con để đồng hành với con sử dụng Internet an toàn, MSD, 2020.*

3. "Con có thể cùng chơi hay dạy bố/mẹ được không?" - Cùng nhau học tập và thảo luận các cách thức sử dụng Internet thông minh và an toàn

Trẻ con có thể thậm chí giỏi hơn cả cha mẹ về công nghệ, nhưng cha mẹ cũng có "vốn sống" để chia sẻ với con. Hãy dành thời gian để cả gia đình cùng học hỏi về Internet. Con có thể hướng dẫn bố mẹ cách sử dụng Internet an toàn, như cài đặt mật khẩu mạnh, cảnh báo đăng nhập và bảo vệ 2 lớp, cài đặt riêng tư,... để cả nhà dùng Inetrnet được an toàn hơn. Cha mẹ cũng hãy trò chuyện và cùng con trao đổi các quan điểm và cách xử lý/giải pháp của con khi có khả năng gặp các rủi ro khác nhau khi dùng Internet tại nhà (ví dụ: bị lừa đảo trên mạng, bị bắt nạt trực tuyến, bị xem các thông tin giả, tin và hình ảnh không phù hợp, bị nhắn tin quấy rối, ...). Đặt ra các tình huống, giả thuyết, phân tích và cùng đưa ra giải pháp, cả nhà sẽ học được cách thức tư duy phản biện và có kỹ năng tốt hơn để xử lý tình huống rủi ro xảy ra với trẻ khi đang lướt mạng.

4. "Chúng mình cùng thỏa thuận nhé!" - Tôn trọng và thỏa thuận với trẻ về cách thức đảm bảo an toàn khi sử dụng Internet tại nhà

Một hợp đồng gia đình thỏa thuận cách thức trẻ sử dụng Internet và đảm bảo an toàn khi sử dụng Internet cho không chỉ trẻ mà cả gia đình. Đây là công cụ rất hữu dụng để trẻ ý thức vai trò của bản thân trong sử dụng Internet an toàn, có thể áp dụng cho trẻ trên 10 tuổi. Bản hợp đồng gia đình cần đảm bảo đây là kết quả thảo luận công bằng giữa cha mẹ và con cái với trách nhiệm và quyền hạn bình đẳng thay vì một bản quy định cấm đoán, kiểm soát từ cha mẹ. Hãy quan tâm đến các điều khoản đặt ra các giới hạn trong sử dụng Internet như thời gian sử dụng Internet của

gia đình, các trang hay ứng dụng con có thể xem, ... và cả các quy định liên quan đến tôn trọng quyền riêng tư của con của cha mẹ, và không phản ứng thái quá, dành thời gian chia sẻ và thảo luận với con về mọi vấn đề. Hãy nghiêm chỉnh tuân thủ các điều khoản của hợp đồng, chính cha mẹ cũng cần làm gương cho con rằng bạn tôn trọng các điều khoản hợp đồng và con cũng nên như vậy.

5. "Chúng ta sẽ có cách giải quyết"

Nếu không may con gặp các rủi ro và chia sẻ với cha mẹ, hãy cùng tìm cách giải quyết. Cha mẹ đừng xem nhẹ vấn đề, cũng đừng phóng đại vấn đề và phản ứng thái quá, làm trẻ sợ hãi hoặc không muốn tiếp tục chia sẻ với chúng ta. Đôi khi, vấn đề không nghiêm trọng như chúng ta tưởng, hãy bình tĩnh cùng con suy nghĩ giải pháp khi có những rủi ro hay nguy hại xảy ra và cùng thảo luận các giải pháp. Và quan trọng, hãy biết rằng cha mẹ hay con cái không đơn độc. Trẻ em trên Internet ngoài cha mẹ, còn được pháp luật, các tổ chức xã hội, các cơ quan chức năng bảo vệ và đồng hành. Nếu phát hiện nội dung độc hại, thông tin không phù hợp.

Câu hỏi thực hành

Câu hỏi thực hành 10: Đâu là các rủi ro trên môi trường mạng mà trẻ em 11 tuổi – dưới 16 tuổi thường gặp? (Có thể chọn nhiều đáp án)

A. Học trực tuyến với thầy cô
B. Xem các nội dung không phù hợp
C. Bị lừa đảo mua sắm trực tuyến trên mạng
D. Tham gia các thử thách nguy hiểm
E. Bị tiếp xúc, kết bạn bởi những người xấu
F. Bị xem các ấn phẩm khiêu dâm
G. Sử dụng tài khoản của người lớn
H. Click chuột vào các đường link làm mất thông tin cá nhân
I. Bị lừa gửi ảnh và thông tin cá nhân cho người lạ
K. Chơi trò chơi điện tử trên Internet cùng bạn bè
L. Bị nói xấu, bắt nạt trực tuyến
M. Tham gia các cuộc thi do nhà trường phát động
N. Bị hiếp dâm, xâm hại tình dục
O. Bị bắt cóc, buôn bán

Câu hỏi thực hành 11: Một số các biện pháp cha mẹ nên làm để đồng hành cùng con giai đoạn Tiền trưởng thành (Có thể chọn nhiều đáp án)

A. Hướng dẫn con lập tài khoản và các mật khẩu mạnh
B. Cho con vào tài khoản của bố mẹ để dùng chung cho nhanh và bố mẹ dễ kiểm soát
C. Xây dựng hợp đồng sử dụng An toàn Internet cho cả gia đình
D. Hỏi han con hàng ngày xem con sử dụng Internet như thế nào
E. Kiên nhẫn và tôn trọng việc con sử dụng Internet
F. Mắng mỏ con vì để bạn bè đăng hình nói xấu con và gia đình trên Facebook
G. Tịch thu thiết bị công nghệ khi con xem chương trình không phù hợp
H. Cùng con phân tích các lợi ích và rủi ro của Internet và cách phòng tránh và các giải pháp
I. Hướng dẫn con gọi tới Tổng đài Quốc gia Bảo vệ trẻ em 111 và hoặc báo cáo tới Mạng lưới ứng cứu Bảo vệ trẻ em trên môi trường mạng tại địa chỉ "vn-cop.vn"

PHẦN V

MỘT SỐ CÔNG CỤ, PHẦN MỀM HỖ TRỢ BẢO VỆ TRẺ EM TRÊN MÔI TRƯỜNG MẠNG

5.1. Các công cụ cập nhật kiến thức bảo vệ trẻ em trên môi trường mạng

5.1.1. Website https://vn-cop.vn/

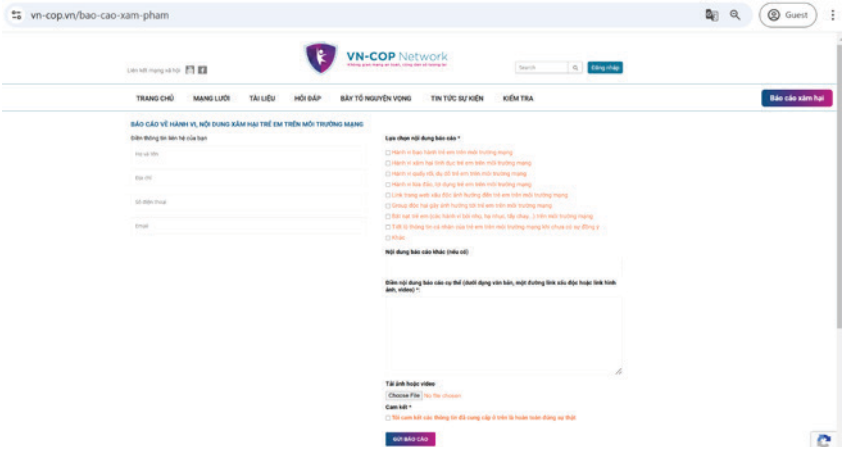
VN-COP.VN là Cổng thông tin chính thức của Mạng lưới ứng cứu, bảo vệ trẻ em trên môi trường mạng (VN-COP). VN-COP là tổ chức phối hợp liên ngành giúp Bộ trưởng Bộ Thông tin và Truyền thông tăng cường hiệu lực, hiệu quả quản lý nhà nước và kết quả thực thi các nhiệm vụ phòng, chống xâm hại trẻ em trên môi trường mạng, góp phần nâng cao nhận thức xã hội và tạo lập một môi trường mạng an toàn, lành mạnh cho trẻ em.

VN-COP hiện có 24 thành viên trực thuộc 5 Bộ (Bộ Thông tin và Truyền thông; Bộ Công An; Bộ Lao động, Thương binh và Xã Hội; Bộ Văn hóa, Thể thao và Du Lịch), doanh nghiệp lớn; các Hội, Hiệp hội và các tổ chức phi chính phủ làm về công tác bảo vệ trẻ em.

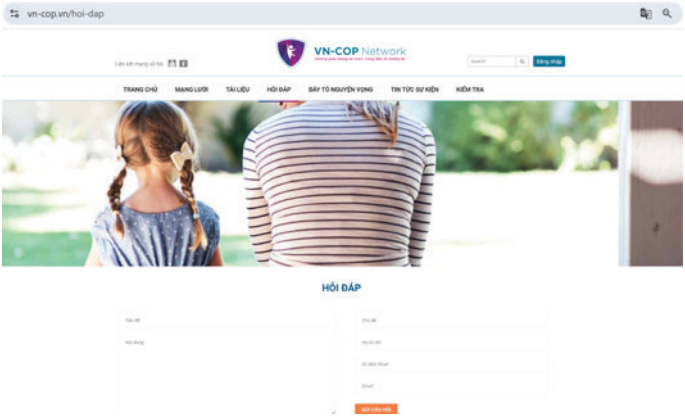
VN-COP cung cấp:

❖ **Kho tư liệu** phong phú phục vụ nhiều đối tượng (nhà trường, phụ huynh, trẻ em, người làm công tác bảo vệ trẻ em) nâng cao nhận thức, kỹ năng kinh nghiệm bảo vệ trẻ em trên môi trường mạng.

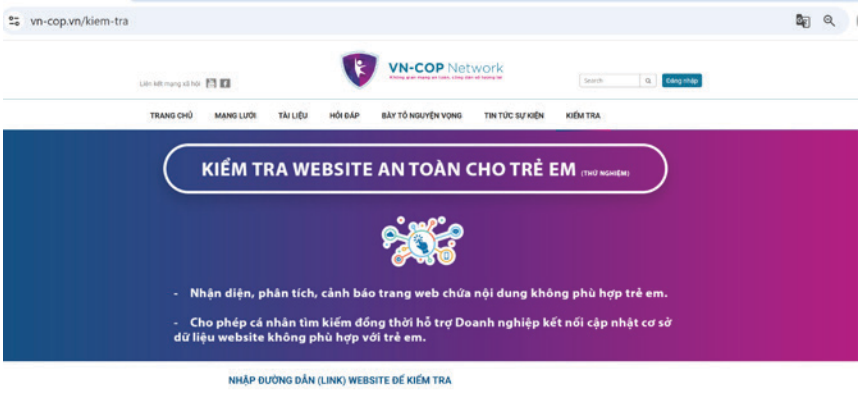
❖ Công cụ **"Báo cáo xâm hại"**, tiếp nhận các báo cáo hành vi xâm hại trẻ em trên môi trường mạng.



❖ Công cụ **"Hỏi đáp"** giúp người dùng có thể đặt câu hỏi để được giải đáp về vấn đề để bảo vệ trẻ em trên môi trường mạng; **"Bày tỏ nguyện vọng"** để trẻ em và người dân thông qua website có thể bày tỏ ý kiến, nguyện vọng của mình.



❖ Công cụ **"Kiểm tra website an toàn cho trẻ em"** giúp nhận diện, phân tích và cảnh báo một trang web cụ thể có chứa những nội dung không phù hợp đối với trẻ em. Đồng thời hỗ trợ phụ huynh nói riêng và người dùng nói chung chủ động đánh giá mức độ phù hợp của website trước khi cho trẻ em sử dụng, nhằm tránh nguy cơ tiếp xúc với những nội dung độc hại



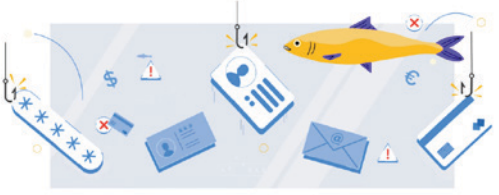
5.1.2. Website https://khonggianmang.vn/

Là cổng thông tin điện tử của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) trực thuộc Cục An toàn thông tin. Cổng thông tin điện tử cung cấp các công cụ an toàn thông tin miễn phí cho người dân, cụ thể:

❖ **Kiểm tra phát hiện lừa đảo, phishing**

Các cuộc tấn công giả mạo thường đánh lừa người dùng bằng việc mạo danh các công ty nổi tiếng và uy tín, thu thập thông tin cá nhân hoặc thông tin tài chính. Với sự phát triển của công nghệ, AI đã và đang làm cho các cuộc tấn công giả mạo trở nên tinh vi và phổ biến hơn.

Để ngăn chặn và bảo vệ bản thân trước mối đe dọa này, người dùng cần phải trang bị những kiến thức, kỹ năng cần thiết giúp nhận diện và phòng chống lừa đảo trực tuyến một cách hiệu quả. Bài kiểm tra phát hiện lừa đảo, phishing sẽ giúp người dùng nâng cao hiểu biết, phân biệt được đâu là thật, đâu là giả trong các cuộc tấn công giả mạo.



Bạn có thể phát hiện ra khi nào bạn bị lừa đảo không?

Các cuộc tấn công giả mạo sẽ tìm cách lừa những người dùng không nghi ngờ tiết lộ thông tin cá nhân hoặc thông tin tài chính, thường là bằng thủ đoạn bắt chước nội dung của các công ty nổi tiếng và uy tín.

AI đã và đang làm cho các cuộc tấn công giả mạo trở nên tinh vi hơn, tập trung vào từng cá nhân và trở nên phổ biến hơn.

Bạn có nghĩ mình phân biệt được đâu là thật, đâu là giả không?

Làm bài trắc nghiệm

❖ **Dấu hiệu lừa đảo**

Thủ đoạn của các đối tượng lừa đảo trên không gian mạng đặc biệt tinh vi nhưng người dùng hoàn toàn có thể ngăn chặn hành động

của chúng khi nắm vững được các kiến thức cơ bản, chủ động phòng tránh kịp thời. Dấu hiệu lừa đảo sẽ cung cấp thông tin về những kịch bản lừa đảo thường gặp, đồng thời chia sẻ 3 nguyên tắc vàng giúp bảo vệ bản thân khỏi lừa đảo trực tuyến.

Ngoài ra, người dùng có thể tham gia bài kiểm tra trắc nghiệm nhằm nâng cao hiểu biết bằng các ví dụ thực tế, nhận diện các tình huống lừa đảo có thể xảy ra trên không gian mạng.

❖ Kiểm tra mã độc trong mạng

Khi một địa chỉ IP bị phát hiện có vấn đề liên quan đến mã độc, botnet… các thiết bị và toàn bộ thông tin dữ liệu trên thiết bị sử

dụng IP này đều có thể bị theo dõi, đánh cắp thông tin. Vì vậy, kiểm tra IP sẽ giúp cá nhân, doanh nghiệp tìm ra vấn đề và giải quyết sớm, tránh thiệt hại đáng tiếc.

Với công cụ kiểm tra nhanh của NCSC, người dùng chỉ cần nhấn vào nút "Kiểm tra", mọi thông tin liên quan đến mạng, nhà cung cấp, phiên bản trình duyệt, hệ điều hành… đều được cung cấp đầy đủ. Hệ thống của NCSC sẽ phân tích và đưa ra đánh giá về độ an toàn khi truy cập mạng, đồng thời đưa ra cảnh báo nếu phát hiện bất kỳ nguy cơ nào trong vòng 30 ngày trước đó.

❖ **Kiểm tra website lừa đảo**

Website lừa đảo là các website giả mạo các cơ quan, tổ chức hay các trang mạng xã hội, ngân hàng, giao dịch trực tuyến, ví điện tử,... do kẻ tấn công tạo ra với giao diện giống hệt trang web gốc, nhằm đánh lừa người dùng chia sẻ các thông tin cá nhân nhạy cảm hoặc lừa đảo chiếm đoạt tài sản.

Để kiểm tra một trang web nghi là Website lừa đảo, người dùng nhập URL vào ô tìm kiếm trên công cụ của NCSC và nhấn "Kiểm tra". Kết quả trả về sẽ giúp người dùng đánh giá mức độ tin cậy của trang web trước khi quyết định sử dụng.

Ngoài việc kiểm tra bằng công cụ, người dùng có thể chú ý một số đặc điểm đáng nghi đối với các Website lừa đảo như chuỗi ký tự vô nghĩa hoặc văn bản bổ sung, chứng thư số không rõ ràng. Nếu phát hiện có trang web giả mạo, người dùng cần báo cáo ngay đến cơ quan có thẩm quyền, yêu cầu được hỗ trợ giải quyết.

CÔNG CỤ KIỂM TRA WEBSITE LỪA ĐẢO

Nhập URL
Check

5.2 Một số công cụ hỗ trợ phụ huynh kiểm soát truy cập sử dụng internet (Parental controls)

Parental controls là những phần mềm hay các công cụ cung cấp cho phụ huynh khả năng kiểm soát quá trình sử dụng Internet của con mình và là một giải pháp hữu hiệu trong việc ngăn chặn trẻ em truy cập các nội dung không lành mạnh.

Hiện nay, thị trường Việt Nam đã có các sản phẩm, giải pháp công nghệ do các nhà cung cấp trong và ngoài nước phát triển có thể hỗ trợ cha mẹ bảo vệ trẻ em trên môi trường mạng. Các sản phẩm bảo vệ trẻ em đang có trên thị trường Việt Nam được chia thành 2 nhóm sản phẩm chính là: sản phẩm phần cứng (network-based) và sản phẩm phần mềm (host-based).

a) Sản phẩm phần cứng, hay còn gọi là network-based: Là giải pháp bảo vệ trẻ em sử dụng thiết bị mạng độc lập với các thiết bị cần giám sát, bảo vệ (máy tính, điện thoại…). Thiết bị mạng độc lập này đóng vai trò là cửa ngõ (gateway) của các thiết bị cần giám sát, bảo vệ.

b) Sản phẩm phần mềm, hay còn gọi là host-based: Là giải pháp bảo vệ trẻ em theo hình thức cài đặt thêm các phần mềm, module bổ sung (add-on) vào thiết bị cần giám sát, bảo vệ (máy tính, điện thoại…).

Các công cụ parental controls cung cấp các tính năng chung như sau:

- Lọc và chặn các nội dung mà phụ huynh cảm thấy không phù hợp với trẻ em, như phim có nội dung bạo lực, người lớn.
- Giới hạn thông tin mà trẻ em có thể chia sẻ.
- Kiểm soát và giới hạn thời gian con được sử dụng Internet.

Dưới đây là một số công cụ phổ biến giúp bố mẹ và người chăm sóc trẻ đồng hành cùng con trên môi trường mạng

5.2.1. Một số công cụ trong nước

SafeGate Family

Giải pháp Internet an toàn giúp cha mẹ có thể quản lý, giới hạn thời gian sử dụng Internet của con, bao gồm phần mềm (cài đặt trên điện thoại bố mẹ) và thiết bị Router Wifi lắp đặt tại gia đình.

Các tính năng mà SafeGate Family cung cấp cho parental controls:

1. Kết nối an toàn:

Khi tìm kiếm thông tin trên Google, YouTube,… các nội dung không phù hợp với trẻ như nội dung người lớn, bạo lực,... sẽ được tự động loại bỏ và ngăn chặn. Đồng thời, bảo vệ tất cả thiết bị kết nối mạng trong gia đình khỏi các địa chỉ lừa đảo, link chứa mã độc, web giả mạo,...

2. Báo cáo tổng quan:

Báo cáo chi tiết về tình hình sử dụng Internet của từng thiết bị trong gia đình.

4. Đảm bảo quyền riêng tư:

Không cần cài đặt thêm bất kì ứng dụng quản lý nào trên thiết bị của con, tránh làm trẻ con thấy khó chịu và bị kiểm soát.

5. Thiết lập thời gian sử dụng:

Tính năng quản lý cho phép phụ huynh lên lịch sử dụng Internet, mạng xã hội, game online của con theo khung giờ nhất định trong ngày.

6. Kiểm soát sử dụng từ xa:

Ngay cả khi không có mặt ở nhà, phụ huynh có thể dễ dàng kiểm tra tình hình sử dụng Internet trong gia đình thông qua báo cáo chi tiết trên ứng dụng.

Tìm hiểu thêm tại: https://safegate.vn/vi

VNPT Family Safe

VNPT Family Safe là ứng dụng được tích hợp sẵn trên mạng internet VNPT, nhằm hỗ trợ phụ huynh bảo vệ con trên môi trường mạng. Phụ huynh chỉ cần đăng ký tài khoản và cài đặt ứng dụng trên điện thoại hoặc máy tính bảng, vô cùng tiện lợi và đơn giản.

Các tính năng mà SafeGate Family cung cấp cho parental controls:

1. Kiểm soát thời gian sử dụng internet:

Cha mẹ có thể đặt giới hạn thời gian sử dụng internet cho trẻ em, giúp trẻ cân bằng giữa học tập và giải trí.

2. Kiểm soát nội dung truy cập:

• Quản lý quyền truy cập Internet của các thiết bị trong mạng.

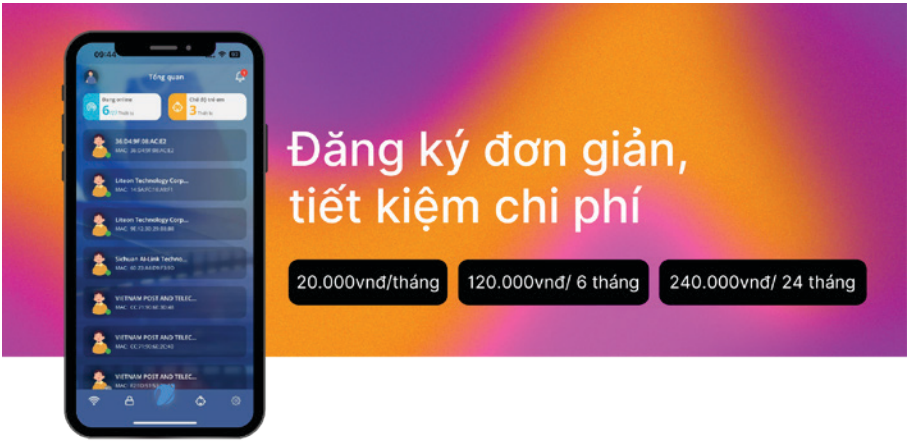
• Đảm bảo từng thiết bị được truy cập vào các nội dung phù hợp với lứa tuổi trên các ứng dụng/website nổi tiếng như Facebook, Youtube…

• Đảm bảo các thiết bị không tìm kiếm được các từ khóa nhạy cảm như bạo lực, giới tính, phản tính, chất kích thích, lừa đảo, cờ bạc … trên các nền tảng tìm kiếm phổ biến (Google, Bing…).

3. Kiểm soát ứng dụng:

Cha mẹ có thể Chặn/Lên lịch cho phép trẻ sử dụng các ứng dụng mạng xã hội, game online,… trên điện thoại, máy tính bảng theo khung giờ nhất định.

Tìm hiểu thêm tại: https://familysafe.vn/



MobiSafe Total Security

MobiSafe Total Security là ứng dụng internet an toàn được đăng ký thương hiệu của MobiFone . Có tính năng bảo vệ trẻ em trên môi trường mạng. Cha mẹ có thể chặn, lọc thông tin độc hại, giới hạn thời gian sử dụng thiết bị, cũng như thiết lập thời gian đi ngủ cho trẻ, giúp cha mẹ yên tâm hơn khi con em mình được tiếp xúc với thế giới số.

Các tính năng giúp cha mẹ quản lý trẻ nhỏ:

1, Lọc nội dung không phù hợp với trẻ nhỏ

2, Giới hạn thời gian sử dụng theo từng ứng dụng

3, Giới hạn và cài đặt thời gian đi ngủ của trẻ

4, Quản lý ứng dụng từ xa dành cho cha mẹ

5, Chặn web đen

6, Giữ cho thiết bị tránh khỏi virus, trojan, phần mềm gián điệp và mã độc tống tiền…

Ưu điểm của App MobiSafe:

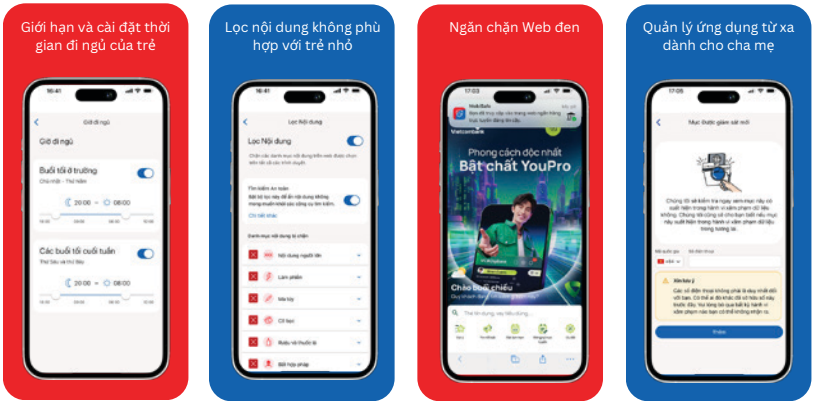
Dễ sử dụng: Giao diện thân thiện, dễ sử dụng, phù hợp với mọi đối tượng.

Tích hợp nhiều tính năng: Cung cấp đa dạng các tính năng giúp bảo vệ trẻ em toàn diện.

Cập nhật thường xuyên: MobiFone liên tục cập nhật và nâng cấp dịch vụ để đảm bảo hiệu quả bảo vệ.

Giá cả phải chăng: Chi phí sử dụng dịch vụ MobiSafe khá hợp lý.

Tham khảo thêm tại: https://mobisafe.mobifone.vn/



Bkav | Safe Kids

Các tính năng parental controls của Bkav Safe Kids được thực hiện trên các thiết bị mobile (IOS, ADR), máy tính.

Các tính năng mà Bkav Safe Kids cung cấp cho parental controls:

Giám sát sử dụng phần mềm và web:

Giám sát các phần mềm và trang web mà con đã sử dụng trên máy tính. Cấu hình các phần mềm và trang web con được phép/không được phép sử dụng

Giám sát nội dung: Hiển thị đầy đủ lịch sử tìm kiếm, từ khóa tìm kiếm của con trên các công cụ tìm kiếm Google, Bing…

Trang bị bộ tính năng: Chặn nội dung người lớn; chặn chơi game; chặn mạng xã hội, kênh video phổ biến

Tìm kiếm an toàn: Điều chỉnh, cấu hình các phần mềm và trang web con được phép hay không được phép sử dụng

Đảm bảo các thông tin mà trẻ tiếp cận sẽ luôn được chọn lọc, an toàn

Tập trung học tập: Là chế độ mà con trẻ sẽ chỉ truy cập được các phần mềm, trang web đã được cấu hình (các trang web giáo dục, kênh video phổ biến kiến thức…), mà không bị ảnh hưởng, phân tán bởi những thứ khác (Game, mạng xã hội, Youtube…)

Báo cáo thông minh: Cung cấp các thống kê, báo cáo chi tiết, trực quan, sinh động cho phụ huynh

Dễ dàng xem báo cáo ngay trên máy tính hoặc smartphone

Điều khiển máy tính từ xa: Điều khiển máy tính của con bằng smartphone mọi lúc mọi nơi, ngăn chặn hoặc cho phép con sử dụng các phần mềm, internet linh hoạt

Quản lý thiết bị: Cho phép quản lý cùng lúc nhiều thiết bị máy tính mà các con sử dụng.

Tham khảo thêm tại: https://www.bkav.com/bkav-safe-kids

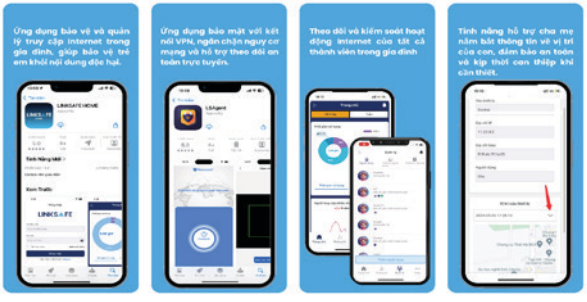
Linksafe Home

Là hệ thống quản lý và bảo vệ truy cập Internet dành cho gia đình, tích hợp công nghệ tiên tiến với nhiều tính năng nổi bật. Từ kiểm soát nội dung, giám sát hoạt động trực tuyến đến bảo vệ các thiết bị thông minh, Linksafe Home giúp phụ huynh yên tâm hơn khi con trẻ truy cập Internet. Với nhiều gói linh hoạt như **Gia đình hạnh phúc**, **Con em chăm ngoan**, **Du học gắn kết**, và **Lợi thế công nghệ, bảo vệ nhiều nhà**, Linksafe Home phù hợp với đa số nhu cầu của các gia đình hiện đại.

Điểm nổi bật:

- **Quản lý và giám sát tập trung**: Theo dõi và kiểm soát hoạt động Internet của tất cả thành viên trong gia đình, ngay cả khi con không ở nhà hoặc có thể kiểm soát một lúc nhiều căn nhà. Dễ dàng điều khiển và giám sát mạng gia đình mọi lúc, mọi nơi qua ứng dụng.
- **Bảo vệ toàn diện**: Tự động chặn nội dung không phù hợp, bảo vệ an toàn cho các thiết bị IoT trong gia đình như camera an ninh, smart TV, thiết bị nhà thông minh đảm bảo môi trường truy cập an toàn.
- **Giám sát vị trí của thiết bị:** Vị trí của con bạn có thể được cập nhật liên tục mỗi khi có di chuyển, ngay khi mất kết nối phụ huynh sẽ nhận được thông báo về vị trí cuối cùng nhận được.

Báo cáo chi tiết: Cung cấp thống kê truy cập, giúp bạn hiểu rõ hơn về thói quen sử dụng mạng của các thành viên. Báo cáo chi tiết về tình hình truy cập Internet của con em; đưa ra các cảnh báo về vi phạm truy cập, cũng như các cảnh báo về hành vi tắt/ gỡ bỏ ứng dụng.



Linksafe Home không chỉ mang lại an toàn mà còn tạo ra môi trường kết nối thông minh, lành mạnh, giúp gắn kết yêu thương trong gia đình.

5.2.2 Một số công cụ quốc tế

Family Link

Bằng việc tạo một tài khoản Google cho con, phụ huynh có thể thực kiện các biện pháp kiểm soát parental controls thông qua ứng dụng Family Link.

Các tính năng mà Google cung cấp cho parental controls gồm:

1) Giám sát các thiết lập trên tài khoản của con:

- Kiểm soát các thanh toán, tải về và nội dung nào được hiển thị.
- Kiểm soát trình duyệt Chrome (blacklist/whitelist website, kiểm soát quyền truy cập trang web). Phụ huynh không thể thấy được lịch sử duyệt web qua Family Link mà chỉ có thể thực hiện xóa lịch sử từ xa. Phụ huynh nếu cần kiểm tra lịch sử duyệt web sẽ phải thực hiện trên chính thiết bị của con.
- Lọc nội dung được hiển thị trên Google Search.
- Thấy được địa điểm thiết bị của con.
- Kiểm soát ứng dụng nào con được tải về từ Play store.

2) Cập nhật thông tin cá nhân cho tài khoản của con.

Khi con đạt tới độ tuổi nhất định (ở Việt Nam là 15 tuổi), trẻ em có thể chọn việc tắt parental controls trên tài khoản của mình. Phụ huynh cũng sẽ được thông báo khi con tắt parental controls và thiết bị của con sẽ tạm thời bị khóa.

Tham khảo thêm tại:

https://families.google.com/intl/vi_ALL/familylink/

Apple

Khác với Google, các tính năng parental controls của Apple chỉ được thực hiện trên các thiết bị iOS hoặc Mac.

Các tính năng mà Apple cung cấp cho parental controls:

1) Giới hạn nội dung và thông tin cá nhân.

2) Hạn chế các thanh toán từ iTunes và App Store.

3) Tắt các app built-in.

4) Ẩn các nội dung không phù hợp như nhạc, phim ảnh có rating không phù hợp với con.

5) Ẩn các trang web có nội dung người lớn (chỉ khả dụng khi con sử dụng Safari) hoặc giới hạn trang web nào con được quyền truy cập.

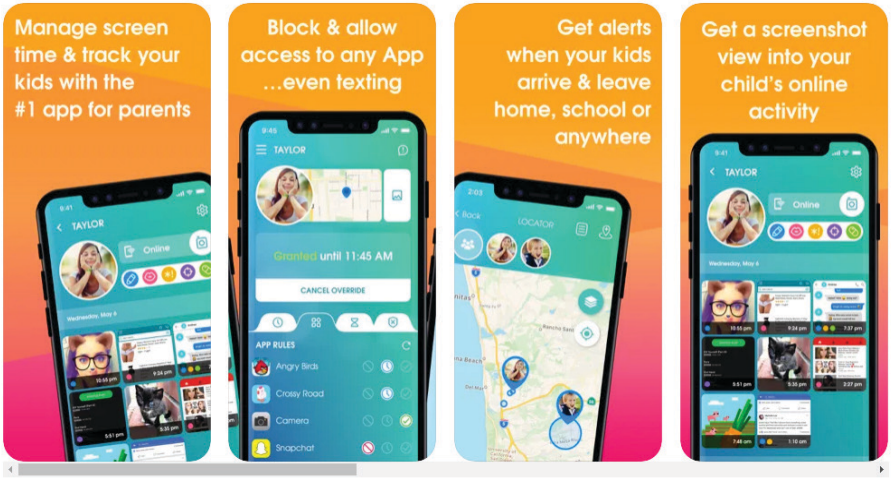
6) Giới hạn nội dung tìm kiếm Siri.

7) Giới hạn một số tính năng của Game Center.

8) Kiểm soát các permision mà các app yêu cầu.

9) Kiểm soát các cài đặt và tính năng có trên thiết bị của con.

Tham khảo thêm tại: https://support.apple.com/en-vn/HT201304



Microsoft

Phụ huynh có thể thiết lập một family group cho các tài khoản Microsoft trong gia đình để có thể sử dụng các tính năng parental controls mà Microsoft cung cấp.

Các tính năng parental controls của Microsoft chỉ sử dụng được với các thiết bị Windows 10, Xbox.

Các tính năng parental controls được Microsoft cung cấp:

1) Báo cáo hoạt động (Activity reporting): Thấy được lịch sử tìm kiếm, duyệt web và các app được sử dụng. Tính năng thấy lịch sử tìm kiếm và duyệt web chỉ khả dụng khi con sử dụng Bing để tìm kiếm, và tài khoản của con được đăng nhập vào Microsoft Edge.

2) Giới hạn thời gian sử dụng thiết bị (Screen time limits): Thiết lập giới hạn thời gian mà con được sử dụng thiết bị và thời gian nào con được sử dụng thiết bị trong ngày. Ngoài ra phụ huynh có thể thấy được thời lượng sử dụng thiết bị của con trong khung thời gian nào.

3) Bộ lọc nội dung (Content filters): Lọc các nội dung không phù hợp khi con duyệt web trên Microsoft Edge. Phụ huynh có thể thiết lập blacklist, whitelist các trang web cho con. Ngoài ra, phụ huynh còn có thể lọc những ứng dụng và trò chơi không phù hợp (chỉ áp dụng được cho Microsoft Store).

4) Quản lý chi tiêu (Manage speding): Phụ huynh có thể kiểm soát giao dịch của con trên Microsoft Store, gồm thêm số dư vào tài khoản của con, yêu cầu phải có sự chấp thuận của phụ huynh và xem lịch sử thanh toán.

5) Định vị các thành viên trong gia đình (Locate): Phụ huynh có thể xem địa điểm hiện tại của thiết bị con sử dụng qua ứng dụng Microsoft Family Safety. Thêm nữa, phụ huynh có thể thiết lập cảnh báo khi con rời trường, nhà hoặc những địa điểm được thiết lập.

Tham khảo thêm tại:

https://support.microsoft.com/vi-vn/account-billing/b%E1%BA%AFt-%C4%91%E1%BA%A7u-v%E1%BB%9Bi-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344.

Kaspersky Safe Kids

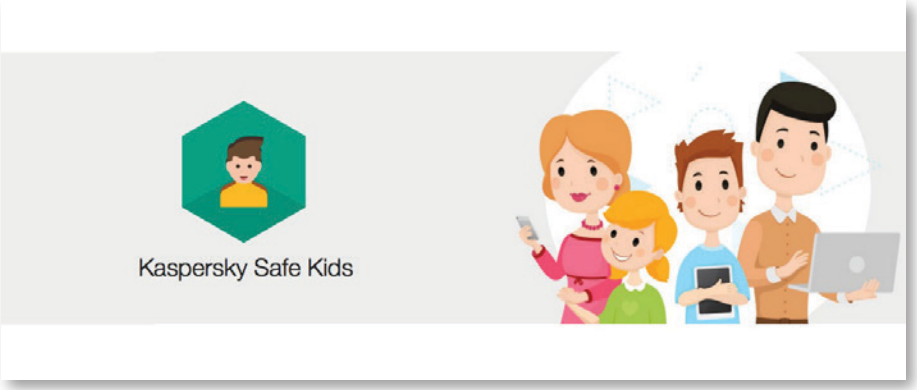
Kaspersky Safe Kids là một ứng dụng đa nền tảng, có thể chạy trên các thiết bị Windows, iOS, Android và Mac OS.

Kapersky Safe Kids cung cấp các tính năng sau:

- Chặn quyền truy cập vào nội dung không phù hợp hoặc có hại.
- Đặt giới hạn thời gian sử dụng thiết bị cho mỗi trẻ em, mỗi thiết bị.
- Theo dõi vị trí của con bằng GPS.

Tham khảo thêm tại:

https://kaspersky.proguide.vn/kaspersky-safe-kids/



DANH MỤC TÀI LIỆU THAM KHẢO

1. Một số giải pháp đảm bảo an toàn cho học sinh khi sử dụng Internet – Bộ Thông tin và Truyền thông, Nxb, 2020.

2. An toàn thông tin khi sử dụng Mạng xã hội – Bộ Thông tin và Truyền thông, Nxb, 2021.

3. Chương trình tư duy thời đại số – Facebook, 2021.

4. Education for a Connected World – UK Council for Internet Safety, 2020 edition.

5. Cẩm nang An toàn sử dụng Internet – Bộ Giáo dục và Đào tạo, Vietnet – ICT và Microsoft, 2019.

6. Kiểm soát thách thức – ITU – Child Online Protection, 2020.

7. Sách hành động trực tuyến an toàn – ITU – Child Online Protection, 2020.

8. 5 điều nói với con để đồng hành cùng con sử dụng Internet an toàn – MSD, 2020.

9. 5 nguyên tắc , 10 hành động đồng hành cùng con trên môi trường mạng – Bộ Lao động – Thương binh và Xã hội, MSD và World Vision, 2020.

10. Sổ tay dành cho cha mẹ về kỹ năng bảo vệ trẻ trước nguy cơ bị xâm hại tình dục trên môi trường mạng – Save the Children, 2017.

11. Fake vs Real – Giả mạo và sự thật, Đại sứ quán Thuỵ Điển, 2019.

12. Cha mẹ 0.4 học 4.0 – Đồng hành cùng con sử dụng Internet an toàn – MSD, Nxb Trí thức, 2021.

13. Sổ tay hướng dẫn sinh hoạt Câu lạc bộ trẻ em, Công dân số chuẩn – World Vision, 2019.

14. Online is real – Save the Children, 2011.

15. Shin Yee Jin, Cha mẹ thời đại kỹ thuật số – Nxb Văn học, 2014.

16. Tài liệu dự án Swipe Safe – An toàn trên mạng – Tổ chức Child Fund tại Việt Nam, 2017.

17. Tài liệu An toàn bảo mật thông tin – TECHLAB.

Đáp án chi tiết

Câu hỏi thực hành 1:
Đáp án: A - 5, B - 1, C - 6, D - 3, E - 4, F - 2

Câu hỏi thực hành 2:
Đáp án: Độc giả trình bày theo ý kiến và quan điểm cá nhân

Câu hỏi thực hành 3:
Ví dụ:
Tên trẻ: Nam
Độ tuổi: C. Phát triển (8 tuổi)
Giai đoạn: A. 0 Internet B. Ươm mầm C. Phát triển D. Tiền trưởng thành
Mong muốn của bản thân: Bố mẹ mong muốn con sử dụng Internet có trách nhiệm

Câu hỏi thực hành 4:
Đáp án đúng: D

Câu hỏi thực hành 5:
Đáp án đúng: Tất cả các đáp án trên

Câu hỏi thực hành 6:
Đáp án đúng: A, D, H

Câu hỏi thực hành 7:
Đáp án: C. @Antoan_8456#

Câu hỏi thực hành 8:
Đáp án đúng: A, C, D, G.

Câu hỏi thực hành 9:
Đáp án: Cha mẹ hãy:
- Chia sẻ: Ngồi xuống chia sẻ cùng trẻ. Cám ơn con đã nói chuyện

và chia sẻ cùng cha mẹ; Cuộc trò chuyện phải đủ gần gũi, lắng nghe chân thành để con nói ra các cảm xúc của mình, nguyên nhân và mối quan hệ với các bạn đang trêu hoặc bắt nạt con trực tuyến;

- Phân tích cùng con việc các bạn trêu/ bắt nạt con trên mạng là đúng hay sai, phù hợp hay không phù hợp, liệu động cơ của các bạn là gì? ĐỘ nghiêm trọng tới đâu

- Cùng con phân tích 1 số giải pháp ứng phó:

✓ Tảng lờ: Mục đích của kẻ bắt nạt là muốn người bị nhắm mục tiêu sợ hãi, tức giận hoặc xấu hổ do đó hướng dẫn trẻ không nên phản hồi lại bắt nạt trực tuyến khiến cho kẻ bắt nạt đạt được mục đích và tiếp tục lặp lại hành động bắt nạt

✓ Chặn: Chặn (block) hoặc báo cáo vi phạm (report) người bắt nạt mình nếu hiện tượng bắt nạt tiếp diễn

✓ Chụp màn hình: Chụp lại màn hình những tình tiết bắt nạt trực tuyến làm bằng chứng phục vụ cho việc trình báo với các cơ quan chức năng

✓ Trao đổi: Nói với con trẻ những góc nhìn khác về vấn đề đang gặp phải. Chẳng hạn, nhiều trẻ lần đầu thấy những bình luận sốc và cảm thấy mọi thứ như sụp đổ. Nhưng nếu biết vấn đề này không to tát khi nhìn dưới lăng kính của người lớn, trẻ sẽ vững vàng hơn

✓ Nếu con tiếp tục phát hiện những bất thường, hoặc phát hiện bạn bè đang gặp các rủi ro, hãy lên tiếng cảnh báo bạn bè, nhanh chóng tìm kiếm sự trợ giúp của thầy cô, cha mẹ và hoặc các cơ quan chức năng, Tổng đài Quốc gia Bảo vệ trẻ em 111 hoặc báo cáo tới Mạng lưới ứng cứu bảo vệ trẻ em trên môi trường mạng tại địa chỉ "vn-cop.vn".

Câu hỏi thực hành 10:

Đáp án đúng: B, C, D, E, F, G, H, I, L

Giải thích thêm: Trẻ hoàn toàn có thể bị dụ dỗ trên mạng, dẫn tới gặp gỡ ngoài đời và là nạn nhân của bị hiếp dâm, xâm hại tình dục trực tiếp hoặc bị bắt cóc, buôn bán,...

Câu hỏi thực hành 11:

Đáp án đúng: A, C, D, E, H, I

MỤC LỤC