End Violence Against Children

World Vision VIỆT NAM

MSD

Hãy trở thành *Công dân số* CHUẨN

Sử dụng Internet thông minh, an toàn

Nhân vật chính của chúng ta là ai nhỉ?

Em Nấm

Chị Bơ

Anh Củ Cải

Chim hạc

Xây dựng nội dung: ThS. Nguyễn Phương Linh - ThS. Lưu Vũ Thùy Linh – Thiết kế: Lê Thị Loan

CÁC ĐẶC TÍNH CỦA INTERNET

- **Công khai:** Bất kỳ ai có Điện thoại thông minh hoặc máy tính đều có thể truy cập mạng internet và có thể đăng tin, tải lên và tải về các dữ liệu từ mạng internet. Nếu chúng ta sử dụng mạng internet hoặc có một "sự hiện diện trực tuyến", thì người khác có thể tìm thấy thông tin về chúng ta.
- **Vĩnh viễn:** Các thông tin, hình ảnh một khi đã được tải lên internet sẽ tồn tại vĩnh viễn, dù sau đó chúng ta có xóa chúng đi.
- **Kết nối:** nhờ internet chúng ta có thể giao tiếp, làm việc với những người khác nhau trên khắp thế giới.
- **Ẩn danh:** Chúng ta không thể biết danh tính thực của người chúng ta đang giao tiếp do không gặp mặt trực tiếp. Người xấu vì thế có thể giả danh một ai đó khác so với con người thực tế của họ.
- **Nguồn thông tin:** Internet cho phép tất cả mọi người đăng tải và chia sẻ thông tin, vì vậy không phải tất cả các thông tin trên internet đều chính xác hoặc đáng tin cậy.
- **Giới hạn và sự tôn trọng:** Văn hóa ứng xử ở ngoài đời thực cũng cần được áp dụng trên mạng. Hãy đặt ra những nguyên tắc cho bản thân, tôn trọng và giúp đỡ người khác trên internet.

CÔNG DÂN SỐ CHUẨN SNET

S – Safe – an toàn: Công dân số có kiến thức phân tích các đặc điểm của Internet để sử dụng internet an toàn như bảo mật thông tin, cài đặt riêng tư, đăng nhập an toàn, kết nối chọn lọc, v.v.

S – Smart – thông minh: Công dân số có các kỹ năng, tư duy logic và tư duy phản biện để biết cân nhắc khi chia sẻ các thông tin cá nhân và của người khác, quyết định tham gia hay không tham gia, ngăn chặn các rủi ro trên mạng internet, v.v.

S – SUPER – Siêu nhân: Công dân số biết ứng phó tìm kiếm các giải pháp, sống thật là mình và biết là hình mẫu, tấm gương để truyền cảm hứng cho các bạn thanh thiếu niên khác

SUPERB NET: Công dân số biết liên kết để có các mạng lưới cùng hỗ trợ nhau có các trải nghiệm tuyệt vời trên Internet.

"Khi tham gia sử dụng internet, chúng ta đã trở thành những công dân của thế giới trực tuyến. Hãy nhớ rằng, bên cạnh những Quyền lợi mà chúng ta có được trên mạng, chúng ta cũng cần có những trách nhiệm cụ thể. Quy tắc và văn hóa ứng xử ngoài đời thực cũng được áp dụng trong thế giới trực tuyến."

Chúng ta đều có những hình ảnh và dấu ấn cá nhân trên mạng (cũng như vân tay của chúng ta chẳng ai giống ai vậy), hãy đảm bảo rằng những dấu ấn và hình ảnh này nói lên con người thật của chúng ta

Sống ảo khiến nhiều người cố chạy theo một hình tượng mà mình mong muốn trong khi bỏ đi những giá trị thật của bản thân. Điều này ấn chứa rất nhiều những rủi ro như bắt nạt, lừa đảo, hoặc những vấn đề về tâm lý, v.v... Hãy Nói Không Với Sống Ảo

Các bạn hãy về nhà, xem lại tài khoản của mình và xác định những việc mình sẽ làm để bản thân có những dấu ấn cá nhân thật trên mạng.

NGƯNG SỐNG ẢO -

Xây dựng hình ảnh và dấu ấn thật trên mạng

BẠN BÈ & CÁC MỐI QUAN HỆ TRÊN MẠNG – CHỌN BẠN MÀ CHƠI

Trong khi tính kết nối của môi trường mạng giúp ta tìm kiếm và kết nối với bạn bè dễ dàng hơn, thì tính ẩn danh lại khiến cho việc chúng ta xác nhận một ai đó chính là con người thật của họ ở ngoài đời là rất khó khăn. Vì vậy, chúng ta cần phải biết được những rủi ro tiềm ẩn của những mối quan hệ trên mạng và đưa ra những tiêu chí phù hợp cho việc kết bạn.

Chúng ta cần đưa ra những tiêu chí phù hợp khi kết bạn với một ai đó:

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.

NÓI KHÔNG với BẮT NẠT TRÊN MẠNG

Bắt nạt trên mạng là khi một ai đó sử dụng công nghệ để quấy rối, đe dọa người khác (thông qua email, chat, trò chơi trực tuyến, tin nhắn, hình ảnh). Hành động này lặp đi lặp lại với cường độ thường xuyên khiến cho nạn nhân không có sức chống đỡ.

Có 07 loại bắt nạt trên mạng:

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).

Các Phương pháp bắt nạt trên mạng: Email, tin nhắn hoặc hình ảnh trực tuyến hoặc qua đt, trên web hoặc blog, group chat, trên mạng xã hội

Các cách để ứng phó với Bắt nạt trên mạng:

- Cài đặt quyền riêng tư trên mạng xã hội;
- Lờ đi (Ignore);
- Chặn tin nhắn, tài khoản;
- Lấy bằng chứng;
- Kêu gọi sự hỗ trợ của người thân và các cơ quan chức năng.

ĐỪNG HIỂU NHẦM VỀ XÂM HẠI TÌNH DỤC TRÊN MẠNG!

HIỂU BIẾT NGUY CƠ TRẺ EM BỊ XÂM HẠI TRÊN MẠNG

Bị xâm hại trên mạng là khi một ai đó bị

- Gửi và xem/ bắt xem những hình ảnh, nội dung về tình dục qua mạng;
- Nhắn tin, nói chuyện trên mạng về những nội dung tình dục;
- Có hành vi tình dục, trình diễn khiêu dâm hoặc bắt trẻ em trình diễn khiêu dâm qua webcam hoặc điện thoại thông minh;
- Bắt gửi ảnh, tin nhắn hoặc quay phim trẻ em có hành vi hoặc tư thế tình dục qua internet;
- Từ những hành động, tương tác trực tuyến dẫn tới việc gặp gỡ, và tham gia quan hệ tình dục ngoài đời thực.

THỦ THUẬT CỦA KẺ XÂM HẠI TÌNH DỤC TRẺ EM TRÊN MẠNG CẦN ĐỀ PHÒNG

Tiếp cận: Kẻ xâm hại thường tiếp cận đối phương qua các diễn đàn, qua mạng xã hội (các nhóm, hội), hay qua các chatroom;

Tạo niềm tin: Bằng cách khen ngợi, quan tâm, tặng quà và tiền khiến đối phương tin tưởng để từ đó điều khiển đối phương làm những điều mình muốn.

Tạo sự cảm thông: Khiến cho đối phương cảm thấy thương hại, dẫn đến việc có những hành động đáp ứng nhu cầu của kẻ xâm hại;

Liên tục đòi hỏi: Liên tục yêu cầu một điều gì đó mặc dù đối phương đã từ chối;

Lừa đảo tình dục (Sextortion): Yêu cầu đối phương phải gửi tiền, hoặc tiếp tục gửi ảnh hoặc video nhạy cảm của bản thân, hoặc phải gặp gỡ và quan hệ tình dục với kẻ xâm hại nếu không sẽ bị phát tán các hình ảnh riêng tư trên mạng.

CÁC QUY TẮC PHÒNG TRÁNH XÂM HẠI TRẺ EM TRÊN MẠNG

Hãy nhớ, trong quá trình trở thành một công dân số, và đặc biệt là khi gặp bất cứ vấn đề gì liên quan tới xâm hại tình dục trên mạng, các em hãy tìm tới các địa chỉ sau đây:

- Cha mẹ, thầy cô, người thân và bạn bè
- Tổng đài Quốc gia bảo vệ trẻ em 111
- Cảnh sát – đường dây nóng 113
- Các trung tâm công tác xã hội tỉnh/thành phố

Có những tiêu chí cụ thể khi kết bạn *(Tham khảo: Bạn bè và mối quan hệ trên mạng)*

Mỗi người đều có quyền kiểm soát cơ thể mình và chúng ta hoàn toàn có thể nói "Không" khi không muốn điều gì đó;

Chúng ta không có trách nhiệm cung cấp tên, gửi ảnh hay cho người khác nhìn thấy mình qua webcam. Không nên gặp bạn bè trên "mạng" một mình mà không hỏi ý kiến người thân;

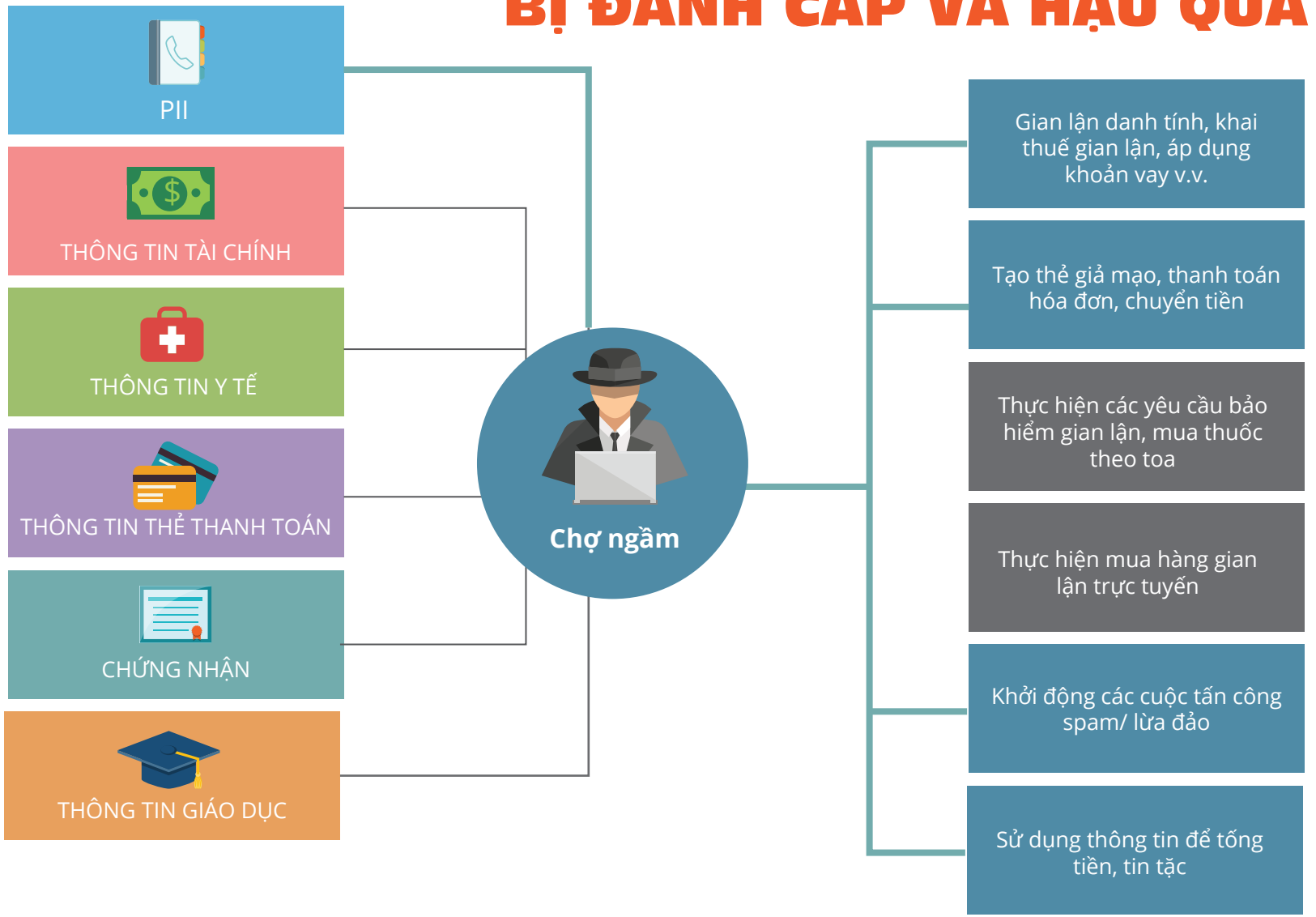
Không nên đăng tải thông tin riêng tư, cá nhân hay những hình ảnh tự sướng có tính chất hở hang, cũng như đặt những nickname không phù hợp vì đó là kẽ hở để kẻ xấu lợi dụng;

Sử dụng các công cụ báo cáo, chặn khi thấy có những nội dung hoặc người kết bạn không phù hợp;

Khi nhắn tin và gặp các tin nhắn khiêu khích tình dục, bạn cần ngừng nhắn tin, chặn và báo lại cho cha mẹ, thầy cô;

Bạn không bao giờ là người phải xấu hổ hay có lỗi khi có một ai có ý định hoặc đã xâm hại tình dục bạn. Hãy lên tiếng để được trợ giúp.

CÁC THÔNG TIN CÓ THỂ BỊ ĐÁNH CẮP VÀ HẬU QUẢ



Người dùng có có nhiều loại thông tin khác nhau, có thể bị đánh cắp hoặc bị lộ bởi phần mềm độc hại, hacking, v.v.

Hầu hết các thông tin bị đánh cắp này đều bị bán dưới các thị trường ngầm

Tùy thuộc vào loại thông tin, các hacker và cybercriminals có thể được sử dụng theo những cách khác nhau theo nhiều cách khác nhau

LỪA ĐẢO TRÊN MẠNG VÀ CÁCH PHÒNG TRÁNH

CÁC PHƯƠNG PHÁP LỪA ĐẢO PHỔ BIẾN TRÊN MẠNG

- Đánh cắp thông tin cá nhân thông qua các thông báo trúng thưởng, email không rõ nguồn gốc
- Thanh toán và giao dịch trực tuyến
- Lừa đảo thông qua nhờ vả hoặc đe dọa trên mạng xã hội

CÁC CÁCH PHÒNG TRÁNH LỪA ĐẢO TRÊN MẠNG

- Luôn nhớ rằng thông tin cá nhân của mỗi chúng ta là rất quan trọng và không thể cho đi dễ dàng;
- Luôn kiểm tra website cũng như thông tin, uy tín của nhà cung cấp trước khi thực hiện các giao dịch trực tuyến;
- Không vội vàng tin vào những lời nhờ vả hoặc đe dọa trên mạng xã hội;
- Chia sẻ với người thân, bạn bè, hoặc thầy cô để được tư vấn giúp đỡ. Gọi công an hoặc tổng đài 111 để được tư vấn, hỗ trợ khi cần thiết.

TRÒ CHƠI ĐIỆN TỬ - GAME ĐỦ, GAME ĐÚNG CÁCH, GAME TÍCH CỰC

Chơi game online không phải là xấu nếu người chơi biết lựa chọn những trò chơi phù hợp, và chơi có chừng mực.

Lựa chọn những trò chơi phù hợp với lứa tuổi, văn hóa, và có tính chất giáo dục;

Không chơi game có chứa yếu tố bạo lực, đánh bạc, khiêu dâm hoặc sai lệch về đạo đức;

Sắp xếp thời gian phù hợp khi chơi game (không quá 8h/tuần) để không ảnh hưởng tới những hoạt động khác trong cuộc sống;

Game đủ, Game đúng cách, Game tích cực là rất cần thiết đối với mỗi chúng ta.

PHÂN BIỆT CÁC LOẠI THÔNG TIN TRÊN MẠNG

Có 03 loại thông tin chính mà chúng ta thường gặp trên mạng xã hội:

- **Thông tin về bản thân:**
  Là những cảm xúc, hoạt động, địa điểm của bản thân mà chúng ta chia sẻ trên mạng xã hội;

- **Thông tin về người khác:**
  Là những cảm xúc, hoạt động, địa điểm mà bạn của chúng ta chia sẻ trên mạng xã hội;

- **Thông tin được chia sẻ lại về một sự vật, sự việc hoặc hiện tượng nào đó có thể do người thân, bạn bè hoặc được quảng cáo trên mạng xã hội:**
  Thông tin này thường được chia sẻ dưới dạng đường link gắn vào website; hoặc một bài viết của một ai đó về một sự vật, sự việc hoặc hiện tượng họ đã chứng kiến hoặc trải qua.

Việc chia sẻ, bình luận hay bày tỏ cảm xúc thể hiện văn hóa cá nhân khi tham gia mạng xã hội. Ngoài việc ảnh hưởng tới văn hóa cá nhân, thì nó còn ảnh hưởng tới sự an toàn của chúng ta và bạn bè.

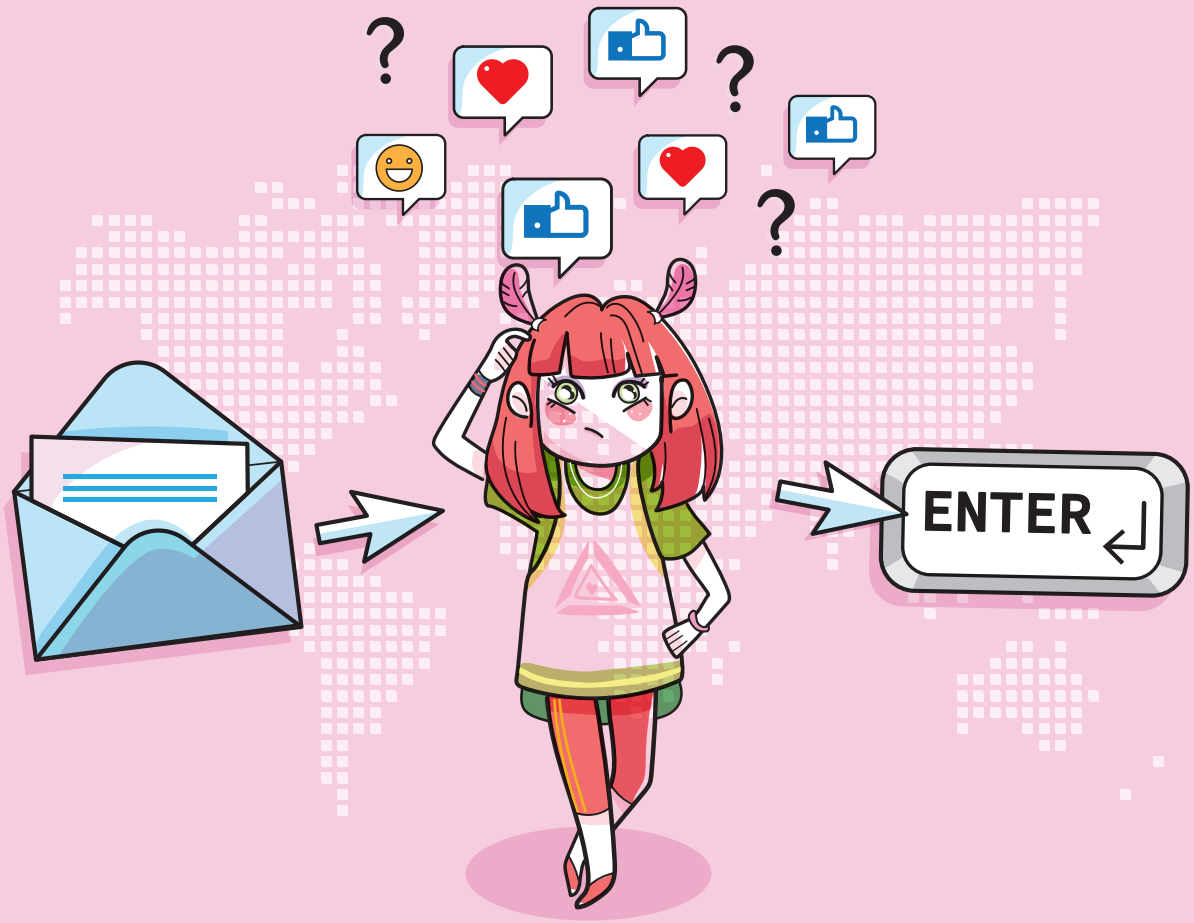
Những điều bạn đã share, comment sẽ không bao giờ mất đi, nó có thể được tiếp tục chia sẻ nhanh hơn bạn nghĩ và nó có thể gây ảnh hưởng đến các bạn sau này (sai 1 like, bay vạn dặm).

Đối với thông tin của bản thân, hãy luôn nhớ:

- Đảm bảo việc chia sẻ thông tin không ảnh hưởng đến sự an toàn của bạn;
- Đảm bảo việc chia sẻ thông tin không ảnh hướng tới hình ảnh/văn hóa/giá trị mà bạn đang thể hiện;
- Đâu là những thông tin nên chia sẻ, đâu là những thông tin không nên chia sẻ. Những giới hạn này giúp chúng ta tránh mắc phải những rủi ro để lộ thông tin, dẫn tới mất an toàn của bản thân.

Đối với thông tin của bạn bè hay người thân, hãy luôn nhớ:

- Không tương tác với những thông tin có thể gây mất an toàn cho họ;
- Không tương tác với những thông tin có thể gây ảnh hưởng tới hình ảnh/văn hóa/giá trị mà họ mong muốn thể hiện. Vì vậy, bạn hãy đặt mình vào vị trí của người khác trước khi tương tác với những trạng thái của họ hay về họ;
- Nếu bình luận hay chia sẻ với bất cứ trạng thái nào của bạn bè hay người thân, hãy cách bình luận và chia sẻ mang tính xây dựng, sử dụng từ ngữ lịch sự, không đùa cợt, nói tục, chửi bậy, v.v.



LIKE, SHARE, COMMENT CÓ VĂN HOÁ – GIỚI HẠN VÀ SỰ TÔN TRỌNG

LIKE, SHARE, COMMENT CÓ TƯ DUY PHẢN BIỆN

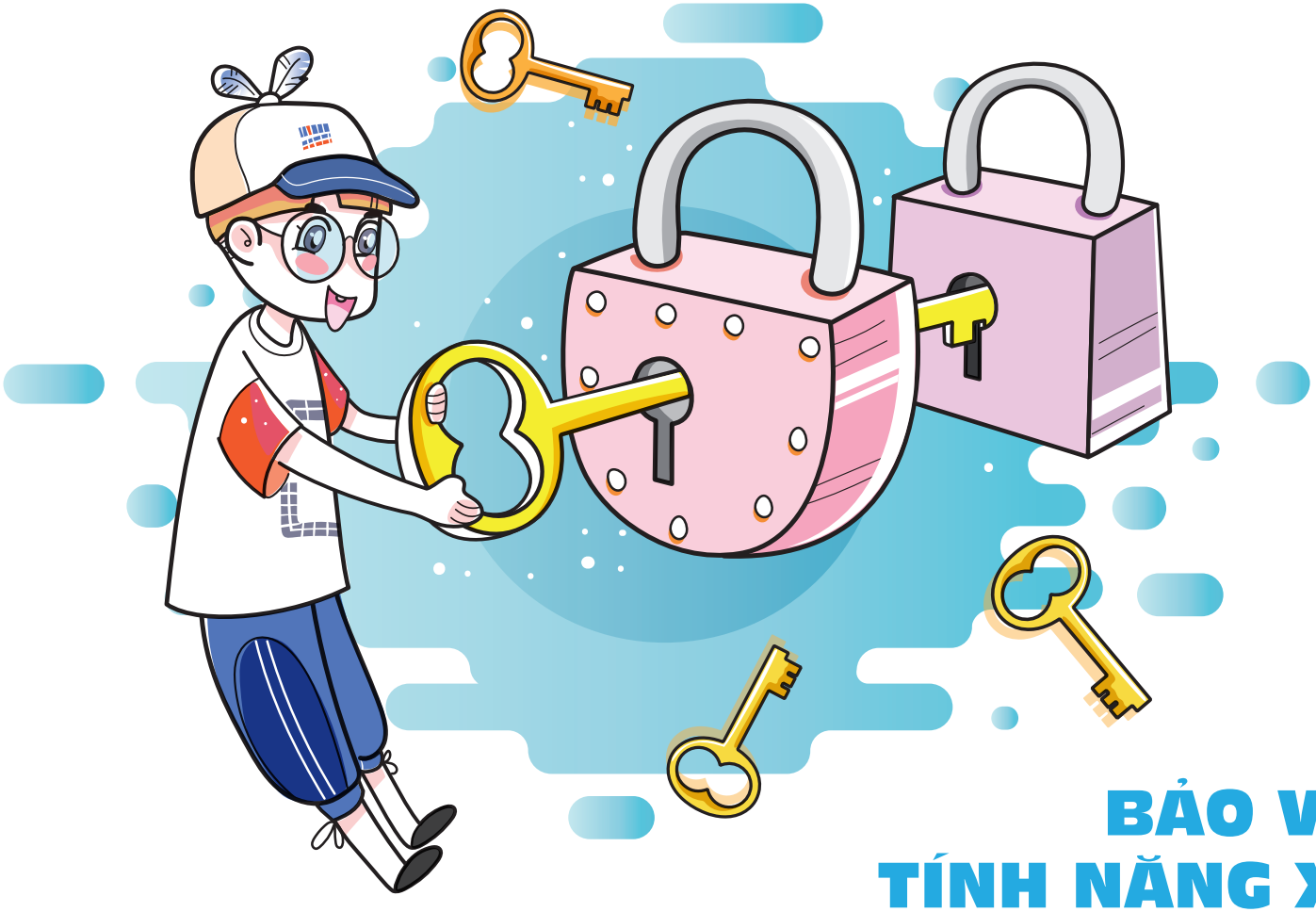
Tuy duy phản biện là khả năng kiểm chứng một vấn đề thông qua quá trình kiểm tra, phân tích, đánh giá để khẳng định tính chính xác của vấn đề đó

Hãy luôn kiểm chứng thông tin trên mạng xã hội bằng tư duy phản biện trước khi tương tác, bình luận hay chia sẻ trên mạng xã hội, bằng cách:

- Không vội vàng, đọc lướt; Kiểm tra và đối chiếu các nguồn tin khác nhau về một vấn đề, Kiểm tra Trích nguồn, tác giả và Chứng cứ lập luận; Nếu đươc trích nguồn, kiểm tra nguồn đó có đang tín tưởng không (ví dụ về website như ở trên); Hình ảnh đúng không có nghĩa nội dung đúng;
- Việc chia sẻ những thông tin sai lệch sẽ ảnh hưởng tới thông tin của cả một cộng đồng, gây ra những hậu quả khó lường và nên nhớ em hoàn toàn có thể IM LẶNG hoặc BÁO CÁO những thông tin không chính xác trên mạng xã hội.

GIỮ AN TOÀN CHO TÀI KHOẢN QUA CÀI ĐẶT MẬT KHẨU MẠNH

- Sử dụng mật khẩu khó đoán, có ít nhất 6 ký tự, kết hợp số, chữ in hoa và cả in thường, và ký tự đặc biệt.
- Sử dụng mật khẩu khác nhau cho tài khoản khác nhau
- Không chia sẻ mật khẩu với người khác. Thay đổi mật khẩu cho tài khoản ít nhất 6 tháng 1 lần



BẢO VỆ TÀI KHOẢN QUA TÍNH NĂNG XÁC THỰC HAI LỚP

BẢO VỆ HAI LỚP VÀ THIẾT LẬP CẢNH BÁO

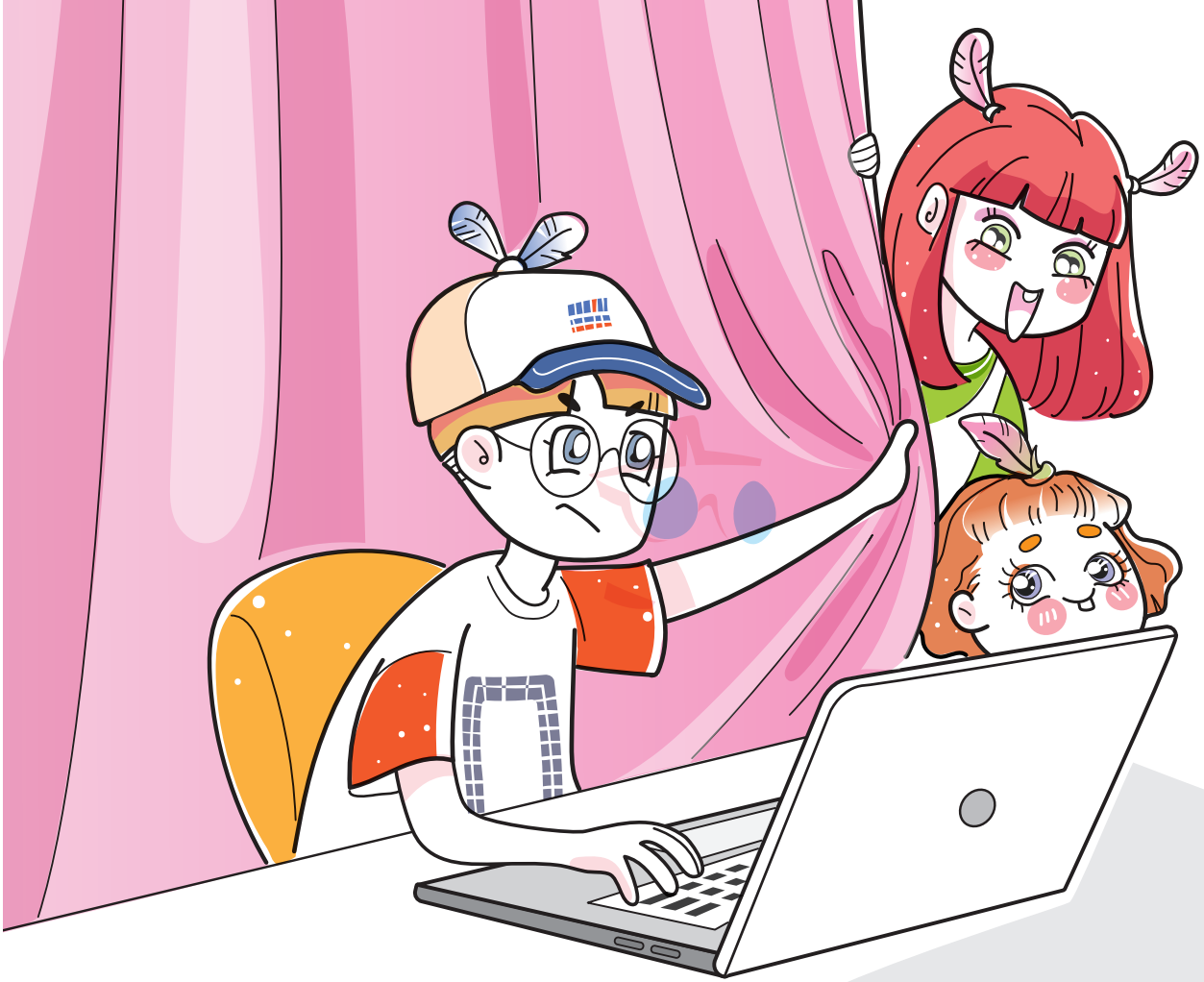
Tính năng xác thực 2 lớp: Mã xác thực mỗi khi bạn đăng nhập vào tài khoản email hoặc mạng xã hội bằng máy tính mới. Nếu người lạ cố gắng xâm nhập vào tài khoản của bạn, họ sẽ không thể đăng nhập được vì không có mã khóa này

Thiết lập cảnh báo: Một số ứng dụng email hoặc mạng xã hội có chức năng cảnh báo khi có ai đó khác đăng nhập vào tài khoản của bạn. Cảnh báo này sẽ cho bạn biết thiệt bị nào đang cố gắng đăng nhập vào tải khoản của bạn cũng như vị trí đăng nhập

GIỮ AN TOÀN CHO TÀI KHOẢN
Đăng nhập an toàn

Đăng nhập sẽ là khi bạn dễ sơ ý để lộ thông tin nhất, hãy nhớ:

- *Không sử dụng tài khoản Face-book hay Google, ... để đăng nhập vào nền tảng khác;*
- *Hạn chế chọn ´lưu mật khẩu´ khi đăng nhập;*
- *Hạn chế sử dụng thiết bị công cộng, hoặc lưu ý đăng xuất khi bạn dùng thiết bị công cộng để truy cập tài khoản.*



AI CŨNG CÓ QUYỀN RIÊNG TƯ

Quyền riêng tư là quyền của cá nhân được tôn trọng và được luật pháp bảo vệ. Việc thu thập, công bố thông tin, tư liệu về đời tư của cá nhân phải được người đó đồng ý. Thư tín, điện thoại, điện tín, các phương tiện thông tin điện tử khác của cá nhân được bảo đảm an toàn và bí mật.

Chúng ta đều có quyền riêng tư, và riêng tư của mỗi người là không giống nhau

Giới hạn riêng tư của mỗi người là khác nhau tuỳ vào mục tiêu, sở thích, mong muốn, và các đặc điểm tính cách khác, v.v. Điều quan trọng ở chỗ, mỗi người đều phải xác định giới hạn riêng tư phù hợp đối với bản thân mình, lường trước được các rủi ro ở mỗi giới hạn để quyết định cài đặt riêng tư phù hợp.

RIÊNG TƯ TRÊN MẠNG:

Chúng ta được quyền quyết định mình chia sẻ những thông tin nào, và chia sẻ thông tin đó với ai, ai được phép chia sẻ hoặc gửi thông tin của chúng ta;

Được quyền quyết định mình xem hay không xem thông tin gì, mà không bị làm phiền.

Đối với trình duyệt trang điện tử (web): Cài đặt riêng tư giúp bạn duyệt các trang web an toàn, kiểm soát thông tin trang web có thể sử dụng và nội dung trang web có thể hiện thị cho bạn, lưu lịch sử, dịch vụ gợi ý để hoàn thành tìm kiếm, v.v.

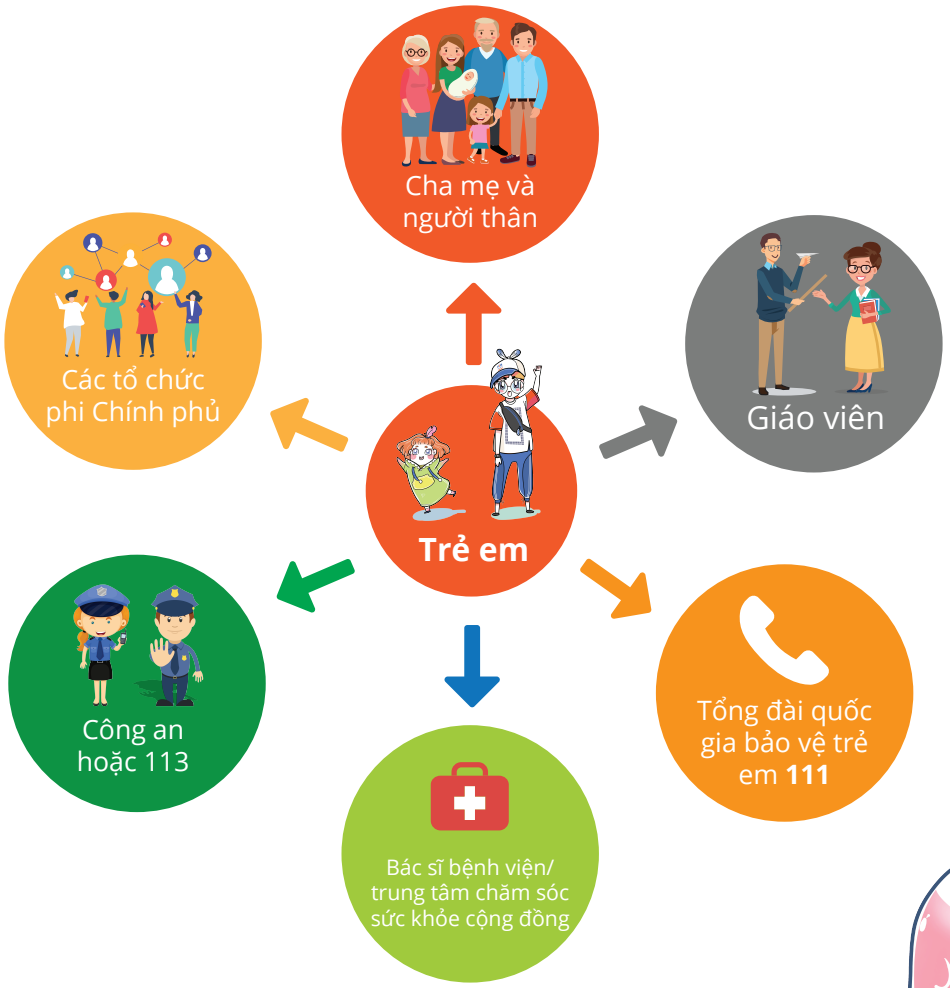
Mạng xã hội: chế độ cài đặt riêng tư cho phép các tính năng khác nhau (dòng thời gian, gắn thẻ, địa điểm, chế độ người xem)

ẢNH TỰ SƯỚNG (SELFIE) –
Sướng mà an toàn

Các bức ảnh selfie không an toàn là các bức ảnh:

- Những bức ảnh 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;
- Những bức selfie cho thấy những phần cơ thể riêng tư luôn luôn là không an toàn;
- Những bức selfie có thể làm ô uế danh tiếng của bạn là không an toàn (ví dụ như một bức selfie 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; v.v.

MẠNG LƯỚI BẢO VỆ TRẺ EM



Để sử dụng mạng lưới hỗ trợ hiệu quả, chính trẻ em phải là những người chủ động:

Em cần xác định những người hỗ trợ có thể giúp gì được cho em: lắng nghe, đưa ra lời khuyên, hỗ trợ em chuyển gửi tới những đơn vị cần thiết (ví dụ: đưa em tới bác sỹ, báo với công an hoặc gọi điện cho Tổng đài quốc gia bảo vệ trẻ em), v.v.

Mạng lưới hỗ trợ là những người em muốn tin tưởng và họ cũng tin tưởng em, tôn trọng em, do đó, việc giữ liên lạc thường xuyên, trao đổi chia sẻ cả chuyện tốt lẫn không tốt, dành thời gian để duy trì mối quan hệ là vô cùng quan trọng.

Nếu em có vấn đề cần được giúp đỡ, nhưng người hỗ trợ trong mạng lưới không tin hoặc không làm gì thì em cần tiếp tục kiên trì thuyết phục người hỗ trợ đó tin em và hành động. Nếu người hỗ trợ vẫn không tin và không giúp thì em cần tìm sự giúp đỡ từ người hỗ trợ khác trong mạng lưới. Hãy kiên trì thuyết phục cho đến khi có người tin em và hỗ trợ em.

"Hãy tin rằng em không một mình, luôn có những người lớn/ các cơ quan tổ chức sẵn sàng giúp đỡ và hỗ trợ trẻ em để phòng tránh các rủi ro trên môi trường mạng và cả trong cuộc sống."

THÔNG TIN LIÊN HỆ

Viện Nghiên cứu Quản lý Phát triển bền vững (MSD)

A: Tầng 6, Số 15 Yên Lãng, Đống Đa, Hà Nội
T: (84-24)-6276 9056 - E: contact@msdvietnam.org
FB: Msd Vietnam - W: msdvietnam.org

Tổ chức Tầm nhìn Thế giới Quốc tế tại Việt Nam

Tầng 9, Tòa nhà Mercury, 444 Hoàng Hoa Thám, Tây Hồ, Hà Nội
T: (84-24) 3943 9920
FB: worldvisioninvietnam - W: www.wvi.org/vietnam

World Vision Vietnam gratefully acknowledges financial support provided for this Programme by **the Fund to End Violence Against Children**

TRẢI NGHIỆM TRÊN INTERNET CÓ TUYỆT VỜI HAY KHÔNG DO CHÍNH BẠN QUYẾT ĐỊNH!

Hãy là những Công dân số chuẩn!