TỔ CHỨC BỘ CÔNG AN CỤC AN NINH MẠNG VÀ PHÒNG CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO | DẪN DẮT CHIẾN DỊCH DTA | ĐỒNG HÀNH PVcomBank MB AGRIBANK

CẨM NANG

CÙNG NHAU AN TOÀN TRỰC TUYẾN

#01MINH
#KHONGMOTMINH
#CONGUOCHANOI
#NIEMTINSO

#01MINH
#KHONGMOTMINH
#CONGUOCHANOI
#NIEMTINSO

MỤC LỤC

01101101 11100001 10111011 10011111 00100000
11000100 10010001 11100001 10111010 10100111
01110101

(LỜI)

MỞ ĐẦU

Một tin nhắn Zalo, một lời nhắc “giữ bí mật”, một đoạn giấy tờ giả mạo – và chỉ trong vài giờ, một cô gái hay một cậu học sinh bình thường có thể trở thành “nạn nhân tự nguyện” của một kịch bản tội phạm tinh vi.

Có bao giờ
bạn nghĩ rằng
một cuộc gọi
[tưởng chừng vô hại]
lại có thể thay đổi
hoàn toàn
↳ cuộc đời
của một người?

Đó chính là bản chất của bắt cóc online.

Không tiếng kêu cứu vang lên từ căn phòng tối. Không có sợi dây thừng trói tay trói chân.

Nhưng bằng những chiêu trò tâm lý, kẻ xấu khiến nạn nhân tự cô lập, tự quay clip nhạy cảm, tự tìm cách vay tiền, và thậm chí tự rời khỏi nhà để đến những nơi xa lạ.

Điểm nguy hiểm nằm ở chỗ: tất cả những gì chúng cần chỉ là một chiếc điện thoại và một vài dữ liệu cá nhân có sẵn trên mạng. Còn phần còn lại – nỗi sợ, sự hoang mang, niềm tin mù quáng – chính nạn nhân sẽ tự bù đắp.

Cuốn cẩm nang này không chỉ liệt kê thủ đoạn hay dặn dò sáo rỗng. Nó kể lại những câu chuyện đã từng xảy ra, với những con người thật, những gia đình thật. Bạn sẽ thấy mình hoặc người thân đâu đó trong những tình huống này. Và từ những câu chuyện, chúng ta cùng nhau học cách nhận diện, cách giữ bình tĩnh, cách thoát ra khỏi chiếc bẫy vô hình ấy.

Hãy đọc cuốn sách này như thể bạn đang nghe một người bạn tin cậy kể lại, chứ không phải một bài giảng cứng nhắc.

Vì điều chúng ta cần không chỉ là kiến thức, mà là sức mạnh tinh thần để dám nói "không", dám chia sẻ và dám tìm sự giúp đỡ.

(PHẦN 01)

01

NHỮNG CON SỐ BIẾT NÓI

Lừa đảo, dụ dỗ, thao túng trực tuyến đang trở thành một "cơn bão ngầm" đe dọa an ninh mạng và tinh thần xã hội tại Việt Nam, gây thiệt hại lớn không chỉ về tài chính mà còn về sức khỏe tâm lý của nhiều người. Theo báo cáo của Hiệp hội An ninh mạng quốc gia (NCA) công bố cuối năm 2024, **Việt Nam nằm trong nhóm các quốc gia bị ảnh hưởng nặng nề nhất bởi tội phạm mạng.**

THIỆT HẠI ƯỚC TÍNH LÊN ĐẾN

18.900

TỶ ĐỒNG CHỈ TRONG NĂM 2024 – tăng gấp đôi so với năm 2023 (khoảng 8.000 - 10.000 tỷ đồng), theo thống kê từ Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

220

người dùng smartphone thì có **1 NGƯỜI** trở thành nạn nhân

TỶ LỆ "NẠN NHÂN TIỀM NĂNG" ĐÁNG BÁO ĐỘNG

70%

NGƯỜI DÂN TIẾP XÚC VỚI ÍT NHẤT MỘT CUỘC GỌI HOẶC TIN NHẮN LỪA ĐẢO MỖI THÁNG.

Những con số này không chỉ là thống kê khô khan, mà là tiếng kêu cứu từ thực tế: Năm 2023, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Bộ Công an đã xử lý hơn **1.500 vụ án lừa đảo trực tuyến**, chủ yếu liên quan đến chiếm đoạt tài sản qua mạng. Đến năm 2024, con số vụ việc tiếp tục tăng vọt, với hơn **22.200 phản ánh về lừa đảo trực tuyến** được ghi nhận chỉ trong 9 tháng đầu năm. Tội phạm không chừa một ai – từ học sinh, sinh viên đến người lao động, thậm chí cả những người am hiểu công nghệ.

1.500

VỤ ÁN LỪA ĐẢO TRỰC TUYẾN

22.200

PHẢN ÁNH VỀ LỪA ĐẢO TRỰC TUYẾN

Tuy nhiên, năm 2025 chứng kiến sự chuyển dịch đáng lo ngại: Các đối tượng tập trung "săn mồi" nhằm vào giới trẻ, đặc biệt là học sinh, sinh viên, những người thiếu kỹ năng sống và dễ bị thao túng tâm lý. Thủ đoạn mới nổi lên - **“bắt cóc online”** - đang trở thành mánh khóe tinh vi, biến nạn nhân thành “tù nhân tinh thần” từ xa.

"BẮT CÓC ONLINE"

là gì?

ĐÂY LÀ BIẾN THỂ NGUY HIỂM CỦA LỪA ĐẢO TRỰC TUYẾN, NƠI TỘI PHẠM SỬ DỤNG CÔNG NGHỆ ĐỂ THAO TÚNG TÂM LÝ, ÉP NẠN NHÂN CẮT ĐỨT KẾT NỐI VỚI THẾ GIỚI BÊN NGOÀI, RỒI TỐNG TIỀN GIA ĐÌNH HOẶC BUÔN NGƯỜI.

Theo dữ liệu sơ bộ từ Bộ Công an, từ giữa năm 2024 đến tháng 8/2025, ghi nhận **khoảng 50 vụ việc**, giải cứu thành công **50 nạn nhân** – trong đó **90% là nữ giới (45 trường hợp)** và **10% nam giới (5 trường hợp), 100% thuộc nhóm tuổi 18-22**, chủ yếu là sinh viên xa nhà. Thiệt hại tài chính lên đến hàng tỷ đồng, chưa kể tổn thương tâm lý kéo dài.

50

VỤ VIỆC

50

NẠN NHÂN

NỮ GIỚI
(45 TRƯỜNG HỢP)

90%

NAM GIỚI
(5 TRƯỜNG HỢP)

10%

100%

THUỘC NHÓM
TUỔI 18-22

Thủ đoạn của chúng được chuẩn bị kỹ lưỡng theo một kịch bản dựng sẵn:

Bắt đầu bằng giả mạo thông tin (mạo danh công an, viện kiểm sát, tòa án qua cuộc gọi hoặc tin nhắn, cáo buộc nạn nhân liên quan đến ma túy, rửa tiền với "bằng chứng" giả mạo như lệnh bắt, hồ sơ cá nhân).

Nạn nhân nhanh chóng rơi vào hoảng loạn, bị thao túng tâm lý (yêu cầu giữ bí mật tuyệt đối, tháo SIM, bật chế độ máy bay, chỉ liên lạc qua ứng dụng OTT như Zalo, Telegram; hướng dẫn di chuyển đến nơi kín đáo như khách sạn, nhà nghỉ, hoặc thậm chí biên giới – báo vị trí định kỳ mỗi giờ).

Chúng còn ép cung cấp hình ảnh/video nhạy cảm hoặc tự tạo dấu vết "hành hung" để tăng tính thuyết phục.

Sau khi cô lập nạn nhân, tội phạm chuyển sang tống tiền gia đình:

Sử dụng tài khoản mạng xã hội của nạn nhân (hoặc giả mạo) để gửi thông báo “bị bắt cóc”, kèm đe dọa kinh hoàng như bán nội tạng, xuất cảnh trái phép, hoặc phát tán nội dung nhạy cảm. Yêu cầu chuyển tiền ngay lập tức (từ hàng trăm triệu đến vài tỷ đồng vào tài khoản chỉ định), và thường “kéo dài” bằng lý do giả tạo như “tăng tiền chuộc” hoặc “phát sinh chi phí”.

Quá trình này chỉ dừng khi gia đình kiệt quệ tài chính hoặc lực lượng chức năng can thiệp. Hậu quả không dừng ở tiền bạc: Nạn nhân thường rơi vào sốc tâm lý, lo âu kéo dài, gia đình sa sút tinh thần, xã hội lan tỏa nỗi bất an – đặc biệt với cha mẹ có con học xa nhà.

Tình hình năm 2025:

CẢNH BÁO ĐỎ!

Từ tháng 7/2025 - đúng mùa nhập học – thủ đoạn này bùng nổ với quy mô lớn hơn, tập trung tại các đô thị lớn:

Thành phố Hồ Chí Minh (25 vụ), Cần Thơ (7 vụ), Hà Nội (5 vụ), Đà Nẵng (2 vụ) và các tỉnh biên giới như Tây Ninh (5 vụ), Quảng Ninh (3 vụ).

Dù cơ quan chức năng, báo chí, nhà trường liên tục tuyên truyền nhưng vẫn có rất nhiều người sập bẫy vì những công nghệ mới (AI giả giọng nói, giả khuôn mặt...) bị lợi dụng và nỗi sợ hãi bản năng. Nếu thiếu cảnh giác, đặc biệt trong giai đoạn cao điểm như năm học mới, nguy cơ sẽ tiếp tục gia tăng, đe dọa thế hệ trẻ - tương lai của đất nước.

Những con số không chỉ "biết nói" mà còn "kêu cứu": An toàn trực tuyến không phải chuyện của riêng ai, mà là trách nhiệm chung để bảo vệ thế hệ mai sau.

(PHẦN 02)

NHỮNG CÂU CHUYỆN CÓ THẬT

NHỮNG CÂU CHUYỆN DƯỚI ĐÂY LÀ NHỮNG TRẢI NGHIỆM ĐAU LÒNG CỦA CÁC THANH THIẾU NIÊN TẠI VIỆT NAM, NƠI SỰ NGÂY THƠ VÀ THIẾU CẢNH GIÁC ĐÃ BỊ TỘI PHẠM TRỰC TUYẾN LỢI DỤNG.

Mỗi câu chuyện là một bài học sống động, cho thấy cách tội phạm giăng bẫy để cô lập nạn nhân, từ những lời đe dọa lạnh lùng đến những màn kịch tinh vi.

Nhưng đồng thời, chúng cũng là minh chứng cho sức mạnh của sự kết nối, khi gia đình, bạn bè hoặc cộng đồng kịp thời can thiệp, nạn nhân đã được kéo ra khỏi lằn ranh nguy hiểm.

NHỮNG CÂU CHUYỆN NÀY LÀ LỜI CẢNH BÁO, NHƯNG CŨNG LÀ ÁNH SÁNG HY VỌNG, NHẮC NHỞ RẰNG KHÔNG AI PHẢI ĐỐI MẶT VỚI TỘI PHẠM MỘT MÌNH.

01

PHÒNG ZOOM KHÔNG CÓ CỬA SỔ

Linh, sinh viên năm nhất một trường đại học tại Hà Nội, đi học xa nhà nên phải thuê trọ. Sáng Chủ nhật, ngày 05/01/2025, đang ở phòng trọ, Linh nhận được cuộc gọi từ số lạ. Người đàn ông ở đầu dây tự xưng là cán bộ Cục Cảnh sát Hình sự, khẳng định Linh liên quan đến đường dây rửa tiền và đe dọa sẽ ra lệnh bắt giữ nếu không hợp tác.

Để tăng tính thuyết phục, đối tượng xấu lập tức gửi qua Zalo nhiều giấy tờ có hình ảnh, tên, ngày sinh, số căn cước công dân, địa chỉ nơi ở của Linh. Trước những thông tin cá nhân trùng khớp, Linh hoang mang và bắt đầu tin rằng mình thật sự bị điều tra.

> **“Em phải làm theo hướng dẫn. Tắt máy, không được liên lạc với bố mẹ, nếu không gia đình sẽ bị liên lụy. Sau đó, truy cập ngay phòng Zoom theo đường link chúng tôi gửi” - đối tượng ra lệnh.**

Linh làm theo, trong Zoom có nhiều đối tượng dàn cảnh đang trong giờ làm việc tại cơ quan Công an với nhiều người mặc quân phục, ngồi trước “bàn làm việc”. Họ đọc điều khoản pháp luật, giọng điệu chắc nịch, rồi yêu cầu Linh phối hợp để “phục vụ điều tra”; muốn chứng minh danh tính, minh oan cần cung cấp hình ảnh cá nhân, quay một số đoạn video để xác thực.

Trong trạng thái sợ hãi, Linh tuân thủ không chút nghi ngờ. Khi thủ tục này hoàn tất, nhóm đối tượng tiếp tục yêu cầu:

> **“Ngày mai, em phải lên xe khách vào TP. HCM để làm việc trực tiếp. Sẽ có người đón. Tuyệt đối không được báo cho gia đình, nếu không hậu quả sẽ rất nặng nề”.**

Những cuộc điện thoại, những phiên làm việc qua Zoom liên tục diễn ra khiến Linh hoảng sợ, bị thao túng tâm lý và tin rằng im lặng và nghe lời là cách duy nhất để không ảnh hưởng đến gia đình và việc học tập của bản thân.

Tối cùng ngày, Linh được yêu cầu rời khỏi nhà trọ và đến nhiều địa điểm khác nhau. Khi Linh rơi vào tình trạng mệt mỏi về thể xác và tinh thần, cùng với thời điểm tối muộn, chúng yêu cầu Linh thuê khách sạn để đảm bảo an toàn, bí mật và tiếp tục cung cấp thông tin phục vụ quá trình điều tra.

Tại khách sạn, Linh tiếp tục bị gieo rắc suy nghĩ phải tự chứng minh mình "vô tội", như có khả năng tài chính, nguồn tiền sạch, không liên quan đến rửa tiền, ma túy. Khi biết Linh không có đủ tiền trong tài khoản, chúng hướng dẫn Linh tự dàn cảnh bị bắt cóc để gia đình chuyển tiền chuộc.

Trong trạng thái sợ hãi, Linh tuân thủ không chút nghi ngờ

Linh đồng ý, tự làm rối tóc, ướt quần áo, tự gây thương tích lên tay chân, sử dụng dây rèm cửa buộc chân, buộc tay,... và quay video clip gửi cho các đối tượng.

Các đối tượng sau đó gọi điện yêu cầu gia đình chuyển 500 triệu chuộc con. Trong đêm, các đối tượng liên tục gửi hình ảnh, clip để gây áp lực và đe dọa chuyển tiền ngay nếu không Linh sẽ nguy hiểm tới tính mạng.

Tìm mọi cách nhưng không liên lạc được, quá lo lắng vì sự an toàn của con, bố mẹ Linh đã vay mượn 500 triệu đồng chuyển cho các đối tượng.

Cùng diễn biến đó, gia đình lo lắng đã báo Công an. Trưa hôm sau, Linh được tìm thấy và "giải cứu" tại khách sạn.

02

GÓI HÀNG "ĐÃ NHẬN"

Tâm là nữ sinh lớp 12 trường THPT tại Hà Nội, em là học sinh giỏi toàn diện, bố mẹ là công chức Nhà nước, em là chị gái trong gia đình có hai chị em. Tâm thường đặt, mua đồ dùng học tập, tặng phẩm trên một số sàn thương mại điện tử.

Trưa ngày 21/7/2025, vừa đi học về Tâm nhận thông báo từ ứng dụng thương mại điện tử: "Đơn hàng của bạn đã được giao thành công". Tâm ngạc nhiên vì gần đây mình không đặt hàng.

Ít phút sau, một cuộc gọi từ số lạ, giọng người đàn ông nghiêm nghị:

> **"Chúng tôi là cơ quan chức năng. Gói hàng vừa rồi đã bị giữ vì liên quan đến đường dây vận chuyển ma túy. Người đứng tên nhận chính là em"**

Tâm hoảng hốt:

> **"Nhưng... em không đặt gì hết!".**
>
> **"Không cần chối. Trong hệ thống ghi rõ tên em. Nếu muốn minh oan, phải hợp tác ngay. Chúng tôi sẽ mở phòng Zoom để em làm việc với đại diện công an, viện kiểm sát, tòa án. Nếu từ chối, em sẽ bị bắt ngay lập tức" - đối tượng đe dọa.**

Do sợ hãi, Tâm làm theo, nhấn vào đường link Zoom. Trong cuộc gọi Zoom là ba người mặc quân phục cảnh sát, phía trước là "bàn làm việc", phía sau có phông nền giống như tại trụ sở cơ quan Công an. Một người đập bàn, quát lớn:

> "Em phải chứng minh bản thân trong sạch. Mở camera, quay video xác minh toàn thân ngay".

Trước việc liên tục bị gây áp lực, đe dọa, thao túng tâm lý, Tâm làm theo.

Sau đó, các đối tượng yêu cầu Tâm cắt liên lạc với gia đình, thuê phòng khách sạn để đảm bảo bí mật quá trình điều tra. Tại phòng thuê trong khách sạn, Tâm nhận được tin nhắn từ đối tượng xấu, nội dung gồm hình ảnh, video nhạy cảm của bản thân vừa quay kèm lời đe dọa:

> “Chuyển ngay 450 triệu đồng nếu không muốn những bức hình này đăng lên mạng”.

Tâm bàng hoàng, chưa kịp định thần thì một cuộc gọi khác tới:

> **“Hãy liên lạc với người thân, nói cần tiền gấp để làm hồ sơ đi du học”.**

Trong cơn hoảng loạn, Tâm gọi về nhà:

> **“Bố mẹ... con muốn đi du học, cần 450 triệu gấp”.**

Người mẹ bất ngờ, im lặng vài giây. Con gái chưa từng đề cập chuyện du học, sao nay lại xin tiền vội vã, giọng còn run run? Bà gặng hỏi, nhưng Tâm chỉ lặp lại: “Bố mẹ cứ gửi tiền cho con, chuyện này rất quan trọng”.

Nhận thấy có điều bất thường, gia đình lập tức đến Công an địa phương trình báo. Lực lượng chức năng đã nhanh chóng vào cuộc, xác định Tâm đang ở một khách sạn trong thành phố và kịp thời giải cứu.

“ Nếu từ chối, em sẽ bị bắt ngay lập tức ”
–
đối tượng đe dọa.

03

CHIẾC KÉT SẮT TẦNG BA

Chiều ngày 15/6/2025, Hải, học sinh lớp 11 ở Cao Bằng, đang ở nhà một mình thì nhận cuộc gọi từ số lạ. Người đàn ông trong điện thoại tự xưng là công an, nói:

> **“Chúng tôi vừa bắt giữ một đối tượng vận chuyển ma túy. Trong tang vật có thông tin cho thấy cháu có liên quan”.**

Hải bối rối:

> **“Cháu... cháu không biết gì cả”.**

Người đàn ông yêu cầu Hải thực hiện cuộc gọi video qua Zalo để thông báo các thông tin, hình ảnh liên quan đến Hải. Gọi video, trên màn hình hiện cảnh một người bị còng tay ngồi cạnh gói ma túy, xung quanh có vài người mặc quân phục Cảnh sát. Chúng tiếp tục gửi giấy tờ giả mạo, trong đó ghi chính xác tên, địa chỉ và thông tin cá nhân của Hải.

> **“Đây là lệnh bắt giữ và phong tỏa tài sản. Cháu phải hợp tác ngay. Vào phòng Zoom để làm việc với cơ quan điều tra. Tuyệt đối không được cho ai biết” - đối tượng ra lệnh.**

Trong phòng Zoom, một nhóm người mặc quân phục liên tục thao túng tâm lý Hải bằng việc đọc điều luật, gắn Hải với nhiều tội danh nguy hiểm liên quan tội phạm ma túy, tội phạm hình sự,...

Sau khi nhận thấy Hải xuất hiện dấu hiệu tâm lý yếu, không kiểm soát được nhận thức bản thân, các đối tượng bắt đầu yêu cầu Hải mở tài khoản ngân hàng để kiểm tra thông tin, “kiểm tra tiền sạch”, chứng minh nhà mình có điều kiện sẽ không có chuyện tham gia vào đường dây buôn bán ma túy. Khi biết tài khoản của Hải không có tiền, chúng chuyển hướng:

“Trong nhà cháu có két sắt đúng không? Hãy mở ra để chứng minh. Nếu không làm, coi như cháu chống đối pháp luật”.

Hải lúng túng:

“Chìa khóa... bố mẹ giữ rồi”.

“Không sao. Cháu đi mua búa và xà beng, phá két ngay. Đây là lệnh điều tra”.

Lo sợ, Hải làm theo. Nhân việc bố mẹ đi vắng, Hải phá khóa két sắt của gia đình, bên trong có nhiều trang sức, vàng. Đối tượng xấu lập tức hối thúc:

“Giờ đem đi bán, lấy tiền chuyển khoản để chứng minh vô tội”.

Khi Hải mang túi vàng đi bán, bố mẹ trở về và thấy két sắt bị phá đã trình báo Công an. May mắn, chưa kịp bán số tài sản trên, Hải đã được Công an tìm thấy. Gặp lại bố mẹ, Hải bật khóc:

“Con chỉ muốn chứng minh mình vô tội...”

Chúng gửi giấy tờ giả mạo, trong đó ghi chính xác tên, địa chỉ và thông tin cá nhân...

04

CHIẾC VALI Ở BIÊN GIỚI

Một buổi sáng tháng 4/2025 tại thư viện trường, Hoa, học sinh lớp 12 tại Tây Ninh, nhận cuộc gọi từ số lạ. Người đàn ông trong điện thoại tự xưng là cán bộ Cục Cảnh sát Kinh tế, nói nghiêm giọng:

> **"Em đang liên quan đến một vụ rửa tiền lớn. Nhiều tài khoản ngân hàng mang tên em đã thực hiện giao dịch bất hợp pháp".**

Hoa ngỡ ngàng:

> **"Em chưa từng mở tài khoản nào..."**

Ngay sau đó, đối tượng gửi hình ảnh giả mạo: thẻ ngân hàng, giấy tờ mang tên Hoa. Thấy thông tin trùng khớp, Hoa hoang mang và bắt đầu tin rằng mình bị điều tra.

> **"Đây là án mật. Em phải hợp tác ngay. Vào phòng Zoom làm việc với cơ quan điều tra. Tuyệt đối không được nói với gia đình" – đối tượng ra lệnh.**

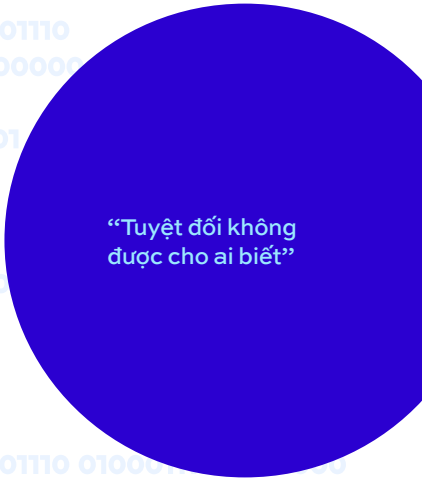
Hoa truy cập vào phòng Zoom từ đường link đối tượng gửi qua tin nhắn điện thoại.

Trong phòng Zoom, những đối tượng xấu dàn cảnh với nhiều người mặc quân phục Công an, ngồi trước bàn làm việc, bắt đầu thao túng, đẩy em vào thế hoảng loạn và bất an về tâm lý.

Khi thấy em có dấu hiệu hoảng sợ, các đối tượng bắt đầu ngon ngọt trấn an bằng việc họ sẽ đồng hành với em để tháo gỡ vấn đề và không ai có thể giúp em ngoài họ.

Những đối tượng xấu dùng lời lẽ ân cần và thấu hiểu rằng họ hiểu em không tham gia đường dây rửa tiền và ma túy và muốn em chứng minh điều đó để trả lại sự trong sạch.

Liên tục hối thúc trong phòng Zoom, các đối tượng hướng dẫn Hoa thực hiện nhiều hành động để "phối hợp điều tra", "chứng minh vô tội"; yêu cầu Hoa chuẩn bị di chuyển vào TP. HCM để "xác minh trực tiếp". Liên tục nhắc lại "Tuyệt đối không được cho ai biết" vì cuộc điều tra đang bí mật, đối tượng xấu nhấn mạnh nếu người khác biết sẽ ảnh hưởng đến vụ án và không chứng minh được sự trong sạch của bản thân. Hoa đã đồng ý và làm theo.



Ngay chiều hôm đó, Hoa về nhà thu xếp quần áo, bắt xe lên TP. Hồ Chí Minh. Khi đến tới bến xe Miền Đông, một người đàn ông gọi điện, tự nhận được "cán bộ" cử đến đón. Hoa lên xe, tin rằng sẽ được đưa tới cơ quan công an. Tuy nhiên, xe lại chạy ngược về hướng Tây Ninh. Để trấn an Hoa, trong quá trình di chuyển, các đối tượng tiếp tục gọi Zoom, nói:

> **"Đây là thủ tục điều tra. Em sẽ được đưa đến cửa khẩu Mộc Bài, sau đó sang Campuchia tạm lánh."**

Ngồi trong xe, Hoa ôm chặt vali, lo lắng nhưng vẫn không hề nghi ngờ. May mắn, gia đình phát hiện con gái mất liên lạc bất thường nên lập tức báo công an. Lực lượng chức năng nhanh chóng truy vết, xác định Hoa đang ở một nhà trọ gần biên giới. Cháu được giải cứu kịp thời trước khi bị đưa ra khỏi biên giới.

05

HỌC BỔNG TRONG MƠ

Tháng 8/2025, Mai Trang, sinh viên năm hai tại một trường đại học ở Hà Nội, nhận cuộc gọi từ người tự xưng là cán bộ phụ trách đào tạo hệ quốc tế tại một trung tâm giáo dục có tiếng trong nước. Người này thông báo:

> **“Trung tâm đang có suất học bổng du học nước ngoài với chi phí thấp. Chúc mừng em đủ tiêu chí được nhận học bổng. Đây là cơ hội đặc biệt, em có muốn đăng ký không? Trung tâm sẽ tạo điều kiện, hỗ trợ em làm thủ tục cần thiết”.**

Trang vốn có ước mơ đi du học nên lập tức chú ý. Đối tượng nhanh chóng gửi một đường link, yêu cầu đăng nhập, điền đầy đủ thông tin cá nhân và chuyển một khoản tiền “giữ chỗ” để được ưu tiên xét duyệt. Kèm theo đó là lời dặn:

> “Đây là cơ hội hiếm có. Em phải giữ bí mật, đừng nói với ai. Nếu có nhiều người biết sẽ đăng ký thì cơ hội của em sẽ ít đi”.

Dưới áp lực thúc giục, do không đủ tiền nộp “giữ chỗ”, Trang nhắn cho mẹ:

> “Mẹ ơi, con có suất đi du học, cần tiền gấp để đăng ký”.

Sau đó, theo hướng dẫn của "cán bộ trung tâm đào tạo", Trang tự thuê phòng khách sạn để "có không gian riêng", thuận lợi cho quá trình xác minh danh tính, làm thủ tục đăng ký. Nhận thấy Trang có dấu hiệu tin tưởng, cung cấp thông tin cá nhân, hoàn thiện thủ tục đăng ký, đối tượng liên tục gọi điện thoại, nhắn tin hối thúc:

> "Nếu không chuyển tiền ngay, em sẽ mất suất học bổng này".

Trong lúc Trang chuẩn bị yêu cầu mẹ chuyển tiền, gia đình nhận thấy bất thường. Trước đó, con gái chưa từng nhắc đến chuyện du học, nay lại xin tiền vội vã với lý do khẩn cấp. Linh cảm có điều không ổn, gia đình lập tức báo Công an.

Chiều cùng ngày, lực lượng chức năng phối hợp xác định vị trí của Trang tại khách sạn. Cô được giải cứu an toàn trước khi kịp chuyển tiền cho đối tượng.

"Đây là cơ hội hiếm có"

(PHẦN 03)

NHỮNG BẢN CHẤT LỘ DIỆN

01 ĐIỂM MẤU CHỐT

Mấu chốt của bắt cóc trực tuyến là khiến nạn nhân tự cô lập, mất kết nối với gia đình, bạn bè. Ngược lại, kết nối là chìa khóa để thoát ra. Trong những câu chuyện thực tế về lừa đảo trực tuyến, những kẻ lừa đảo chỉ thành công khi "ngắt kết nối" mục tiêu và những người xung quanh.

Mỗi giây im lặng của nạn nhân là một viên gạch xây nên bức tường cô lập.

nơi họ phải một mình đối mặt với toàn bộ sự tinh vi và sức mạnh của sự "chuyên nghiệp" đã tôi luyện qua hàng trăm, hàng nghìn vụ việc trước đó. Khi nạn nhân chọn im lặng, họ vô tình ngắt mình khỏi sức mạnh của cộng đồng, tự cắt đứt sợi dây tỉnh táo cuối cùng.

↳ **Từ khoảnh khắc ấy, khi đồng tình hoặc làm theo lời kẻ xấu, họ đã tự biến mình thành con mồi trong lưới lừa đảo trực tuyến.**

Điểm cốt lõi của mọi vụ lừa đảo trực tuyến chính là “kết nối”.

Từ những giây đầu tiên cho đến toàn bộ quá trình lừa đảo sau đó, những kẻ lừa đảo tung ra mọi thủ đoạn tinh vi nhất, lành nghề nhất chỉ để đạt mục đích bao vây, cô lập, “ngắt kết nối” mục tiêu với những người xung quanh.

Chúng đe dọa làm mục tiêu sợ hãi, chúng thao túng tâm lý kiểm soát cảm xúc và hành vi của mục tiêu hoặc dụ dỗ bằng những món hời vật chất, tinh thần. Tất cả chỉ để mục tiêu làm theo sự dẫn dắt mà không dám, không muốn hoặc không thể chia sẻ vấn đề của mình với những người xung quanh

CHỈ KHI “CÔ LẬP” ĐƯỢC MỤC TIÊU, BUỘC MỤC TIÊU PHẢI MỘT MÌNH ĐỐI MẶT VỚI TOÀN BỘ SỨC MẠNH CỦA TỔ CHỨC TỘI PHẠM THÌ NHỮNG KẺ LỪA ĐẢO MỚI CÓ CƠ HỘI CHIẾN THẮNG TRONG TRÒ CHƠI DO CHÚNG SẮP ĐẶT.

Và trong mọi vụ việc được ngăn chặn trên thực tế, người bị những kẻ lừa đảo nhắm mục tiêu hoặc đã tỉnh táo nhận ra hoặc đã chia sẻ câu chuyện của mình với người thân, bạn bè, cộng đồng để không "tự cô lập" mình dưới áp lực đe dọa, dụ dỗ, thao túng của những kẻ lừa đảo.

Hoặc người thân, bạn bè, cộng đồng kịp nhận ra những dấu hiệu nguy hiểm của vụ lừa đảo và sử dụng sức mạnh kết nối để "kéo" nạn nhân trở lại, như những vụ "giải cứu" thành công khi nạn nhân đang trong hành trình tự đưa mình qua bên kia biên giới theo chỉ dẫn của những kẻ buôn người

Đây là khi cộng đồng đã chọn "giữ kết nối" để bảo vệ các thành viên của mình.

Thực tế cho thấy rằng, không phải lúc nào chúng ta cũng đủ kiến thức, kỹ năng để nhận ra chiêu trò lừa đảo luôn biến hóa của tội phạm.

Nhưng thực tế cũng đã chứng minh, sự kết nối, sự chia sẻ vấn đề gặp phải với những người xung quanh hoặc sự quan tâm chia sẻ, hỗ trợ, giúp đỡ của những người xung quanh luôn giúp chúng ta thoát khỏi "lưới lừa đảo trực tuyến" bủa vây.

Chính sức mạnh của sự gắn kết – với gia đình, bạn bè, hay những người xung quanh – là vũ khí mạnh nhất để chống lại mọi chiêu trò dụ dỗ, thao túng, lừa đảo, "bắt cóc" trực tuyến.

02 NHỮNG THỦ ĐOẠN

• ĐE DOẠ (THREATS)

Sử dụng nỗi sợ hãi để ép buộc tuân thủ

Đây là thủ đoạn phổ biến và dễ thực hiện nhất trong các vụ lừa đảo trực tuyến. Đe dọa thường được sử dụng độc lập ngay từ đầu hoặc xuất hiện như bước cuối trong chuỗi thao túng và dụ dỗ, nhằm ép buộc nạn nhân tuân theo ý muốn của tội phạm. Các hình thức đe dọa phổ biến bao gồm:

ĐE DỌA XỬ LÝ PHÁP LÝ

ĐE DỌA TUNG HÌNH ẢNH NHẠY CẢM

ĐE DỌA BẠO LỰC

Đe dọa xử lý pháp lý

Tội phạm giả danh Công an, Viện kiểm sát, Tòa án hoặc các cơ quan chức năng, liên lạc với nạn nhân qua điện thoại, tin nhắn hoặc email, thông báo rằng nạn nhân bị liên quan đến các vụ án nghiêm trọng như ma túy, rửa tiền, lừa đảo hoặc tội phạm xuyên quốc gia.

Chúng gửi các giấy tờ giả mạo (lệnh bắt, lệnh khám xét) chứa thông tin cá nhân của nạn nhân, kèm theo hình ảnh hoặc video giả tạo (như cảnh bắt giữ tội phạm với tang vật) để tăng tính thuyết phục.

Nạn nhân bị đe dọa sẽ bị bắt giữ, phạt tù hoặc bị tịch thu tài sản nếu không làm theo hướng dẫn, như chuyển tiền hoặc cung cấp thông tin cá nhân.

> Trong câu chuyện "Chiếc vali ở biên giới" kẻ xấu giả danh là cán bộ Cục Cảnh sát Kinh tế, đe dọa Hoa có liên quan đến vụ án rửa tiền lớn.
>
> Bằng thủ đoạn này, chúng đẩy em vào trạng thái sợ hãi và tuân theo các yêu cầu của chúng.

Đe dọa tung hình ảnh nhạy cảm

Sau khi lừa nạn nhân gửi ảnh hoặc video nhạy cảm (thường qua các ứng dụng chat hoặc mạng xã hội)

Tội phạm gửi lại nội dung này cho nạn nhân và đe dọa phát tán lên mạng xã hội, gửi đến gia đình, bạn bè hoặc trường học nếu nạn nhân không tiếp tục cung cấp thêm hình ảnh, video hoặc tiền bạc.

↳ Nỗi sợ bị bêu xấu khiến nạn nhân rơi vào trạng thái hoảng loạn và tuân thủ

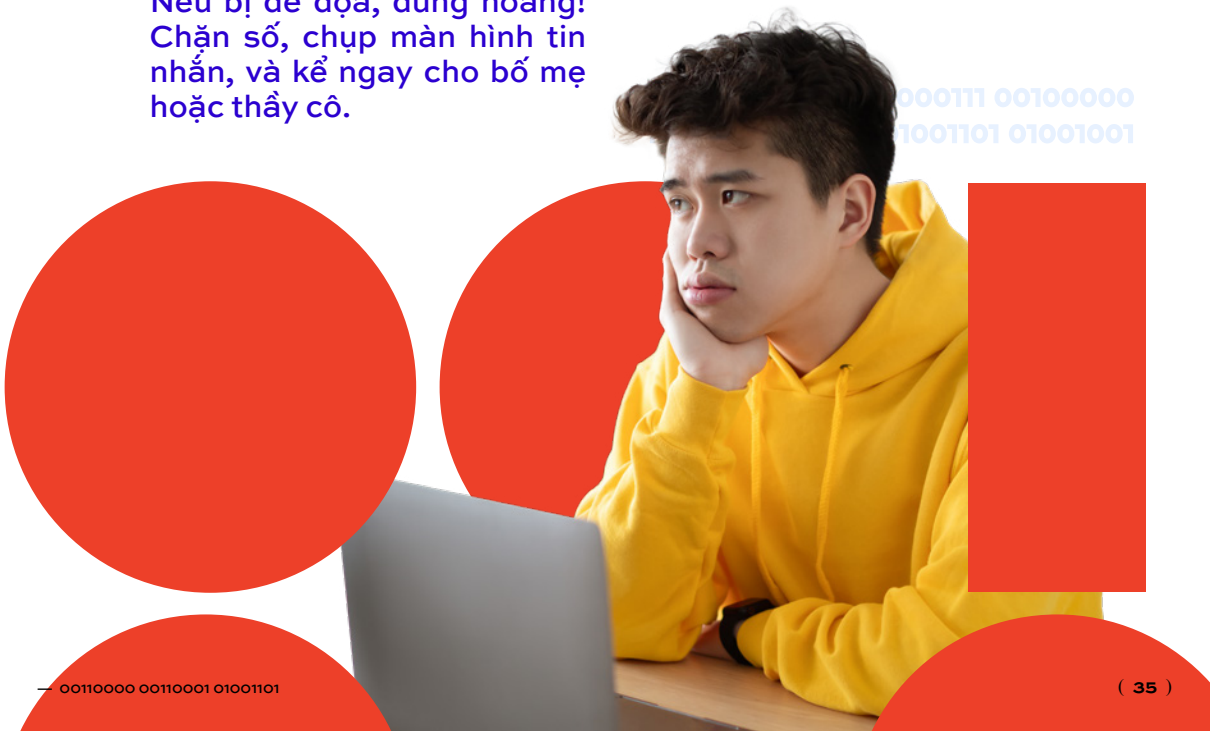
Đe dọa bạo lực

Tội phạm sử dụng thông tin cá nhân (địa chỉ nhà, trường học, nơi làm việc) thu thập từ mạng xã hội hoặc các cuộc trò chuyện trước đó để đe dọa sẽ đến tận nơi đánh đập, bắt cóc hoặc gây tổn hại cho nạn nhân và người thân.

Lời đe dọa thường đi kèm chi tiết cụ thể để tạo cảm giác nạn nhân bị theo dõi, khiến họ sợ hãi và làm theo yêu cầu.

Làm gì?

Nếu bị đe dọa, đừng hoảng! Chặn số, chụp màn hình tin nhắn, và kể ngay cho bố mẹ hoặc thầy cô.



- THAO TÚNG (MANIPULATION)

Kiểm soát cảm xúc và hành vi lâu dài

Thao túng là thủ đoạn tinh vi, tập trung vào việc kiểm soát tâm lý nạn nhân để khiến họ phụ thuộc và mất khả năng tự quyết. Tội phạm sử dụng các chiến thuật tâm lý phức tạp để duy trì sự kiểm soát lâu dài, bao gồm:

GÂY NGHI NGỜ VÀ LÚNG TÚNG

TẠO SỰ PHỤ THUỘC

ĐƯA RA GIẢI PHÁP GIẢ TẠO

SỬ DỤNG "TRAUMA BONDING"

Gây nghi ngờ và lúng túng

Tội phạm khiến nạn nhân nghi ngờ chính suy nghĩ và nhận thức của mình bằng cách cung cấp thông tin mập mờ, sai lệch hoặc mâu thuẫn.

Ví dụ:

Chúng có thể nói rằng tài khoản ngân hàng của nạn nhân bị liên quan đến hoạt động phạm pháp và yêu cầu nạn nhân cung cấp thông tin để "kiểm tra", khiến nạn nhân hoang mang và không biết phải làm gì.

↳ Khiến nạn nhân hoang mang và không biết phải làm gì

Tạo sự phụ thuộc

Tội phạm hướng dẫn nạn nhân rằng để giải quyết vấn đề, họ phải làm theo chỉ dẫn cụ thể, như chuyển tiền vào tài khoản **"bảo lãnh"**, đến một địa điểm cụ thể để **"làm việc riêng"**, hoặc tham gia các cuộc gọi Zoom giả mạo với sự xuất hiện của đồng bọn đóng vai công an, kiểm sát viên, hoặc thẩm phán.

Những chỉ dẫn này khiến nạn nhân tin rằng họ không thể tự giải quyết vấn đề mà phải dựa vào kẻ lừa đảo.

> Trong câu chuyện "Chiếc két sắt tầng 3" kẻ xấu gọi video call, hướng dẫn Hải tham gia phòng Zoom trực tuyến và liên tục đưa ra lời đe dọa "Nếu muốn thoát tội phải hợp tác ngay".
>
> Áp lực dồn dập này khiến Hải hình thành tâm lý phụ thuộc và kẻ xấu, từ đó tìm mọi cách để chứng minh mình không liên quan đến hoạt động vận chuyển ma túy.

Đưa ra giải pháp giả tạo

Tội phạm gợi ý những giải pháp nghe có vẻ hợp lý nhưng thực chất là cái bẫy, như yêu cầu nạn nhân chuyển tiền để "bảo toàn tài sản", quay video nhạy cảm để "chứng minh vô tội", hoặc giữ bí mật tuyệt đối để "bảo vệ an toàn".

↳ Những giải pháp này khiến nạn nhân tự đẩy mình vào thế bị kiểm soát

Sử dụng (GẮN KẾT ĐAU THƯƠNG) “trauma bonding”

Tội phạm xen kẽ giữa hành vi ép buộc và cử chỉ thân thiện, như khen ngợi, tỏ ra thấu hiểu hoặc hứa hẹn hỗ trợ, để tạo mối liên kết cảm xúc độc hại.

Làm gì?

Nếu cảm thấy bối rối hoặc bị ép buộc, dừng lại, hỏi ý kiến bố mẹ hoặc thầy cô. Đừng tin lời khen từ người lạ!

(VÍ DỤ) Sau khi ép nạn nhân gửi ảnh nhạy cảm. Chúng có thể trò chuyện vui vẻ, khiến nạn nhân cảm thấy vừa sợ hãi vừa phụ thuộc vào kẻ lừa đảo

• DỤ DỖ (LURING/GROOMING)

Xây dựng lòng tin để tiếp cận

Dụ dỗ là quá trình tội phạm xây dựng lòng tin với nạn nhân, đặc biệt là trẻ em và thanh thiếu niên, để dẫn dắt họ vào các hành vi nguy hiểm. Nạn nhân, đặc biệt là thanh thiếu niên có thể đã được học "đề phòng" người lạ nhưng lại không biết cách để xử lý một "người lạ thân thiện" kiên trì theo đuổi dụ dỗ. Thủ đoạn này thường kéo dài và dựa trên những tác động tâm lý tinh tế, bao gồm:

DỤ DỖ BẰNG VẬT CHẤT

DỤ DỖ BẰNG LỢI ÍCH TINH THẦN

THÚC ĐẨY HÀNH VI NGUY HIỂM

Hứa hẹn tặng quà

(DỤ DỖ BẰNG VẬT CHẤT)

Tội phạm hứa hẹn tặng quà, tiền, tài khoản game cao cấp, hoặc cơ hội việc làm **“nhẹ nhàng”, “lương cao”** để thu hút nạn nhân.

Ví dụ:

Chúng có thể mời nạn nhân tham gia các dự án đầu tư giả mạo, hứa hẹn lợi nhuận cao, hoặc tặng vật phẩm ảo trong game để đổi lấy thông tin cá nhân hoặc hình ảnh nhạy cảm.

“Trong câu chuyện “Học bổng trong mơ”, kẻ xấu đã khéo léo dẫn dụ Trang tin tưởng, tự nguyện làm theo các hướng dẫn với mong muốn dành được suất “học bổng trong mơ”.

Dẫn đến việc Trang nôn nóng, bỏ nhà đến khách sạn một mình, thúc giục gia đình chuyển tiền cho kẻ xấu.”

Giả làm bạn thân, người yêu

(DỤ DỖ BẰNG LỢI ÍCH TINH THẦN)

Tội phạm đóng vai người bạn thân thiết, người yêu lý tưởng hoặc người cố vấn, luôn lắng nghe, thấu hiểu và khen ngợi nạn nhân. Chúng tạo cảm giác gần gũi bằng cách **chia sẻ sở thích, câu chuyện cá nhân giả tạo, hoặc tỏ ra đồng cảm với khó khăn của nạn nhân.**

Mối quan hệ này thường được thúc đẩy trong bí mật, với yêu cầu nạn nhân không chia sẻ với người thân hoặc bạn bè để "giữ riêng tư", từ đó ngắt kết nối nạn nhân với cộng đồng.

Thúc đẩy hành vi nguy hiểm

Sau khi xây dựng lòng tin, tội phạm dần yêu cầu nạn nhân thực hiện các hành vi rủi ro, như gửi ảnh nhạy cảm, tham gia video call riêng tư, hoặc gặp mặt ngoài đời thực.

Chúng sử dụng các lời hứa hẹn hoặc áp lực nhẹ nhàng như "nếu em yêu anh thì làm đi" để khiến nạn nhân cảm thấy phải tuân theo.

Làm gì?

Không nhận quà từ người lạ, không gặp riêng, và kể ngay cho bố mẹ nếu có ai tỏ ra quá thân thiện trên mạng.

Chúng sử dụng các lời hứa hẹn hoặc áp lực nhẹ nhàng như "nếu em yêu anh thì làm đi". Để khiến nạn nhân cảm thấy phải tuân theo

03 NHỮNG DẤU HIỆU TỪ BÊN TRONG

Chiêu trò của những kẻ phạm tội thường thay đổi hoặc được biến hóa sử dụng kết hợp nhiều thủ đoạn, thủ đoạn cũ nhưng thêm những yếu tố mới.

Đó là lí do vì sao thực tế vẫn có thêm nhiều nạn nhân mới của lừa đảo trực tuyến. Thực tế này gợi ý rằng, để nhận ra lừa đảo trực tuyến, tập trung phát hiện dấu hiệu hành vi của những kẻ lừa đảo là không đủ.

Hàng nghìn vụ lừa đảo đã chỉ ra, dù dấu hiệu bề ngoài khác nhau, nhưng những dấu hiệu "bên trong" không thay đổi.

Tập trung vào những dấu hiệu "bên trong" là mảnh ghép quan trọng còn thiếu. Dưới đây là ba dấu hiệu "bên trong" giúp nhận ra chúng ta hoặc người thân của chúng ta có đang trong tiến trình trở thành nạn nhân của lừa đảo trực tuyến hay không.

3 DẤU HIỆU

- SỢ HÃI
- TIN MÙ QUÁNG
- ĐỒNG TÌNH

SỢ HÃI

Sợ hãi là dấu hiệu đầu tiên và rõ ràng nhất cho thấy một người có thể đang trở thành nạn nhân của lừa đảo trực tuyến. Tội phạm sử dụng đe dọa như một công cụ chính để kiểm soát, khiến nạn nhân rơi vào trạng thái hoảng loạn, mất khả năng suy nghĩ tỉnh táo.

Sự sợ hãi này không chỉ đến từ lời nói mà còn từ cách tội phạm cá nhân hóa các mối đe dọa, khiến nạn nhân cảm thấy bị tấn công trực tiếp và không còn lối thoát.

CÁC DẤU HIỆU CỤ THỂ BAO GỒM:

SỢ BỊ XÂM PHẠM AN TOÀN CÁ NHÂN

Tội phạm thường sử dụng thông tin cá nhân (địa chỉ nhà, trường học, nơi làm việc) để đe dọa bạo lực, khiến nạn nhân cảm thấy bị theo dõi hoặc đe dọa trực tiếp đến tính mạng, sức khỏe của bản thân hoặc người thân. Ví dụ, một thiếu niên có thể sợ hãi khi nhận được tin nhắn đe dọa rằng tội phạm sẽ đến trường để "xử lý" nếu không làm theo.

SỢ MẤT TÀI SẢN HOẶC CƠ HỘI

Nạn nhân có thể sợ không lấy lại được số tiền đã đầu tư, mất cơ hội việc làm, hoặc bị cắt đứt mối quan hệ "tình cảm" với tội phạm. Điều này khiến họ tiếp tục làm theo yêu cầu, như chuyển thêm tiền hoặc cung cấp thêm thông tin, với hy vọng "giải quyết vấn đề".

PHẢN ỨNG HOẢNG LOẠN TRƯỚC THÔNG TIN TỪ NGƯỜI LẠ

Khi nhận được cuộc gọi, tin nhắn hoặc thông báo từ một nguồn không rõ ràng, như thông báo liên quan đến vi phạm pháp luật hoặc đe dọa tung hình ảnh nhạy cảm, nạn nhân thường cảm thấy sợ hãi, lo lắng tột độ. Họ có thể nói lắp, run rẩy, hoặc trả lời một cách lúng túng khi đối mặt với những lời buộc tội hoặc đe dọa vô căn cứ. Ví dụ, một học sinh có thể hoảng sợ khi nhận được tin nhắn từ "công an" yêu cầu cung cấp thông tin để "tránh bị bắt".

SỢ BỊ BÊU XẤU HOẶC MẤT DANH DỰ

Nạn nhân, đặc biệt là thanh thiếu niên, sợ rằng hình ảnh nhạy cảm hoặc thông tin cá nhân sẽ bị phát tán đến gia đình, bạn bè hoặc trường học. Nỗi sợ này khiến họ dễ dàng tuân thủ yêu cầu của tội phạm, như gửi thêm hình ảnh hoặc chuyển tiền để "ngăn chặn" việc phát tán.

BIỂU HIỆN THỂ CHẤT VÀ TÂM LÝ

Nạn nhân có thể biểu hiện sự sợ hãi qua các dấu hiệu như mất ngủ, căng thẳng, né tránh giao tiếp với người thân, hoặc trở nên nhút nhát bất thường khi sử dụng điện thoại hoặc máy tính. Những thay đổi này thường là dấu hiệu cho thấy họ đang chịu áp lực từ một mối đe dọa trực tuyến.

TIN MÙ QUÁNG

Tin mù quáng là dấu hiệu rõ ràng nhất cho thấy một người đang bị thao túng, đặc biệt khi niềm tin đó không dựa trên cơ sở thông tin rõ ràng, có thể kiểm chứng.

Tội phạm khai thác điểm yếu tâm lý để khiến nạn nhân tin tưởng một cách mù quáng, bỏ qua lý trí và cảnh báo từ những người xung quanh.

CÁC DẤU HIỆU CỤ THỂ BAO GỒM:

LÀM THEO CHỈ DẪN KHÔNG DO DỰ

Nạn nhân tuân thủ mọi yêu cầu của tội phạm mà không đặt câu hỏi, như chuyển tiền, gửi hình ảnh nhạy cảm, hoặc thực hiện các hành động bất thường theo hướng dẫn qua tin nhắn, cuộc gọi hoặc video call. Ví dụ, nạn nhân có thể lập tức chuyển tiền vào tài khoản lạ chỉ vì một cuộc gọi từ "công an" mà không kiểm tra tính xác thực.

BỎ QUA LỜI KHUYÊN TỪ NGƯỜI THÂN

Nạn nhân phản ứng phòng thủ khi được cha mẹ, bạn bè hoặc người thân can ngăn, thường nói những câu như "Đừng xen vào chuyện của con", "Đây là việc riêng của con" hoặc "Họ sẽ giúp con giải quyết vấn đề". Điều này cho thấy nạn nhân đã bị thao túng đến mức xem tội phạm là nguồn tin cậy duy nhất.

BẤT THƯỜNG TRONG HÀNH VI

Nạn nhân có những thay đổi đột ngột trong thói quen, như thường xuyên ra ngoài không rõ lý do, khóa cửa phòng khi sử dụng điện thoại, hoặc trở nên kín đáo hơn về các hoạt động trực tuyến. Những dấu hiệu này thường đi kèm với sự lo lắng hoặc căng thẳng khi bị hỏi về các hoạt động của mình.

CHE GIẤU HÀNH VI

Nạn nhân bí mật thực hiện các yêu cầu của tội phạm, như xóa lịch sử chat, khóa thiết bị, thay đổi mật khẩu hoặc nói dối về lịch trình ra ngoài. Ví dụ, một học sinh có thể giấu cha mẹ về việc liên lạc với "người bạn online" hoặc tham gia các cuộc gặp bí mật.

ĐỒNG TÌNH

Đồng tình là dấu hiệu cho thấy nạn nhân đã bị dụ dỗ hoặc thao túng đến mức chấp nhận hoặc biện minh cho hành vi sai trái của tội phạm, ngay cả khi họ nhận thức được sự bất thường.

Đây là giai đoạn nguy hiểm, khi nạn nhân bắt đầu tự thuyết phục mình rằng hành động của họ là đúng đắn hoặc không còn lựa chọn nào khác.

CÁC DẤU HIỆU CỤ THỂ BAO GỒM:

CHẤP NHẬN QUÀ TẶNG KHÔNG RÕ NGUỒN GỐC

ạn nhân nhận tiền, quà tặng hoặc vật phẩm ảo có giá trị từ người lạ mà không thắc mắc lý do. Ví dụ, một học sinh có thể nhận tài khoản game cao cấp từ một "người bạn online" và xem đó là bình thường, dù không biết rõ danh tính đối phương.

BẢO VỆ HOẶC BIỆN MINH CHO TỘI PHẠM

Khi được hỏi về mối quan hệ với người lạ, nạn nhân có xu hướng bảo vệ hoặc đưa ra lý do để biện minh, như "Anh ấy rất tốt với con", "Họ chỉ muốn giúp con" hoặc "Họ hiểu con hơn mọi người". Điều này cho thấy nạn nhân đã bị cuốn vào mối quan hệ độc hại.

IM LẶNG TRƯỚC HÀNH VI SAI TRÁI

Nạn nhân biết rằng hành vi của tội phạm (như yêu cầu gửi ảnh nhạy cảm, ép buộc gặp mặt hoặc chuyển tiền) là sai trái nhưng chọn im lặng, không chia sẻ với người thân hoặc cơ quan chức năng. Họ có thể tự thuyết phục rằng việc tuân theo sẽ giúp giải quyết vấn đề hoặc tránh rắc rối lớn hơn.

TỰ TRÁCH MÌNH

Nạn nhân cảm thấy xấu hổ hoặc tự trách mình vì đã rơi vào bẫy, dẫn đến việc tiếp tục làm theo yêu cầu của tội phạm để "sửa chữa sai lầm" hoặc "giữ bí mật". Ví dụ, một thanh thiếu niên có thể tiếp tục gửi ảnh nhạy cảm vì sợ rằng việc dừng lại sẽ khiến ảnh bị phát tán.

(PHẦN 04)

04 NHỮNG LỜI KHUYÊN ĐỒNG HÀNH

THỰC TẾ CHỨNG MINH RẰNG, KHÔNG MỘT AI CÓ THỂ HOÀN TOÀN TRÁNH KHỎI NHỮNG CHIÊU TRÒ BIẾN HÓA CỦA TỘI PHẠM TRỰC TUYẾN.

Nhưng sự kết nối và hành động kịp thời chính là chìa khóa để phá vỡ vòng vây cô lập mà chúng giăng ra!

NHỮNG LỜI KHUYÊN DƯỚI ĐÂY KHÔNG CHỈ LÀ LÝ THUYẾT, MÀ LÀ NHỮNG BƯỚC ĐI CỤ THỂ, DỄ ÁP DỤNG, ĐƯỢC RÚT RA TỪ HÀNG NGÀN VỤ VIỆC ĐÃ ĐƯỢC NGĂN CHẶN THÀNH CÔNG.

Dù bạn là thanh thiếu niên – những mục tiêu chính của "bắt cóc online" – hay là gia đình, nhà trường, cơ quan chức năng, cộng đồng và các nền tảng, hãy nhớ rằng:

Mỗi hành động nhỏ để duy trì kết nối đều là một viên gạch xây dựng bức tường bảo vệ vững chắc.

Chúng ta không chiến đấu một mình; chúng ta chiến đấu cùng nhau, với sự tỉnh táo và lòng tin vào cộng đồng.

01 NẾU BẠN LÀ THANH THIẾU NIÊN

Chúng ta là những người trẻ đầy năng lượng, dễ bị cuốn hút bởi thế giới trực tuyến rộng lớn, nhưng cũng chính là nhóm dễ bị nhắm đến nhất bởi các thủ đoạn dụ dỗ, thao túng và đe dọa.

↳ **Nhưng chúng ta không cần phải sợ hãi công nghệ, mà cần học cách sử dụng nó một cách thông minh, và có trách nhiệm, luôn giữ vững sự kết nối với thế giới thực để không rơi vào bẫy cô lập.**

Dưới đây là những nguyên tắc cơ bản để các em tự bảo vệ mình.

TRUY CẬP AN TOÀN

Hãy coi truy cập internet như việc bước vào một khu phố đông đúc:

Luôn chọn con đường sáng sủa, đông người!

Không chấp nhận lời mời kết bạn từ người lạ, và luôn kiểm tra URL trước khi nhập thông tin cá nhân.

Đừng tò mò tham gia các phòng chat, group, hoặc Zoom do người lạ mời, vì đây thường là cánh cửa dẫn đến bẫy dụ dỗ. Nhớ rằng, các nền tảng mạng xã hội hay game online chỉ an toàn khi các em đặt chế độ riêng tư cao nhất.

Không bao giờ truy cập các đường link lạ, tải ứng dụng từ nguồn không rõ ràng, hoặc click vào liên kết từ tin nhắn lạ – dù chúng hứa hẹn “quà tặng miễn phí” hay “tài khoản game cao cấp”.

Mẹo cài đặt bảo mật:

- Thiết lập mật khẩu gồm cả ký tự số, chữ thường, chữ hoa và các ký tự đặc biệt.
- Đặt câu hỏi bảo mật.
- Sử dụng các mật khẩu khác nhau.
- Bật chế độ cảnh báo khi có thiết bị lạ đăng nhập.

Mỗi lần truy cập là một lần nhắc nhở

Mình đang ở nơi công cộng, không chia sẻ bí mật riêng tư.

GIAO TIẾP AN TOÀN

Giao tiếp trực tuyến giống như trò chuyện với bạn bè ở quán cà phê:

Vui vẻ nhưng luôn giữ khoảng cách.

Chặn ngay tài khoản đáng ngờ và báo cáo lên nền tảng để ngăn chặn sớm.

Không kết bạn hoặc trả lời tin nhắn từ người lạ hoặc những người không quen biết ngoài đời thực. Nếu có lời mời kết bạn, hãy chắc chắn rằng đó là người quen biết, như bạn học hoặc người thân, trước khi đồng ý.

Không chia sẻ vị trí thực tế, địa chỉ nhà, trường học hay lịch trình hàng ngày với bất kỳ ai chưa từng gặp mặt. Nếu ai đó bắt đầu bằng lời khen ngợi quá mức, hứa hẹn tình yêu hay cơ hội "kiếm tiền dễ dàng", hãy dừng lại và kiểm tra: Họ có thực sự là bạn bè không?

Không gặp mặt một mình người quen online; nếu có hẹn, chỉ gặp ở nơi công cộng, có người lớn đi cùng, và thông báo trước cho cha mẹ và người thân.

Hãy giữ quy tắc "3 giây suy nghĩ" : Trước khi trả lời bất kỳ yêu cầu nào – dù là gửi ảnh hay chuyển tiền – hãy đếm đến 3 và tự hỏi:

Điều này có bình thường không?

LƯU Ý

TIÊU CHUẨN KẾT BẠN AN TOÀN TRÊN MẠNG

Khi nhận được lời mời kết bạn trên mạng xã hội, hãy kiểm tra kỹ để tránh rủi ro từ người lạ:

- ĐÃ GẶP NGOÀI ĐỜI CHƯA? → Chỉ kết bạn với những người em thực sự quen biết, như bạn học, thầy cô, hoặc người thân.
- HÌNH ẢNH CÓ THẬT KHÔNG? → Dùng công cụ như Google Reverse Image Search để kiểm tra ảnh đại diện có bị lấy cắp từ internet hay không.
- CÓ BẠN CHUNG ĐÁNG TIN KHÔNG? → Xem danh sách bạn chung – nếu chỉ toàn người lạ hoặc không có bạn chung, hãy cẩn thận.
- ĐỊA ĐIỂM, THÔNG TIN CÓ KHỚP KHÔNG? → Kiểm tra nơi ở, trường học, hoặc thông tin trên trang cá nhân có hợp lý và khớp với người quen biết không.
- HOẠT ĐỘNG TRÊN TRANG CÓ ĐÁNG NGỜ KHÔNG? → Xem bài đăng, bình luận, hoặc tương tác của họ – nếu trống rỗng hoặc chỉ toàn nội dung quảng cáo, đó có thể là tài khoản giả.

(HÃY NHỚ)

Mỗi người nên tự xây dựng tiêu chuẩn kết bạn riêng, nhưng dù ai đó đáp ứng đủ tiêu chí, vẫn phải cẩn trọng. Kết bạn không có nghĩa là họ chắc chắn đáng tin. Nếu nghi ngờ, hãy hỏi ý kiến bố mẹ hoặc bạn bè thân trước khi chấp nhận lời mời. An toàn là ưu tiên số một!

CHIA SẺ AN TOÀN

Chia sẻ trên mạng giống như kể chuyện cho cả lớp nghe:

Chỉ kể những gì em muốn mọi người biết.

Không bao giờ quay video hoặc chụp ảnh theo đề nghị của người lạ, đặc biệt là ảnh nhạy cảm

Không bật camera điện thoại hoặc máy tính trong những thời điểm riêng tư (như khi thay đồ hoặc ở phòng riêng).

Không công khai hình ảnh hoặc thông tin cá nhân như số điện thoại, CCCD, địa chỉ nhà, hoặc kể lể về khó khăn cá nhân trên mạng xã hội, vì đây là "mồi" cho tội phạm lợi dụng.

Nếu ai đó yêu cầu giữ bí mật về mối quan hệ trực tuyến, đó chính là dấu hiệu đỏ: Hãy chọn chia sẻ ngay với cha mẹ, người thân, hoặc bạn bè quen biết để không bị cô lập.

Mỗi lần chia sẻ là cơ hội để các em khẳng định:

Mình kiểm soát câu chuyện của chính mình, không để ai khác dẫn dắt.

XÂY DỰNG HÌNH ẢNH CÁ NHÂN TRÊN INTERNET

SỐNG ẢO NHƯNG SỐNG THẬT

Mạng xã hội có thể khiến chúng ta cảm thấy áp lực phải xây dựng hình ảnh hoàn hảo – luôn xinh đẹp, thành công, hoặc nổi tiếng.

Nhưng hãy nhớ, sống thật với chính mình mới là cách bảo vệ bản thân khỏi những rủi ro. Đừng chạy theo lượt like, bình luận, hay cố gắng gây ấn tượng bằng cách khoe khoang vật chất, vì điều này dễ khiến em trở thành mục tiêu của các chiêu trò dụ dỗ (luring) như hứa hẹn quà tặng, tài khoản game, hoặc tiền bạc.

Tránh để bản thân rơi vào "trauma bonding" – cảm giác phụ thuộc vào những lời khen ngợi giả tạo từ người lạ, khiến em đánh mất sự tỉnh táo.

Hãy tập trung xây dựng hình ảnh tích cực, phản ánh đúng con người thật của em, như sở thích, đam mê, hoặc những khoảnh khắc vui vẻ lành mạnh bên gia đình, bạn bè.

SELFIE VÀ LIVESTREAM AN TOÀN

Không phải mọi bức ảnh selfie hay livestream đều an toàn. Ảnh selfie không an toàn là những bức ảnh tiết lộ thông tin cá nhân (như địa chỉ nhà, trường học, biển số xe), ảnh nhạy cảm (trang phục hở hang, bối cảnh riêng tư), hoặc ảnh có bật định vị (geotag).

Khi livestream, tránh để lộ thông tin về nơi ở, lịch trình, hoặc trò chuyện với người lạ yêu cầu bật camera. Nếu lỡ đăng ảnh/livestream không an toàn, hãy ngay lập tức xóa bài, tắt định vị trên thiết bị, chặn tài khoản lạ tương tác, và báo cho cha mẹ hoặc thầy cô để xử lý.

Hãy kiểm tra cài đặt quyền riêng tư trước khi đăng: Chỉ cho bạn bè thân thiết xem, và luôn tự hỏi: "Mình có muốn cả thế giới thấy bức ảnh này không?".

XÂY DỰNG MỐI QUAN HỆ LÀNH MẠNH VÀ GIỮ KẾT NỐI

ĐỪNG NGẠI KỂ VỚI THẦY CÔ HAY BẠN THÂN VỀ NHỮNG GÌ CHÚNG TA GẶP TRÊN MẠNG

Mạng xã hội có thể cho chúng ta hàng trăm, hàng nghìn bạn bè ảo, nhưng những mối quan hệ thực sự – với cha mẹ, thầy cô, bạn bè thân thiết – mới là chỗ dựa vững chắc khi gặp khó khăn.

Hãy kết bạn với bố mẹ trên mạng xã hội, chia sẻ những câu chuyện vui, những bài đăng thú vị, để bố mẹ hiểu thế giới online của mình. Đừng ngại kể với thầy cô hay bạn thân về những gì chúng ta gặp trên mạng, dù là một tin nhắn lạ hay một lời mời kết bạn đáng ngờ.

MỘT MỐI QUAN HỆ LÀNH MẠNH LÀ NƠI CHÚNG TA CẢM THẤY AN TOÀN ĐỂ CỞI MỞ KHÔNG SỢ BỊ PHÁN XÉT.

DÙ LÀ MỘT TIN NHẮN LẠ HAY MỘT LỜI MỜI KẾT BẠN ĐÁNG NGỜ.

Hãy nhớ: **Kết nối với gia đình và bạn bè ngoài đời thực là "lá chắn" mạnh mẽ nhất, giúp chúng ta không bị cô lập trước những chiêu trò thao túng trực tuyến.**

Mỗi lần trò chuyện với người thân là một lần chúng ta khẳng định:

"Mình không đơn độc, mình có cả thế giới thực để dựa vào!"

MÁCH NHỎ XỬ LÝ TÌNH HUỐNG “ĐỪNG IM LẶNG – HÃY KẾT NỐI”

SỢ HÃI

Sợ hãi là phản ứng tự nhiên khi nhận tin nhắn đe dọa tung ảnh nhạy cảm hay giả danh công an đe dọa xử lý theo pháp luật - nhưng đừng để nó kiểm soát. Hãy dừng mọi liên lạc ngay lập tức:

Chặn số điện thoại, tài khoản lạ, và không làm theo bất kỳ yêu cầu nào như “giữ bí mật” hay “chuyển tiền để xóa bằng chứng” hay “quay toàn thân để xác minh danh tính”.

Thay vào đó, hít thở sâu, ghi lại bằng chứng (ảnh chụp màn hình, ghi âm), và tìm sự hỗ trợ từ những người lớn tin cậy như ông bà, cha mẹ, thầy cô,

hoặc gọi Tổng đài Quốc gia Bảo vệ trẻ em **111** của Bộ Y tế để được hỗ trợ tâm lý và bảo vệ.

Nhớ rằng, cơ quan công an và các cơ quan chức năng khác (tòa án, viện kiểm sát...) không bao giờ yêu cầu làm việc qua điện thoại hay cuộc gọi video.

Các cơ quan cũng không yêu cầu chuyển tiền hoặc kiểm tra tài khoản để chứng minh sự trong sạch hay phòng chống rửa tiền.

NIỀM TIN MÙ QUÁNG

Niềm tin không đúng chỗ khiến chúng ta dễ dàng bỏ qua lời khuyên từ cha mẹ, người thân, xóa lịch sử trò chuyện hay biện minh cho "người lạ thân thiện" – nhưng đó chính là lúc cần dừng lại và kiểm chứng. Hãy tự hỏi:

"Thông tin này có thể kiểm tra được không? Họ có yêu cầu giữ bí mật để ngắt kết nối mình với mọi người?".

Nếu có, hãy kiểm chứng thông tin bằng cách tìm kiếm trên Google, hỏi ý kiến bạn bè hoặc sử dụng công cụ như Google Reverse Image Search để kiểm tra ảnh đại diện của họ.

Quan trọng hơn, hãy có niềm tin vào bản thân: Chúng ta đủ thông minh để nhận ra sự bất thường, không cần phụ thuộc vào lời hứa hẹn từ người lạ.

Chia sẻ toàn bộ câu chuyện với cha mẹ, một người bạn thân hoặc thầy cô giáo mà mình tin tưởng, dù chỉ là đang bối rối về một "người quen online".

Kết nối lại với thực tế: Gọi cho cha mẹ, kể hết, và bạn sẽ thấy niềm tin thực sự đến từ những người quanh mình, không phải từ màn hình hay trên mạng internet.

" NGHI NGỜ
THÌ DỪNG LẠI

LO LẮNG
THÌ CHIA SẺ "

DỤ DỖ

Dụ dỗ bắt đầu bằng quà tặng ảo hay lời khen có cánh, dẫn đến yêu cầu gặp mặt hoặc gửi ảnh – nhưng chúng ta có quyền nói "không" mà không cần giải thích. Không nhận quà tặng, tiền hoặc vật phẩm ảo từ người lạ, dù họ hứa hẹn tài khoản game hay lợi ích lớn.

Nếu ai đó thúc đẩy mối quan hệ bí mật hoặc hứa hẹn lợi ích, hãy nhận ra đó là bẫy: Không gặp mặt ngoài đời thực mà chưa có người lớn đồng hành, và luôn báo cáo tài khoản đáng ngờ trên nền tảng.

Nếu đã lỡ chia sẻ gì đó, đừng tự trách – hãy chặn liên lạc và chia sẻ thông tin với cha mẹ, thầy cô và người thân tin cậy để cùng xử lý. Mỗi lần từ chối dụ dỗ là một bước khẳng định:

"Mình xứng đáng với những mối quan hệ lành mạnh, không phải bí mật độc hại".

→ 3 KHÔNG

01 KHÔNG làm theo yêu cầu giữ bí mật.

02 KHÔNG chia sẻ thông tin cá nhân hoặc ảnh nhạy cảm.

03 KHÔNG tham gia link, Zoom, hoặc gặp mặt người lạ.

→ 3 PHẢI

01 PHẢI chặn và báo cáo ngay.

02 PHẢI kiểm chứng thông tin.

03 PHẢI chia sẻ với người thân.

02 NẾU LÀ GIA ĐÌNH CỦA THANH THIẾU NIÊN

Gia đình là "tấm khiên", là tuyến phòng thủ đầu tiên và vững chắc nhất, nơi sự kết nối được xây dựng từ những cuộc trò chuyện hàng ngày. Cha mẹ và người thân không cần trở thành "giám sát viên" khắc nghiệt, mà hãy là người bạn đồng hành đáng tin cậy của con, giúp con nhận ra dấu hiệu nguy hiểm mà không làm con sợ hãi.

Trách nhiệm của gia đình là cùng con trang bị các công cụ để tự bảo vệ, đồng thời duy trì sợi dây kết nối không bao giờ đứt.

TRANG BỊ KIẾN THỨC, KỸ NĂNG

Hãy biến bữa tối thành **"giờ học an toàn mạng"**. Hãy bắt đầu câu chuyện một cách thân thiện: "Hôm nay ở trên mạng có gì hay không con?" hay "có điều gì làm con băn khoăn không?"

Và bắt đầu thảo luận về các thủ đoạn dụ dỗ qua game online hay đe dọa trên mạng sử dụng ví dụ thực tế từ báo chí để con dễ hình dung.

Dạy con về tư duy phản biện, đặc biệt là quy tắc **“không chia sẻ thông tin cá nhân”**. Tham gia các hội thảo của nhà trường, cơ quan chức năng, hay tổ chức uy tín để cập nhật kiến thức, và thực hành tình huống giả định: **“Nếu con nhận tin nhắn yêu cầu gửi ảnh, con sẽ làm gì?”.**

CHUẨN BỊ SẴN SÀNG NHỮNG PHƯƠNG ÁN ỨNG PHÓ KHI GẶP ĐIỀU KHÔNG MONG MUỐN

BỊ XÂM HẠI, BẠO LỰC HAY “BẮT CÓC ONLINE”.

10

Kiến thức không phải gánh nặng, mà là áo giáp giúp con tự tin đối mặt thế giới trực tuyến.

HỌC HỎI CÙNG CON, CHA MẸ CÓ THỂ ÍT KỸ NĂNG HƠN CON MÌNH TRONG SỬ DỤNG CÔNG NGHỆ

NHƯNG VỚI KINH NGHIỆM VÀ NHỮNG TRẢI NGHIỆM CỦA MÌNH, CHA MẸ CÓ THỂ GIÚP CON QUYẾT ĐỊNH PHÙ HỢP VỚI NHỮNG MỐI QUAN HỆ TRÊN MẠNG.

HÃY CÙNG CON HỌC CÁCH SỬ DỤNG INTERNET VÀ MẠNG XÃ HỘI MỘT CÁCH AN TOÀN VÀ PHÙ HỢP; CÁCH CÀI ĐẶT RIÊNG TƯ VÀ CHIA SẺ THÔNG TIN CÁ NHÂN PHÙ HỢP.

DUY TRÌ KẾT NỐI

KẾT NỐI
KHÔNG PHẢI
THEO DÕI, MÀ LÀ
LẮNG NGHE

Hỏi con về "người bạn online" mà không phán xét, khuyến khích con chia sẻ mọi bí mật mà không sợ bị mắng.

Thiết lập thói quen gia đình như "chia sẻ màn hình hàng tuần" để cùng xem nội dung con thích, xây dựng lòng tin để con dám kể khi bị thao túng.

NHỚ RẰNG,
SỰ CÔ LẬP BẮT ĐẦU
TỪ IM LẶNG.

HÃY CHO CON BIẾT
CHA MẸ LUÔN Ở ĐÓ ĐỂ
ĐỒNG HÀNH
VÀ HỖ TRỢ CON KHI
CẦN THIẾT.

– Hãy là nơi con quay về đầu tiên khi sợ hãi.

• CHÚ Ý CÁC DẤU HIỆU

Hãy quan sát mà không xâm phạm: Thay đổi đột ngột như con khóa mật khẩu, né tránh điện thoại.

Có hành vi hoặc thái độ khác thường, thường mang tính lén lút, hoặc có tiền hay món đồ mới là dấu hiệu đỏ.

CHA MẸ CHÍNH LÀ NHỮNG NGƯỜI GẦN GŨI NHẤT ĐỂ PHÁT HIỆN CÁC VẤN ĐỀ CỦA CON

DÙ VẤN ĐỀ HAY NỖI LO SỢ ĐƯỢC NÓI HAY KHÔNG NÓI BẰNG LỜI.

Sớm nhận ra sợ hãi, tin mù quáng hay đồng tình với người lạ sẽ giúp gia đình can thiệp kịp thời, kéo con ra khỏi bẫy.

Đừng bỏ qua – hãy trò chuyện nhẹ nhàng:

“Có gì đang làm con bận tâm không?”

BÌNH TĨNH XỬ LÝ

Khi con kể về mối đe dọa hoặc dụ dỗ, đừng hoảng loạn hay đổ lỗi – điều đó sẽ đẩy con sâu hơn vào cô lập.

Tìm kiếm sự hỗ trợ ngay từ cơ quan công an địa phương, nhà trường, hoặc chuyên gia tâm lý qua Tổng đài:

111 để được hướng dẫn.

Bình tĩnh là sức mạnh, biến khủng hoảng thành bài học để con trưởng thành.

Hợp tác với ngân hàng nếu có chuyển khoản sai. Theo dõi sức khỏe tinh thần của con.

Dừng mọi liên lạc với đối tượng lạ, chặn số điện thoại, tài khoản mạng xã hội, và không đáp ứng bất kỳ yêu cầu nào.

Sao lưu chứng cứ cẩn thận: chụp ảnh màn hình tin nhắn, ID, URL, lưu file gốc, ghi lại thời gian, nickname, số điện thoại (nếu có), và ghi âm cuộc gọi nếu có thể.

Hãy tìm hiểu nguyên nhân bằng cách nhẹ nhàng hỏi: “Con đã nói chuyện với ai? Họ yêu cầu gì?” để hiểu rõ tình huống. Đồng hành với con bằng cách trấn an: “Chúng ta sẽ cùng giải quyết, con không một mình.”

CHỦ ĐỘNG PHÒNG NGỪA

Chủ động là xây dựng mạng lưới an toàn trước khi nguy hiểm ập đến.

Phòng ngừa bắt đầu từ thói quen:

VỚI TRẺ EM, ĐƯA ĐÓN CON ĐÚNG GIỜ, THỐNG NHẤT VỚI NHÀ TRƯỜNG VỀ NGƯỜI ĐÓN, VÀ HẠN CHẾ CON Ở NHÀ MỘT MÌNH VỚI THIẾT BỊ KẾT NỐI INTERNET.

Tạo tài khoản riêng cho trẻ trên Google hoặc Apple với chế độ quản lý gia đình, cài đặt các công cụ kiểm soát dành cho cha mẹ như Family Link, Screen Time để giới hạn thời gian online, kiểm soát ứng dụng tải về, và nhận báo cáo hoạt động trực tuyến hàng tuần.

Trên cơ sở tôn trọng và thỏa thuận với con về cách thức đảm bảo an toàn khi sử dụng internet.

CHỦ ĐỘNG THIẾT LẬP MẠNG XÃ HỘI CỦA CON Ở CHẾ ĐỘ RIÊNG TƯ, CHỈ CHO PHÉP BẠN BÈ THẬT XEM THÔNG TIN.

KIỂM TRA ĐỊNH KỲ CÙNG CON VÀ CÙNG THẢO LUẬN VỀ DANH SÁCH BẠN BÈ, NHÓM CHAT, VÀ GAME CON ĐANG CHƠI ĐỂ PHÁT HIỆN DẤU HIỆU BẤT THƯỜNG.

Với thanh niên, hướng dẫn các biện pháp an toàn; cùng nói chuyện về những nguy cơ và rủi ro trên mạng, cách thích nghi và phòng tránh. Xây dựng nội quy, thỏa thuận sử dụng internet an toàn. Đảm bảo rằng, cha mẹ sẽ luôn là người hỗ trợ con.

Điều quan trọng, cần trao đổi cởi mở, thẳng thắn và thống nhất với con về những nguyên tắc và giải pháp này

Để con hiểu được bản chất của sự đồng hành mà không phải là kiểm soát "quá đà".

LÀM GƯƠNG

KHI CON THẤY BỐ MẸ TỈNH TÁO VÀ CẨN TRỌNG, CON SẼ HỌC THEO.

Cha mẹ là tấm gương sống về an toàn trực tuyến: Hạn chế chia sẻ quá nhiều thông tin gia đình hay lịch sinh hoạt trên mạng xã hội, như ảnh chụp nhà cửa, trường học, thông tin của con, hoặc lịch trình hàng ngày. Tuân thủ các nguyên tắc bảo vệ thông tin cá nhân của con em.

Cập nhật kiến thức số bằng việc học cách dùng thiết bị thông minh hay mạng xã hội hoặc ứng dụng con thường sử dụng để hiểu rủi ro và trò chuyện với con trên cùng "ngôn ngữ".

BIẾN GIA ĐÌNH THÀNH PHÁO ĐÀI KẾT NỐI VỮNG VÀNG.

Đồng hành thay vì kiểm soát tuyệt đối: Hãy để con cảm thấy an toàn, được tôn trọng quyền riêng tư, nhưng vẫn biết rằng gia đình luôn là nơi con có thể chia sẻ mọi thứ.

03 NẾU LÀ NHÀ TRƯỜNG

Nhà trường không chỉ là nơi truyền đạt kiến thức, mà còn là môi trường rèn luyện kỹ năng sống, nơi học sinh học cách nhận diện và chống lại những cạm bẫy trực tuyến.

↳ Với vai trò là "ngôi nhà thứ hai", nhà trường cần tích hợp giáo dục an toàn mạng vào mọi hoạt động, biến lớp học thành không gian kết nối an toàn.

Nơi không em nào bị cô lập trước những mối nguy trực tuyến.

TRANG BỊ KIẾN THỨC, KỸ NĂNG

TỔ CHỨC CÁC CHƯƠNG TRÌNH NGOẠI KHÓA VỀ CHỦ ĐỀ AN TOÀN MẠNG VÀ "BẮT CÓC ONLINE".

Lồng ghép nội dung an toàn số vào các môn học như Tin học, Giáo dục công dân, hoặc Hoạt động trải nghiệm, sử dụng trò chơi tương tác để dạy quy tắc **"không chia sẻ thông tin cá nhân"** hay **"không gặp người lạ online"**. Kiến thức phải thực tế, giúp học sinh tự tin tuyên ngôn: **"Em biết cách bảo vệ mình trước đe dọa"**.

Dạy học sinh nhận diện dấu hiệu thao túng: yêu cầu bất thường, yêu cầu giữ bí mật, gây sợ hãi, hoặc khen ngợi quá mức đều là tín hiệu đỏ – cần báo ngay cho thầy cô hoặc cha mẹ.

Tập huấn kỹ năng phòng tránh qua các buổi đóng vai tình huống, như cách phản ứng khi nhận được tin nhắn đe dọa hoặc lời mời gặp mặt từ người lạ.

MỜI CHUYÊN GIA TỪ CÁC TỔ CHỨC UY TÍN HOẶC CƠ QUAN CÔNG AN CHIA SẺ CÁC CÂU CHUYỆN THỰC TẾ ĐỂ HỌC SINH DỄ HÌNH DUNG.

TẠO MÔI TRƯỜNG KẾT NỐI

XÂY DỰNG MÔI TRƯỜNG TRƯỜNG HỌC AN TOÀN VÀ CỞI MỞ, NƠI HỌC SINH CẢM THẤY ĐƯỢC BẢO VỆ VÀ LẮNG NGHE.

Hỗ trợ tâm lý cho học sinh bằng cách thiết lập phòng tư vấn tâm lý học đường, duy trì hoạt động thường xuyên để cập nhật và hỗ trợ kịp thời cho học sinh; bảo mật thông tin và tránh kỳ thị khi có học sinh bị dụ dỗ, xâm hại trên mạng.

KHI HỌC SINH CHIA SẺ VẤN ĐỀ, GIÁO VIÊN CẦN LẮNG NGHE KHÔNG PHÁN XÉT, GHI NHẬN VÀ XỬ LÝ NGAY, THAY VÌ TRÁCH MẮNG.

Khuyến khích học sinh tố giác hành vi xấu qua **"hộp thư bí mật"** hoặc nhóm tư vấn, và tổ chức các cuộc thi đua, tuyên truyền về an toàn mạng để lan tỏa nhận thức.

ĐÀO TẠO GIÁO VIÊN NHẬN DIỆN CÁC DẤU HIỆU TRẺ BỊ THAO TÚNG ONLINE

NHƯ LO LẮNG BẤT THƯỜNG HOẶC NÉ TRÁNH GIAO TIẾP, CHE GIẤU ĐIỆN THOẠI, NHẬN QUÀ KHÔNG RÕ NGUỒN GỐC, HOẶC VẮNG MẶT KHÔNG LÝ DO.

ĐỂ PHÁT HIỆN SỚM DẤU HIỆU BỊ DỤ DỖ.

Phối hợp chặt chẽ với cha mẹ, người thân và cơ quan chức năng: tổ chức hội thảo cho cha mẹ và người thân về an toàn mạng, thiết lập kênh liên lạc nhanh qua ứng dụng trường học, và duy trì liên hệ thường xuyên với công an địa phương để tập huấn, chia sẻ tình huống thực tế.

Môi trường kết nối biến trường học thành mạng lưới bảo vệ, nơi mọi học sinh đều cảm thấy an toàn và được hỗ trợ.

04 NẾU LÀ CƠ QUAN QUẢN LÝ

Cơ quan chức năng là "lá chắn thép", không chỉ xử lý mà còn ngăn chặn tội phạm trực tuyến từ gốc rễ.

↳ Do đó, cơ quan chức năng cần xây dựng hệ thống kết nối thân thiện, biến pháp luật thành công cụ dễ tiếp cận, giúp mọi người cảm thấy được hỗ trợ và không một mình trước những mối nguy trực tuyến.

KẾT NỐI THÂN THIỆN

Xây dựng đường dây nóng với nhân viên thân thiện, hỗ trợ tư vấn tâm lý miễn phí cho trẻ em và gia đình nạn nhân, cùng chính sách bảo mật danh tính và cơ chế bảo vệ sau tố cáo, giúp nạn nhân vượt qua tổn thương và tái hòa nhập cộng đồng.

Tiếp cận và hỗ trợ nạn nhân phù hợp, không gây tổn thương thêm về tâm lý.

Kịp thời lắng nghe phản hồi từ cộng đồng. Tổ chức các chiến dịch tại trường học, nơi lực lượng chức năng chia sẻ câu chuyện thực tế về an toàn trực tuyến và bắt cóc online, giúp trẻ tin tưởng và dám lên tiếng báo cáo mà không sợ hãi.

KẾT NỐI TRI THỨC

Phát hành những sản phẩm tuyên truyền, hướng dẫn trẻ em, cha mẹ và người thân cách nhận diện và phòng tránh dụ dỗ, thao túng, “bắt cóc online” với ngôn ngữ dễ hiểu và ví dụ cụ thể.

CÔNG BỐ CÔNG KHAI CÁC VỤ ÁN ĐÃ XỬ LÝ TRÊN CÁC KÊNH TRUYỀN THÔNG ĐỂ CẢNH BÁO CỘNG ĐỒNG

ĐỒNG THỜI TỔ CHỨC CHIẾN DỊCH TRUYỀN THÔNG QUỐC GIA VỚI THÔNG ĐIỆP DỄ NHỚ PHÁT SÓNG TRÊN TV, MẠNG XÃ HỘI, VÀ TRƯỜNG HỌC.

(Lưu ý: những công bố này đảm bảo danh tính và thông tin cá nhân của nạn nhân được bảo mật và bảo vệ)

KẾT NỐI SỨC MẠNH

Phối hợp liên ngành để xây dựng hệ thống phòng ngừa và xử lý hiệu quả. Hợp tác quốc tế với Interpol, ASEANAPOL, các cơ quan Liên hiệp quốc để xử lý tội phạm xuyên biên giới, chia sẻ dữ liệu và kinh nghiệm ngăn chặn.

> Đối thoại với các nền tảng công nghệ, yêu cầu cam kết bảo vệ trẻ em theo pháp luật Việt Nam, bổ sung cơ chế cảnh báo, chặn lọc và gỡ nội dung độc hại trong thời gian ngắn nhất.

Phát triển hệ thống giám sát quốc gia sử dụng công nghệ AI để phát hiện sớm hành vi dụ dỗ trẻ em, tích hợp cảnh báo sớm và lưu trữ dữ liệu về các đối tượng có lịch sử vi phạm.

Sức mạnh đoàn kết từ các cơ quan và tổ chức sẽ tạo nên mạng lưới bảo vệ trẻ em rộng lớn, không để bất kỳ lỗ hổng nào cho tội phạm lợi dụng.

05 ĐỐI VỚI CỘNG ĐỒNG

Cộng đồng là sức mạnh vô hình nhưng mạnh mẽ nhất, nơi mỗi cá nhân là một mắt xích trong chuỗi bảo vệ.

↳ Không ai có thể bị cô lập nếu cộng đồng luôn chung tay hỗ trợ và hành động kịp thời, biến những vụ việc riêng lẻ thành câu chuyện “chung tay chiến thắng”.

• ỨNG XỬ NHÂN VĂN

Không phán xét hay đánh giá tiêu cực những ai thiếu tỉnh táo và trở thành nạn nhân của "bắt cóc online" – thay vào đó, hãy bảo vệ họ khỏi những lời chỉ trích hay kỳ thị.

Đối xử tử tế, không thờ ơ khi người khác gặp rắc rối trên không gian mạng, vì chúng ta không muốn những điều tương tự xảy ra với bản thân mình.

"Một lời động viên nhẹ nhàng có thể phá vỡ sự im lặng và kéo nạn nhân ra khỏi bóng tối."

Khích lệ báo cáo kịp thời các vụ việc để ngăn chặn nguy cơ, tạo môi trường an toàn nơi mọi người dám lên tiếng. Tránh chỉ trích hay đả kích gia đình có con em là nạn nhân của "bắt cóc online", vì điều này có thể khiến họ thêm cô lập và e ngại tìm kiếm sự hỗ trợ.

CHIA SẺ TRÁCH NHIỆM

TRÁCH NHIỆM CHUNG LÀ BIẾN CỘNG ĐỒNG THÀNH MẠNG LƯỚI CẢNH BÁO.

NƠI MỌI NGƯỜI CÙNG NHAU NGĂN CHẶN TỘI PHẠM.

Chia sẻ thông tin đúng, đã được kiểm chứng, về các thủ đoạn lừa đảo mới và cách phòng tránh trên các nhóm cộng đồng có tính lan tỏa, như nhóm cha mẹ và người thân hoặc tổ dân phố.

Không chia sẻ hình ảnh nhạy cảm, thông tin cá nhân của nạn nhân, và ngừng đăng hoặc xóa bỏ thông tin, hình ảnh đã đăng để hỗ trợ tìm kiếm trước đó khi không còn cần thiết.

Chia sẻ các nội dung tích cực, bảo vệ, thay vì chỉ trích hay phán xét, để xây dựng một cộng đồng đoàn kết.

HỖ TRỢ HIỆU QUẢ

Chia sẻ thông tin cần thiết để hỗ trợ tìm kiếm, giải cứu, hoặc cảnh báo nạn nhân, sử dụng các nhóm cộng đồng cư dân trên mạng xã hội để lan tỏa thông tin nhanh chóng.

Tổ chức các câu lạc bộ tình nguyện hướng dẫn kỹ năng số. Tăng tính đoàn kết cộng đồng bằng cách quan sát lẫn nhau:

> Nếu thấy trẻ đi với người lạ bất thường, hãy hỏi han hoặc cảnh báo phụ huynh ngay. Hỗ trợ khi trẻ cầu cứu bằng cách giúp trẻ gọi Tổng đài 111 hoặc 113, hoặc thông báo cho cơ quan chức năng.

Hỗ trợ các gia đình có trẻ em gặp vấn đề qua tư vấn miễn phí, hoặc theo dõi tâm lý lâu dài.

Cộng đồng mạnh mẽ khi hành động cụ thể!

06 ĐỐI VỚI NỀN TẢNG

Các nền tảng mạng xã hội, game online là "sân chơi" trực tuyến, nhưng cũng là nơi tội phạm ẩn náu.

↳ Với trách nhiệm xã hội, các nền tảng phải ưu tiên tối đa các giải pháp và cam kết bảo vệ trẻ em, biến công nghệ thành người bạn đồng hành an toàn thay vì bẫy rập nguy hiểm.

- ĐỐI TƯỢNG ƯU TIÊN

Xác định trẻ em và thanh thiếu niên là nhóm ưu tiên

Áp dụng chính sách và công nghệ bảo vệ đặc biệt, như tăng cường sử dụng công nghệ xác định người dùng, hạn chế người dùng là trẻ em; thiết lập cơ chế báo cáo và chia sẻ thông tin với cơ quan chức năng; thiết lập đường dây ưu tiên xử lý báo cáo liên quan đến trẻ trong vòng 24 giờ.

Tạo chế độ riêng cho tài khoản trẻ dưới 16 tuổi, mặc định chặn tin nhắn từ người lạ, ẩn thông tin cá nhân, hạn chế livestream trẻ em và nhóm kín.

Tích hợp nút “SOS/Help” hiển thị rõ ràng trong ứng dụng để trẻ báo cáo nhanh khi bị quấy rối, đảm bảo trẻ có công cụ tự bảo vệ dễ tiếp cận.

• ĐỊNH HƯỚNG TÍCH CỰC

Hợp tác với chuyên gia tâm lý để xây dựng nội dung nâng cao nhận thức cho thanh thiếu niên, giúp các em hiểu rủi ro trực tuyến.

Cấm quảng cáo nhắm vào trẻ em với nội dung nguy cơ, như casting giả, lời mời việc làm, hoặc game hẹn gặp.

Khuyến khích đăng tải nội dung giáo dục về kỹ năng số và kỹ năng sống cho trẻ em, như video hướng dẫn nhận diện lừa đảo hoặc cách từ chối yêu cầu bất thường

Định hướng nền tảng thành không gian sáng tạo, nơi trẻ học hỏi và phát triển an toàn.

NGĂN CHẶN HIỆU QUẢ

Ban hành quy định nghiêm ngặt cấm mọi hình thức dụ dỗ, lừa gạt trẻ em, hoặc trao đổi thông tin cá nhân của trẻ. Xây dựng bộ Quy tắc ứng xử cho trẻ em online, yêu cầu người dùng tuân thủ.

Ứng dụng AI và machine learning để phát hiện kịp thời nội dung mang tính dụ dỗ, hẹn gặp, hoặc đe dọa, tự động cảnh báo khi phát hiện hành vi bất thường, như một tài khoản gửi nhiều tin nhạy cảm đến trẻ.

Xác minh danh tính nâng cao cho các tài khoản nhắn tin thường xuyên với trẻ em, gắn cờ hoặc chặn những tài khoản có hành vi gửi kết bạn hàng loạt đến trẻ em và thanh thiếu niên.

Hợp tác chặt chẽ với cơ quan chức năng, chia sẻ dữ liệu về tài khoản nghi vấn và hỗ trợ điều tra xuyên biên giới.

> “Ngăn chặn không chỉ là xóa sổ rủi ro, mà là xây dựng hệ thống nơi an toàn là mặc định, kết nối là ưu tiên.”

Minh bạch báo cáo định kỳ, công khai số lượng tài khoản dụ dỗ trẻ bị gỡ hoặc chặn, cùng thời gian xử lý. Tạo chương trình chứng nhận “Nền tảng an toàn cho trẻ” để khuyến khích cải thiện và tăng uy tín. Thưởng cho người dùng báo cáo tài khoản dụ dỗ trẻ, khuyến khích cộng đồng cùng tham gia bảo vệ.

10 ĐIỀU
THANH THIẾU NIÊN CẦN NHỚ KỸ ĐỂ AN TOÀN TRỰC TUYẾN

01 **KHÔNG CHIA SẺ THÔNG TIN CÁ NHÂN** → Đừng công khai số điện thoại, địa chỉ nhà, CCCD, hoặc thông tin riêng tư trên mạng xã hội. Chỉ chia sẻ những gì chúng ta muốn cả thế giới biết!

02 **CẨN THẬN VỚI NGƯỜI LẠ** → Không kết bạn hoặc trả lời tin nhắn từ người không quen ngoài đời. Kiểm tra kỹ danh tính: Họ có bạn chung đáng tin không? Ảnh đại diện có thật không?

03 **GIỮ BÍ MẬT LÀ DẤU HIỆU ĐỎ** → Nếu ai đó yêu cầu giữ bí mật về cuộc trò chuyện hoặc mối quan hệ online, hãy cảnh giác. Kể ngay cho bố mẹ hoặc bạn bè thân!

04 **KHÔNG CLICK LINK LẠ, KHÔNG THAM GIA ZOOM LẠ** → Đừng truy cập link hoặc phòng chat/Zoom từ người lạ, dù họ hứa tặng quà hay tài khoản game. Công an không bao giờ làm việc qua Zoom!

05 **TỪ CHỐI YÊU CẦU NHẠY CẢM** → Không chụp ảnh, quay video riêng tư theo yêu cầu của bất kỳ ai. Nếu lỡ gửi, chặn liên lạc ngay và báo cho người thân để xử lý.

06 **BẢO VỆ HÌNH ẢNH CÁ NHÂN** → Chỉ đăng ảnh hoặc livestream không tiết lộ địa chỉ, trường học, hoặc thông tin cá nhân.

07 **KẾT NỐI VỚI GIA ĐÌNH, BẠN BÈ** → Kết bạn với bố mẹ trên mạng xã hội, chia sẻ chuyện vui, và kể ngay nếu gặp tin nhắn lạ. Gia đình là "lá chắn" mạnh nhất của chúng ta!

08 **NGỪNG LẠI KHI SỢ HÃI HOẶC BỐI RỐI** → Nếu nhận tin nhắn đe dọa hoặc cảm thấy hoang mang, dừng lại, hít thở sâu, chụp màn hình bằng chứng, và hỏi ý kiến người lớn tin cậy.

09 **KHÔNG NHẬN QUÀ, KHÔNG GẶP RIÊNG** → Từ chối quà tặng, tiền, hoặc vật phẩm ảo từ người lạ. Không gặp người quen online một mình, luôn có người lớn đi cùng ở nơi công cộng.

10 **BÁO CÁO NGAY KHI NGHI NGỜ** → Chặn tài khoản đáng ngờ, báo cáo lên nền tảng (Facebook, Zalo, TikTok), và gọi Tổng đài 111 hoặc công an nếu cảm thấy nguy hiểm. Chúng ta không bao giờ đơn độc!

(NHỚ RẰNG)

Kết nối là chìa khóa!

LUÔN CHIA SẺ VỚI GIA ĐÌNH, BẠN BÈ, HOẶC THẦY CÔ ĐỂ PHÁ VỠ BẪY CÔ LẬP CỦA TỘI PHẠM. CHÚNG TA ĐỦ THÔNG MINH ĐỂ GIỮ AN TOÀN!

(PHẦN 05)

THÔNG TIN CẨM NANG

KHÔNG MÌNH

Ngày bắt đầu: 15/9/2025

Ngày chỉnh sửa cuối: 02/10/2025

Phiên bản: 2.0

Đơn vị dẫn dắt: LIÊN MINH NIỀM TIN SỐ

Tham gia biên tập:

1. CỤC AN NINH MẠNG & PCTP SỬ DỤNG CÔNG NGHỆ CAO
2. HIỆP HỘI AN NINH MẠNG QUỐC GIA
3. CỤC BÀ MẸ VÀ TRẺ EM
4. UNODC
5. UNICEF
6. MSD
7. CHILDFUND VIỆT NAM
8. WORLD VISION INTERNATIONAL
9. SAVE THE CHILDREN
10. PLAN INTERNATIONAL
11. HỘI BẢO VỆ QUYỀN TRẺ EM (VACR)

Phụ trách thiết kế: ZEIT MEDIA

01001011 01001000 01001110 01000111 00100000
01001101 01001111 01010100 00100000 01001101 01001001
01001110 01001000 00100000
01001000 01000001 01001110 00100000
01010011 01001111

01001011 01001000 01001111 01001110 01000111 00100000
00100000 01001101 01001001
01001110 01001000 01001100 01000001 00100000
01000011 01001000 01000001 01001110 00100000
01010011 01001111

01001011 01001000 01001111 01001110 01000111 00100000
01001101 01001111 01010100 00100000 01001101 01001001
01001000 00100000
01000011 01001000 01000001 01001110 00100000
01010011 01001111

01001111 01001110 01000111 00100000
01001101 01001111 01010100 00100000 01001101 01001001
01001110 01001000 01001100 01000001 00100000
01000011 01001000 01000001 01001110 00100000
01010011 01001111

01001011 01001000 01001111 01001110 01000111 00100000
01001101 01001111 01010100 00100000 01001101 01001001
01001110 01000001 00100000
01000011 01001000 01000001 01001110 00100000
01010011 01001111

01001011 01001000 01001111 01001110 01000111
01001101 01001111 01010100 00100000 01001101 01001001
01001110 01001000 01001100 01000001 00100000
01000001 01001110 00100000
01010011 01001111

01001011 01001000 01001110 01000111 00100000
01001101 01001111 01010100 00100000 01001101 01001001
01001100 01000001 00100000
01000011 01001000 01000001 01001110 00100000