

CẨM NANG
KẾT NỐI KHÔNG TÔN THƯƠNG

*Nhận diện, phòng ngừa và ứng phó ban đầu với xâm hại trực tuyến
đối với trẻ em, thanh thiếu niên*

Hà Nội, 2026

MỤC LỤC

LỜI NÓI ĐẦU

PHẦN I. XÂM HẠI TRẺ EM TRÊN KHÔNG GIAN MẠNG LÀ GÌ

Xâm hại trẻ em trên không gian mạng là gì?

Vì sao xâm hại trên mạng lại gây tổn thương thật cho trẻ em?

Thực trạng tại Việt Nam

Ai là người xâm hại trẻ em trên không gian mạng?

Có phải chỉ trẻ em gái mới bị xâm hại tình dục qua mạng?

PHẦN II. CÁC HÌNH THỨC XÂM HẠI TRỰC TUYẾN THƯỜNG GẶP

1. Dụ dỗ, gạ gẫm trẻ em nhằm mục đích tình dục
2. Tổng tiền bằng hình ảnh riêng tư
3. Bắt nạt, làm nhục và cô lập trẻ em trên không gian mạng
4. Phát tán hình ảnh, thông tin riêng tư của trẻ em
5. Lan truyền, tiếp tay làm gia tăng tổn thương
6. Lợi dụng trí tuệ nhân tạo để tạo nội dung xâm hại

PHẦN III. DẤU HIỆU NHẬN BIẾT VÀ LÝ DO TRẺ EM GIỮ IM LẶNG

Những dấu hiệu người lớn cần chú ý

Vì sao trẻ em bị xâm hại thường không kể với cha mẹ hay thầy cô?

Cách mở lời khi nghi ngờ có chuyện

PHẦN IV. CÁC BƯỚC XỬ LÝ KHI TRẺ EM BỊ XÂM HẠI TRỰC TUYẾN

Bước thứ nhất – Dừng lại và cắt nguồn gây hại

Bước thứ hai – Không lan truyền nội dung xâm hại

Bước thứ ba – Lưu giữ bằng chứng một cách an toàn

Bước thứ tư – Báo cáo vi phạm trên nền tảng

Bước thứ năm – Đưa người lớn tin cậy vào cuộc

Khi nào cần báo cơ quan công an?

Người lớn nên nói gì trong lần đầu tiên trẻ kể chuyện?

Có nên hứa giữ bí mật tuyệt đối với trẻ không?

Có nên thu điện thoại của trẻ sau khi sự việc xảy ra không?

PHẦN V. TRÁCH NHIỆM CỦA GIA ĐÌNH, NHÀ TRƯỜNG VÀ CÁC BÊN LIÊN QUAN

Trẻ em, thanh thiếu niên

Cha mẹ và người chăm sóc

Đăng ảnh con lên mạng xã hội có làm tăng nguy cơ cho trẻ không?

Nhà trường và giáo viên

Doanh nghiệp và nền tảng số

Cơ quan báo chí và người có ảnh hưởng

PHẦN VI. ĐỊA CHỈ HỖ TRỢ VÀ CĂN CỨ PHÁP LÝ

Tổng đài quốc gia bảo vệ trẻ em 111

Các đầu mối hỗ trợ khác

Căn cứ pháp lý hiện hành

LỜI KẾT

LỜI NÓI ĐẦU

Cẩm nang này ra đời từ một câu chuyện có thật. Một người mẹ nhận ra con gái mình đã ba đêm liền không ngủ. Cô bé vẫn ăn cơm cùng gia đình, vẫn ngồi vào bàn học như thường lệ, nhưng không còn cầm điện thoại và đã xin nghỉ học hai ngày liên tiếp. Gần một tuần sau, người mẹ mới biết rằng một bức ảnh riêng tư của con đã bị phát tán trong các nhóm lớp.

Trong suốt bảy ngày ấy, một đứa trẻ mười bốn tuổi đã phải tự mình đối mặt với mọi chuyện ngay trong chính ngôi nhà của mình, chỉ cách bố mẹ vài bước chân. Cẩm nang này được viết để góp phần rút ngắn khoảng thời gian đó, giúp người lớn nhận ra sớm hơn và giúp trẻ tìm được sự hỗ trợ ngay khi sự việc xảy ra.

Những vụ xâm hại trẻ em trên không gian mạng hiếm khi bắt đầu bằng một sự việc đủ nghiêm trọng để người lớn nhận ra ngay. Chúng thường khởi đầu từ một lời khen, một món quà nhỏ trong trò chơi, lời đề nghị chuyển sang ứng dụng nhắn tin khác hoặc lời dặn giữ bí mật giữa hai người. Vì những dấu hiệu này đều có vẻ bình thường, gia đình thường chỉ nhận ra khi sự việc đã tiến triển khá xa.

Cẩm nang được trình bày dưới dạng hỏi và đáp. Mỗi mục tập trung vào một câu hỏi mà trẻ em, cha mẹ, thầy cô hoặc cán bộ làm công tác bảo vệ trẻ em thường gặp, kèm theo phần trả lời ngắn gọn và dễ áp dụng. Người đọc có thể tìm trực tiếp đến câu hỏi phù hợp với tình huống của mình mà không cần đọc lần lượt từ đầu đến cuối.

Nội dung cẩm nang gồm sáu phần. Phần thứ nhất giúp người đọc hiểu đúng về xâm hại trực tuyến. Phần thứ hai giới thiệu các hình thức xâm hại thường gặp. Phần thứ ba hướng dẫn nhận biết các dấu hiệu và lý giải vì sao trẻ thường giữ im lặng. Phần thứ tư trình bày cách xử lý khi sự việc đã xảy ra. Phần thứ năm làm rõ trách nhiệm của các bên liên quan. Phần cuối cung cấp địa chỉ hỗ trợ và các căn cứ pháp lý cần thiết.

Thông qua cẩm nang này, đội ngũ biên soạn mong góp phần xây dựng một môi trường số an toàn hơn cho trẻ em, nơi các em có thể học tập, kết bạn, giao tiếp và chia sẻ mà không phải đối mặt với những hành vi gây tổn thương.

Chuyện xảy ra trên mạng vẫn có thể gây tổn thương thật.

Không một đứa trẻ nào phải tự mình đối diện với tổn thương ấy.

PHẦN I

**XÂM HẠI TRẺ EM
TRÊN KHÔNG GIAN MẠNG LÀ GÌ**

Xâm hại trẻ em trên không gian mạng là gì?

Xâm hại trẻ em, thanh thiếu niên trên không gian mạng là việc một người sử dụng môi trường số để gây tổn hại cho trẻ về thân thể, tinh thần, danh dự, nhân phẩm hoặc quyền riêng tư. Hành vi ấy có thể diễn ra hoàn toàn trên mạng như khi một đứa trẻ bị bắt nạt trong nhóm chat của lớp, hoặc bắt đầu trên mạng rồi dẫn đến tổn hại ngoài đời thực như khi một người quen qua trò chơi trực tuyến hẹn gặp đứa trẻ ở ngoài.

Trong khuôn khổ cẩm nang này, xâm hại trực tuyến được hiểu bao gồm sáu nhóm hành vi thường gặp, bao gồm: (1) dụ dỗ và gạ gẫm trẻ em nhằm mục đích tình dục, (2) quấy rối cùng đe dọa và ép buộc trẻ em qua môi trường mạng, (3) bắt nạt, bắt nạt và làm nhục hoặc cô lập trẻ em, (4) xâm phạm quyền riêng tư cùng việc phát tán hay đe dọa phát tán thông tin riêng tư của trẻ em, (5) mạo danh và thao túng để tiếp cận hoặc kiểm soát trẻ em, và (6) hành động lan truyền hay tiếp tay khiến tổn thương của trẻ em gia tăng thêm.

Ranh giới giữa hai thế giới trên mạng và ngoài đời hầu như không tồn tại trong trải nghiệm của trẻ, bởi với các em thì bạn bè trong nhóm chat cũng là bạn bè thật, lời chế giễu trên mạng cũng là lời chế giễu thật, và nỗi sợ mà em mang theo khi tắt máy cũng là nỗi sợ thật.

Người lớn thường phân biệt rạch ròi giữa chuyện trên mạng và chuyện ngoài đời rồi từ đó cho rằng chuyện trên mạng thì nhẹ hơn, trong khi trẻ em lại không phân biệt như vậy bởi các em đang sống liên tục trong cả hai thế giới ấy cùng một lúc.

Vì sao xâm hại trên mạng lại gây tổn thương thật cho trẻ em?

Trước hết, loại xâm hại này không có điểm dừng về thời gian và không gian. Một đứa trẻ bị bắt nạt ở trường vẫn còn một quãng nghỉ khi bước qua cổng nhà, trong khi một đứa trẻ bị bắt nạt trong nhóm chat thì không có quãng nghỉ nào cả do chiếc điện thoại nằm ngay trên bàn học và nhóm ấy vẫn tiếp tục sáng đèn lúc mười một giờ đêm.

Một nội dung xâm hại khi đã rời khỏi tay chủ nhân thường tồn tại tại rất lâu. Các nội dung này có thể được lưu lại trong máy người này rồi chuyển tiếp sang nhóm người kia và bất chợt xuất hiện trở lại sau vài năm ở một nơi mà không ai ngờ tới. Mỗi lần nội dung ấy quay lại thì đứa trẻ trong sự việc đó lại phải chịu thêm một lần tổn thương mới dù sự việc ban đầu đã xảy ra xa từ lâu.

Cuối cùng, và đây là điều khiến việc hỗ trợ trở nên khó khăn nhất, trẻ em thường tự nhận lỗi về phía mình bởi chính em đã chủ động trò chuyện, đã tự tay gửi tấm ảnh hoặc tự nhấn vào đường dẫn. Từ góc nhìn của em thì mọi chuyện xảy ra đều do em gây ra, và suy nghĩ ấy đủ nặng đã khiến nhiều em im lặng trong một thời gian rất dài.

Có thể ví một nội dung xâm hại đã bị phát tán như một vết dầu loang trên mặt nước, bởi nó không tự mất đi mà chỉ lan rộng thêm mỗi khi có người khuấy vào.

Thực trạng tại Việt Nam

Theo nghiên cứu Disrupting Harm tại Việt Nam do ECPAT International, INTERPOL và Quỹ Nhi đồng Liên hợp quốc thực hiện, có 89% trẻ em trong độ tuổi 12–17 sử dụng internet và hầu hết các em truy cập bằng điện thoại thông minh, tức là bằng một thiết bị cá nhân nằm ngoài tầm quan sát trực tiếp của cha mẹ.¹

Cũng theo nghiên cứu này, tại Việt Nam, nghiên cứu Disrupting Harm ước tính có khoảng 94.000 trẻ sử dụng Internet trong độ tuổi 12–17 là nạn nhân của các hành vi xâm hại hoặc bóc lột tình dục qua mạng.

Ở quy mô rộng hơn, báo cáo Through Children’s Eyes: How Digital Technologies Enable Child Sexual Abuse của UNICEF năm 2026 tại 21 quốc gia cho thấy khoảng 20 triệu trẻ em sử dụng Internet đã trải qua ít nhất một hình thức bóc lột hoặc xâm hại tình dục có yếu tố công nghệ trong vòng một năm. Trong số này, hơn 15 triệu trẻ từng tiếp xúc với nội dung tình dục không mong muốn, khoảng 9 triệu trẻ từng bị yêu cầu tham gia các cuộc trò chuyện tình dục hoặc chia sẻ hình ảnh tình dục trái với mong muốn và khoảng 4 triệu trẻ từng bị chia sẻ hình ảnh tình dục của mình mà không có sự đồng ý.

Cũng theo báo cáo của UNICEF, gần 60% các trường hợp được ghi nhận xảy ra trên các nền tảng mạng xã hội phổ biến, khoảng 14% liên quan đến tương tác trong trò chơi trực tuyến. Riêng tại Việt Nam, hơn 56% trường hợp được ghi nhận có liên quan đến nền tảng mạng xã hội.

Ai là người xâm hại trẻ em trên không gian mạng?

Theo nghiên cứu của UNICEF tại 21 quốc gia, 57% các trường hợp được khảo sát liên quan đến người mà trẻ đã quen biết, bao gồm bạn bè cùng trang lứa, người yêu, bạn bè hoặc thành viên gia đình. Đồng thời, 38% trẻ cho biết lần đầu tiếp xúc với người thực hiện hành vi xâm hại là trên môi trường mạng.

Nhiều gia đình vẫn hình dung người gây hại là một kẻ xa lạ, ẩn danh ở phía bên kia màn hình. Tuy nhiên, thực tế thường phức tạp hơn nhiều.

Trong phần lớn các vụ bắt nạt hoặc làm nhục trực tuyến, người gây hại có thể chính là bạn cùng lớp, người vẫn gặp nạn nhân mỗi ngày. Trong các vụ dụ dỗ nhằm mục đích tình dục, người gây hại thường dành nhiều tuần để làm quen, tạo dựng lòng tin và khiến trẻ xem mình như một người bạn đáng tin cậy trước khi đưa ra yêu cầu đầu tiên.

Đối với những vụ phát tán hình ảnh riêng tư, thiệt hại nhiều khi lại đến từ những người ban đầu không có chủ ý gây hại. Đó có thể là các bạn học chỉ đơn giản chuyển tiếp một hình ảnh mà các em thấy buồn cười, nhưng không lường trước được hậu quả đối với người trong ảnh.

Cách nhìn nhận này có ý nghĩa quan trọng đối với việc phòng ngừa và giảm thiểu thiệt hại cho trẻ em. Nếu người gây hại luôn là người lạ, việc dạy trẻ tránh tiếp xúc với người lạ có thể là đủ. Tuy nhiên, trong nhiều trường hợp, người gây hại lại là người quen. Vì vậy, trẻ cần được dạy cách nhận biết những hành vi và dấu hiệu bất thường, thay vì chỉ học cách nhận diện một nhóm người cụ thể.

¹ ECPAT International, INTERPOL và Quỹ Nhi đồng Liên hợp quốc (Văn phòng Nghiên cứu Innocenti), Disrupting Harm in Viet Nam, 2022. Khảo sát 994 trẻ em 12–17 tuổi có sử dụng internet và 994 người chăm sóc, mẫu đại diện quốc gia, thực địa tháng 11/2020 – tháng 02/2021.

Có phải chỉ trẻ em gái mới bị xâm hại tình dục qua mạng?

Nhiều gia đình vẫn cho rằng chỉ con gái mới có nguy cơ bị xâm hại tình dục qua mạng. Vì vậy, họ thường tập trung dặn dò con gái mà ít khi trò chuyện với con trai về những rủi ro tương tự. Khoảng trống này có thể khiến trẻ em nam trở nên đặc biệt dễ tổn thương khi sự việc xảy ra.

Dữ liệu quốc tế về hành vi tống tiền bằng hình ảnh riêng tư cho thấy phần lớn nạn nhân được xác định là trẻ em nam trong độ tuổi từ 14 đến 17. Trong những vụ việc này, kẻ gây hại thường lợi dụng cảm giác xấu hổ và tạo ra áp lực phải phản ứng ngay, khiến nạn nhân hoảng loạn và không nghĩ đến việc tìm kiếm sự giúp đỡ trong những giờ đầu tiên.²

Trẻ em nam còn gặp một bất lợi khác: các em hiếm khi được trò chuyện hoặc hướng dẫn đầy đủ về vấn đề này. Vì thế, khi sự việc xảy ra, các em vừa không biết gọi tên hành vi mình đang gặp phải, vừa ngại chia sẻ vì sợ bị chê cười hoặc đánh giá.

² National Center for Missing & Exploited Children, Sextortion Data 2025.

PHẦN II

**CÁC HÌNH THỨC XÂM HẠI
TRỰC TUYẾN THƯỜNG GẶP**

Kẻ xâm hại dụ dỗ, gạt gẫm trẻ em qua mạng như thế nào?

Định nghĩa: Dụ dỗ, gạt gẫm trẻ em qua mạng là quá trình kẻ xâm hại từng bước tạo dựng lòng tin và hình thành mối quan hệ thân thiết với trẻ nhằm đưa ra những yêu cầu có tính xâm hại. Quá trình này thường diễn ra âm thầm trong thời gian dài, khiến trẻ dần coi kẻ xâm hại là một người bạn đáng tin cậy thay vì một người lạ trên mạng.

Dấu hiệu thường gặp: Kẻ xâm hại thường bắt đầu bằng sự quan tâm dồn dập, những lời khen, sự đồng cảm hoặc quà tặng nhỏ trong trò chơi. Khi trẻ đã bớt cảnh giác, chúng bắt đầu thăm dò mức độ giám sát của gia đình, chẳng hạn hỏi trẻ có thường ở nhà một mình không, bố mẹ có kiểm tra điện thoại không hoặc trẻ có thể nhắn tin vào thời điểm nào mà không bị phát hiện. Sau đó, chúng đề nghị chuyển sang một ứng dụng riêng tư hơn, yêu cầu trẻ xóa tin nhắn, giữ bí mật và khiến trẻ tin rằng đây là mối quan hệ đặc biệt chỉ thuộc về hai người.

Hậu quả: Khi đã tạo được đủ lòng tin và tách trẻ khỏi sự hỗ trợ của người lớn, kẻ xâm hại mới bắt đầu đưa ra những yêu cầu khiến trẻ cảm thấy không thoải mái, thường liên quan đến hình ảnh riêng tư hoặc gặp mặt trực tiếp. Nếu trẻ từ chối hoặc muốn dừng lại, chúng có thể chuyển sang trách móc, đe dọa hoặc sử dụng chính những điều trẻ từng tâm sự để gây áp lực. Trẻ vì thế dễ cảm thấy xấu hổ, có lỗi và tiếp tục im lặng thay vì tìm người giúp đỡ.

Minh học lớp 8 và quen một người anh trong trò chơi trực tuyến, một người chơi rất giỏi lại lúc nào cũng khen em, nên vốn khá lặng lẽ ở lớp thì Minh thấy vui khi lần đầu tiên có người chú ý đến mình nhiều đến vậy. Ít lâu sau, người anh ấy rủ em nhắn tin qua một ứng dụng khác cho tiện kèm theo lời dặn rằng đây là chuyện riêng của hai anh em, và đến khi anh ta đòi em một thứ mà em thấy không đúng rồi em muốn dừng lại thì anh ta dọa sẽ kể cho mọi người nghe những điều em từng tâm sự, khiến suốt nhiều tuần liền Minh vẫn tin rằng đây là lỗi của chính mình.

Quá trình dụ dỗ trẻ em qua mạng có thể diễn ra nhanh đến mức nào?

Nhiều phụ huynh vẫn cho rằng quá trình dụ dỗ trẻ thường kéo dài nhiều tháng. Vì vậy, khi thấy con chỉ chơi trò chơi trực tuyến trong một khoảng thời gian ngắn, họ dễ chủ quan và bỏ lỡ giai đoạn có thể can thiệp sớm nhất.

Theo phân tích của Liên minh Toàn cầu WeProtect, trong các trò chơi trực tuyến có yếu tố tương tác xã hội, một tình huống dụ dỗ có nguy cơ cao có thể hình thành chỉ sau khoảng 45 phút. Trường hợp nhanh nhất từng được ghi nhận chỉ kéo dài 19 giây.³

Điều này không có nghĩa là mọi cuộc trò chuyện trực tuyến đều nguy hiểm. Tuy nhiên, thời lượng sử dụng không phải là căn cứ đáng tin cậy để đánh giá mức độ an toàn. Điều phụ huynh cần quan tâm hơn là nội dung và diễn biến của cuộc trò chuyện, chứ không chỉ là thời gian trẻ ở trên mạng.

³ Liên minh Toàn cầu WeProtect, Global Threat Assessment 2023.

Vì sao trẻ tin một người chưa từng gặp mặt?

Câu hỏi này thường được người lớn đặt ra kèm theo đôi chút trách móc dành cho đứa trẻ, thế nhưng câu trả lời lại khá đơn giản và hoàn toàn không liên quan gì đến sự khờ dại của các em cả.

Người gây hại thường lấp đúng vào một khoảng trống mà đứa trẻ đang có, bởi với một em ít bạn ở lớp thì đó là sự chú ý, với một em hay bị so sánh với anh chị em thì đó là lời khen, còn với một em có cha mẹ quá bận rộn thì đó đơn giản chỉ là một người chịu ngồi nghe em nói mỗi tối.

Mối quan hệ này cũng được xây dựng từng bước, thay vì xuất hiện một cách đột ngột. Vì vậy, đến khi yêu cầu đầu tiên được đưa ra, kẻ xâm hại trong mắt đứa trẻ đã trở thành một người bạn thân thiết chứ không còn là một người xa lạ.

Tổng tiền bằng hình ảnh riêng tư diễn ra như thế nào?

Định nghĩa: Tổng tiền bằng hình ảnh riêng tư là hành vi kẻ xâm hại sử dụng hình ảnh nhạy cảm của trẻ để đe dọa và buộc các em tiếp tục gửi thêm hình ảnh, giữ im lặng, chuyển tiền hoặc làm theo những yêu cầu khác. Hành vi này thường xuất hiện sau giai đoạn dụ dỗ, nhưng cũng có thể bắt đầu khi kẻ xâm hại lừa trẻ gửi ảnh hoặc chiếm được hình ảnh từ tài khoản, thiết bị hay một nguồn khác.

Dấu hiệu thường gặp: Kẻ xâm hại thường tạo ra đồng thời cảm giác xấu hổ và gấp gáp. Chúng có thể dọa gửi hình ảnh cho gia đình, bạn bè, nhà trường hoặc đăng lên mạng ngay trong đêm, đồng thời liên tục đặt ra thời hạn rất ngắn. Trẻ bị thúc ép phải trả lời ngay, không được ngắt liên lạc và không được kể cho bất kỳ ai. Trong trạng thái hoảng loạn, trẻ dễ tin rằng mình chỉ còn vài phút để quyết định và việc làm theo yêu cầu là cách duy nhất để ngăn hình ảnh bị phát tán.

Hậu quả: Việc tiếp tục đáp ứng thường không khiến lời đe dọa chấm dứt. Mỗi lần trẻ làm theo, kẻ xâm hại càng biết rằng cách gây áp lực của mình có hiệu quả và tiếp tục đưa ra những yêu cầu lớn hơn. Trẻ có thể rơi vào vòng lặp kéo dài của sợ hãi, xấu hổ và bị kiểm soát, trong khi càng ngày càng khó tìm kiếm sự giúp đỡ vì lo bị trách mắng hoặc bị người khác biết chuyện.

Bắt nạt, làm nhục và cô lập trẻ em trên không gian mạng diễn ra như thế nào?

Định nghĩa: Bắt nạt trên mạng là việc một người hoặc một nhóm người sử dụng tin nhắn, hình ảnh, video, bình luận hay các nhóm trò chuyện để chế giễu, làm nhục, đe dọa hoặc cô lập một đứa trẻ. Hành vi này có thể diễn ra công khai trước nhiều người hoặc âm thầm trong những nhóm riêng mà người lớn không biết đến.

Dấu hiệu thường gặp: Khác với bắt nạt trực tiếp, bắt nạt trên mạng không dừng lại khi buổi học kết thúc. Trẻ có thể bị đặt biệt danh để chế giễu, bị đưa ra bàn luận trong nhóm chat, bị loại khỏi các nhóm chung hoặc trở thành mục tiêu của những hình ảnh và bình luận ác ý. Hành vi này thường có nhiều người cùng tham gia hoặc hưởng ứng. Phạm vi tổn thương cũng có thể mở rộng rất nhanh. Một lời chế giễu ở sân trường có thể chỉ vài người nghe thấy, nhưng khi được đưa vào nhóm lớp, cả lớp

đều có thể đọc, bình luận, chụp lại và chuyển tiếp sang những nhóm khác. Mỗi lần nội dung ấy được chia sẻ, số người chứng kiến lại tăng lên và trẻ càng cảm thấy mình bị bêu ra trước đám đông.

Hậu quả: Trẻ bị nhắm đến thường không kể ngay với người lớn vì sợ bị coi là mách lẻo, sợ bị trả đũa hoặc không tin rằng cha mẹ và thầy cô sẽ hiểu những gì đang diễn ra trong nhóm chat. Vì vậy, trước khi trẻ lên tiếng, người lớn thường chỉ nhận thấy những thay đổi trong hành vi như thu mình, né tránh bạn bè, không muốn đến trường hoặc trở nên lo lắng mỗi khi điện thoại có thông báo.

Thầy T. nhận ra có chuyện khi một học sinh vốn rất vui vẻ bỗng trở nên lặng lẽ và tránh cả giờ ra chơi, trong khi mỗi lần thầy hỏi thì em chỉ bảo là không sao, và mãi sau thầy mới biết cả lớp đã đặt cho em một biệt danh để chế giễu rồi còn lập thêm một nhóm riêng chỉ để nói về em. Điều làm thầy day dứt nhất là trong cái nhóm ấy có một học sinh mà chỉ học kỳ trước thôi chính em cũng từng bị cả lớp trêu chọc, thế nhưng khi thầy hỏi thì em lại nói rằng em chỉ vào cho vui thôi vì ai cũng làm như vậy.

Vì sao việc chia sẻ lại nội dung xâm hại cũng làm gia tăng tổn thương?

Định nghĩa: Lan truyền và tiếp tay là việc chia sẻ, chuyển tiếp, bình luận, chụp lại hoặc lưu giữ những nội dung đang gây tổn thương cho một đứa trẻ, dù người thực hiện không phải là người tạo ra nội dung ban đầu. Mỗi hành động nhỏ đều góp phần kéo dài thời gian tồn tại và mở rộng phạm vi tiếp cận của nội dung.

Dấu hiệu thường gặp: Người chia sẻ lại thường cho rằng mình chỉ chuyển tiếp một nội dung đã có sẵn, gửi cho một vài người bạn hoặc tham gia vì cả nhóm đều đang làm như vậy. Trong các nhóm chat, một hình ảnh hoặc lời chế giễu có thể được gửi đi rất nhanh vì mỗi người đều cảm thấy phần trách nhiệm của mình quá nhỏ. Chính cảm giác vô can này khiến nội dung xâm hại tiếp tục lan rộng mà không ai chủ động dừng lại.

Hậu quả: Mỗi lượt chia sẻ làm tăng số người chứng kiến, số bản sao và khả năng nội dung tiếp tục xuất hiện trong tương lai. Trẻ bị nhắm đến phải đối mặt với sự chú ý và phán xét từ ngày càng nhiều người, ngay cả khi người đăng ban đầu đã dừng lại. Vì vậy, người chuyển tiếp, bình luận hoặc hưởng ứng cũng trở thành một mắt xích trong chuỗi gây hại và có trách nhiệm đối với hậu quả mà nội dung ấy gây ra.

Khoa thấy một tấm ảnh chế bạn lớp bên nhìn khá buồn cười nên gửi lại vào nhóm bạn, và lúc ấy em chỉ nghĩ đơn giản rằng mình đang chia sẻ lại một tấm ảnh vốn đã có sẵn, để rồi vài hôm sau em nghe tin bạn ấy phải nghỉ học và gia đình phải lên gặp nhà trường. Khoa kể lại rằng trước đây em vẫn nghĩ người có lỗi chỉ là người đăng đầu tiên, nhưng dần dần em hiểu ra rằng mỗi người bấm nút chia sẻ đều đã góp một phần vào quãng đường mà tấm ảnh ấy đi qua.

Trí tuệ nhân tạo đang bị lợi dụng để tạo nội dung xâm hại trẻ em như thế nào?

Định nghĩa: Đây là hành vi sử dụng trí tuệ nhân tạo để tạo mới hoặc chỉnh sửa hình ảnh, video giả mạo có liên quan đến một đứa trẻ nhằm bôi nhọ, đe dọa hoặc tống tiền em. Kẻ xâm hại có thể lấy khuôn mặt của trẻ từ những hình ảnh công khai rồi ghép vào nội dung giả, vì vậy trẻ vẫn có thể trở thành nạn nhân dù chưa từng gửi bất kỳ hình ảnh riêng tư nào.

Dấu hiệu thường gặp: Kẻ xâm hại có thể thu thập ảnh từ trang cá nhân của trẻ hoặc phụ huynh, đặc biệt là những tài khoản công khai có nhiều ảnh rõ khuôn mặt. Nội dung giả sau đó được gửi trực tiếp cho trẻ để đe dọa hoặc phát tán trong nhóm chat nhằm khiến người khác tin rằng đó là hình ảnh thật. Công nghệ ngày càng dễ sử dụng khiến việc tạo nội dung giả mạo không còn đòi hỏi nhiều kỹ năng hoặc thời gian như trước.

Năm 2026, UNICEF, ECPAT International và INTERPOL công bố kết quả nghiên cứu tại 11 quốc gia, cho thấy trong vòng một năm, ít nhất 1,2 triệu trẻ em cho biết hình ảnh của mình đã bị biến đổi thành hình deepfake mang tính chất tình dục.

Hậu quả: Nội dung giả mạo có thể lan truyền nhanh và rất khó thu hồi hoàn toàn. Trẻ có thể bị chế giễu, nghi ngờ hoặc buộc phải giải thích về một nội dung mà mình chưa từng tạo ra. Việc nội dung là giả không làm giảm mức độ tổn thương, bởi phản ứng của bạn bè và cộng đồng vẫn có thể ảnh hưởng trực tiếp đến danh dự, các mối quan hệ và cảm giác an toàn của trẻ.

PHẦN III

**DẤU HIỆU NHẬN BIẾT VÀ LÝ DO TRẺ EM GIỮ IM
LẶNG**

Người lớn cần chú ý những dấu hiệu nào?

Vì trẻ em rất ít khi chủ động nói ra nên người lớn thường phải nhận biết thông qua hành vi, và những thay đổi được nêu dưới đây không nhằm để kết luận bất cứ điều gì mà chỉ để tham khảo, bởi mỗi dấu hiệu riêng lẻ đều có thể xuất phát từ một nguyên nhân hoàn toàn khác.

Về mặt cảm xúc và sinh hoạt, đứa trẻ có thể thay đổi rõ rệt về giấc ngủ hoặc ăn uống sau mỗi lần sử dụng thiết bị, tỏ ra lo lắng bất thường mỗi khi điện thoại có thông báo, hoặc đột ngột né tránh trường lớp cùng bạn bè và những hoạt động mà trước đây em vốn rất yêu thích.

Về mặt sử dụng thiết bị, đứa trẻ có thể giấu màn hình và đổi tư thế ngồi mỗi khi có người lại gần, đột ngột ngừng sử dụng một nền tảng mà trước đó em vẫn dùng hằng ngày, hoặc sở hữu những tài khoản và ứng dụng mà gia đình hoàn toàn không hay biết.

Về mặt quan hệ, đứa trẻ có thể nhắc đến một người bạn trên mạng lớn tuổi hơn nhưng lại ngại nói chi tiết về người ấy, hoặc bỗng nhiên nhận được quà, tiền, thẻ nạp và vật phẩm trò chơi mà em không giải thích được nguồn gốc.

Khi nhiều dấu hiệu cùng xuất hiện trong một khoảng thời gian ngắn thì đó là lúc gia đình nên chủ động trò chuyện với trẻ, và cách mở lời sao cho trẻ chịu chia sẻ sẽ được bàn ở phần ngay sau đây.

Vì sao trẻ em bị xâm hại thường không kể với cha mẹ hay thầy cô?

Dữ liệu mới của UNICEF cho thấy tại Việt Nam, 58,6% các trường hợp xâm hại tình dục trẻ em có yếu tố công nghệ được ghi nhận trong nghiên cứu không được trẻ chia sẻ với bất kỳ ai. Trên 21 quốc gia được khảo sát, chưa đến 1% trường hợp được báo cáo với cơ quan chức năng. Nghiên cứu Disrupting Harm cũng đã hỏi trực tiếp trẻ em về điều này và tổng hợp được ba lý do phổ biến nhất, trong đó cả ba đều nói về người lớn nhiều hơn là nói về bản thân các em.⁴

Lý do được nêu nhiều nhất là các em tin rằng việc kể ra sẽ chẳng thay đổi được gì, bởi nhiều em cho rằng sự việc chưa đủ nghiêm trọng để làm phiền ai hoặc cho rằng người lớn dù có biết thì cũng không làm được gì, và điều này phản ánh khá trực tiếp mức độ tin tưởng của trẻ vào khả năng can thiệp của chúng ta.

Lý do thứ hai là các em lo sợ chính mình sẽ gặp rắc rối, bởi đứa trẻ đã tự tay gửi tấm ảnh và đã tự mình trò chuyện với người lạ, nên khi hình dung ra cảnh bị mắng rồi bị thu điện thoại và bị cấm dùng mạng thì với nhiều em, viễn cảnh ấy còn đáng sợ hơn cả việc tiếp tục âm thầm chịu đựng.

Lý do thứ ba là các em không biết cần đi đâu và nói với ai, bởi em có nghe đến số 111 nhưng chưa từng gọi bao giờ, và em cũng biết mình có cô giáo chủ nhiệm nhưng lại không chắc rằng cô có hiểu được chuyện đang xảy ra bên trong một nhóm chat hay không.

Cả ba lý do này đều nói về người lớn chứ không nói về trẻ em, và điều đó cũng có nghĩa là người lớn hoàn toàn có thể thay đổi được cả ba nếu thực sự muốn.

⁴ Disrupting Harm in Viet Nam, 2022, tài liệu đã dẫn.

Nên mở lời với trẻ như thế nào khi nghi ngờ trẻ bị xâm hại?

Cuộc trò chuyện đầu tiên thường quyết định phần lớn những gì diễn ra sau đó, cho nên người lớn nên chọn một lúc yên tĩnh khi không có mặt anh chị em hay người ngoài, và nên bắt đầu bằng chính điều mà mình quan sát được thay vì bằng một câu hỏi mang tính truy vấn.

Một câu mở đầu như “Mấy hôm nay bố mẹ thấy con có vẻ mệt, có chuyện gì con muốn kể không?” thường mở ra được nhiều hơn hẳn so với câu “Con lại làm gì trên mạng đấy?”, bởi câu thứ nhất đặt người lớn vào vị trí của một người đang quan tâm trong khi câu thứ hai lại đặt đứa trẻ vào vị trí của người phải giải trình.

Trong lúc trẻ đang kể thì người lớn nên nghe cho hết rồi mới hỏi, và nếu trẻ dừng lại giữa chừng thì việc im lặng vài giây thường hiệu quả hơn nhiều so với một câu hỏi tiếp theo, đồng thời ngay từ đầu người lớn cũng nên nói rõ với trẻ một câu rất quan trọng, đó là chuyện này không phải lỗi của con.

PHẦN IV

**CÁC BƯỚC XỬ LÝ KHI TRẺ EM BỊ XÂM HẠI TRỰC
TUYÊN**

Dù có cách khởi đầu khác nhau, các hình thức xâm hại được trình bày ở phần trước đều cần được xử lý theo một trình tự tương đối giống nhau trong những giờ đầu tiên. Phần này hướng dẫn năm bước cần thực hiện, đồng thời làm rõ cách người lớn nên lắng nghe và tiếp nhận lời kể của trẻ.

Việc thực hiện đúng thứ tự có ý nghĩa đặc biệt quan trọng. Khi biết chuyện, người lớn thường muốn lập tức báo cáo hoặc tìm người can thiệp, trong khi nguy cơ đối với trẻ có thể vẫn đang tiếp diễn và những bằng chứng quan trọng có thể bị xóa hoặc thất lạc. Vì vậy, cần ưu tiên bảo đảm an toàn cho trẻ, tiếp đó lưu giữ bằng chứng, rồi mới tiến hành báo cáo và tìm kiếm sự hỗ trợ phù hợp.

Bước thứ nhất — Dừng lại và cắt nguồn gây hại

Việc đầu tiên cần làm là chấm dứt cuộc trò chuyện đang gây tổn thương. Trẻ không nên trả lời thêm, gửi thêm hình ảnh, cung cấp thêm thông tin, chuyển tiền hoặc tiếp tục làm theo bất kỳ yêu cầu nào của kẻ xâm hại.

Đây thường là bước khó nhất, bởi trẻ có thể tin rằng chỉ cần đáp ứng thêm một lần thì mọi chuyện sẽ kết thúc. Trên thực tế, mỗi lần trẻ làm theo chỉ khiến kẻ xâm hại biết rằng cách đe dọa của mình đang có hiệu quả và tiếp tục đưa ra những yêu cầu lớn hơn.

Một cách đơn giản để nhận biết yêu cầu bất thường là tự hỏi: “Mình có được phép dừng lại để hỏi ý kiến một người lớn đáng tin cậy không?”. Một yêu cầu chính đáng sẽ không buộc trẻ phải quyết định ngay, giữ bí mật hoặc làm theo trong trạng thái sợ hãi.

Bước thứ hai — Không lan truyền nội dung xâm hại

Khi gặp chuyện, trẻ thường tìm đến bạn bè trước khi kể với người lớn. Các em có thể gửi ảnh chụp màn hình, chuyển tiếp tin nhắn hoặc chia sẻ nội dung đang gây tổn thương để hỏi ý kiến, tìm sự an ủi hoặc nhờ bạn xác nhận rằng sự việc là nghiêm trọng.

Người bạn nhận được nội dung nên lắng nghe, không bình luận, không chuyển tiếp và không đưa nội dung vào các nhóm chat khác. Điều cần làm là khuyên trẻ dừng liên lạc với kẻ xâm hại và tìm đến một người lớn đáng tin cậy. Nếu cần lưu bằng chứng, chỉ nên ghi lại những thông tin cần thiết theo hướng dẫn ở bước tiếp theo, thay vì tiếp tục phát tán chính nội dung xâm hại.

Nguyên tắc này cũng áp dụng với người lớn. Việc đăng công khai vụ việc lên mạng xã hội để lên án kẻ xâm hại có thể khiến danh tính của trẻ bị suy đoán hoặc lộ ra, kéo theo thêm những lời bình luận, phán xét và tò mò từ cộng đồng. Trong nhiều trường hợp, không chia sẻ lại chính là cách bảo vệ trẻ thiết thực nhất.

Bước thứ ba — Lưu giữ bằng chứng một cách an toàn

Khi có thể thực hiện mà không làm tăng nguy cơ cho trẻ, người hỗ trợ nên ghi lại tên tài khoản, đường dẫn, thời gian xảy ra sự việc và ảnh chụp màn hình những tin nhắn liên quan. Bằng chứng cần được giữ nguyên, không chỉnh sửa, cắt ghép hoặc thêm nội dung.

Phản ứng tự nhiên của nhiều trẻ và phụ huynh là xóa ngay mọi thứ để không phải nhìn thấy nữa. Tuy nhiên, khi bằng chứng đã bị xóa, việc yêu cầu nền tảng xác minh tài khoản, gỡ nội dung hoặc đề nghị cơ quan chức năng can thiệp có thể trở nên khó khăn hơn.

An toàn của trẻ vẫn phải được đặt lên trước. Nếu việc thu thập bằng chứng buộc trẻ phải tiếp tục trả lời, thương lượng hoặc duy trì liên lạc với kẻ xâm hại, gia đình nên dừng lại và chuyển sang bước báo cáo.

Riêng với những nội dung có dấu hiệu xâm hại tình dục trẻ em thì cách làm phải khác đi, bởi người phát hiện tuyệt đối không được tải xuống, không chuyển tiếp và không lưu giữ loại nội dung này kể cả với mục đích làm bằng chứng, do việc lưu giữ có thể tạo ra rủi ro pháp lý cho chính người lưu. Trong trường hợp ấy thì người phát hiện chỉ nên ghi lại thật ngắn gọn đường dẫn cùng tên tài khoản và thời gian, rồi báo ngay cho Tổng đài 111 hoặc cơ quan công an để nơi có thẩm quyền xử lý.

Bước thứ tư — Báo cáo vi phạm trên nền tảng

Người hỗ trợ nên báo cáo ngay tài khoản và nội dung vi phạm trên chính nền tảng nơi sự việc xảy ra. Đây thường là cách nhanh nhất để yêu cầu hạn chế tài khoản, ngăn nội dung tiếp tục lan truyền hoặc gỡ nội dung khỏi nền tảng.

Khi báo cáo, cần cung cấp đường dẫn cụ thể và những thông tin cần thiết để nền tảng xác định đúng tài khoản hoặc nội dung. Sau đó, tùy theo tính chất của vụ việc, gia đình có thể báo thêm với nhà trường, Tổng đài 111 hoặc cơ quan công an.

Người báo tin không cần tự quyết định vụ việc đã đủ nghiêm trọng hay chưa. Việc xác minh và phân loại thuộc trách nhiệm của cơ quan hoặc đơn vị tiếp nhận.

Bước thứ năm — Đưa người lớn tin cậy vào cuộc

Trẻ không nên tự mình xử lý một tình huống có yếu tố đe dọa, ép buộc, tổn tiền hoặc xâm hại tình dục. Các em cần báo cho một người lớn đáng tin cậy càng sớm càng tốt.

Người đó có thể là cha mẹ, ông bà, anh chị đã trưởng thành, giáo viên chủ nhiệm, cán bộ tư vấn học đường hoặc nhân viên Tổng đài 111. Điều quan trọng không nằm ở chức danh của người ấy mà ở khả năng lắng nghe, giữ bình tĩnh và không đổ lỗi cho trẻ.

Khi một đứa trẻ kể ra, người lớn mới có thể nhìn thấy sự việc, ngăn nguy cơ tiếp diễn và đưa sự hỗ trợ đến với em.

Khi nào cần báo cơ quan công an?

Gia đình nên báo cơ quan công an khi trẻ bị đe dọa, ép buộc hoặc khống chế bằng hình ảnh, thông tin hay bí mật cá nhân; khi kẻ xâm hại yêu cầu chuyển tiền hoặc tài sản; khi vụ việc có dấu hiệu xâm hại tình dục, kể cả mới dừng ở việc yêu cầu trẻ gửi hình ảnh; hoặc khi có người đe nghị, dụ dỗ hay ép trẻ gặp mặt ngoài đời thực.

Gia đình nên báo sớm ngay cả khi chưa xác định rõ mức độ nghiêm trọng. Cơ quan chức năng có trách nhiệm đánh giá vụ việc, trong khi việc chậm báo có thể khiến bằng chứng bị mất hoặc kẻ xâm hại tiếp tục tiếp cận trẻ.

Người lớn nên nói gì trong lần đầu tiên trẻ kể chuyện?

Câu đầu tiên trẻ cần được nghe là: “Chuyện này không phải lỗi của con.” Nhiều trẻ im lặng vì tin rằng chính mình đã gây ra sự việc, nhất là khi các em từng chủ động trò chuyện, gửi hình ảnh hoặc làm theo một yêu cầu nào đó.

Người lớn nên để trẻ kể hết trước khi đặt câu hỏi. Tránh hỏi dồn, trách móc hoặc yêu cầu trẻ kể lại nhiều lần. Chỉ nên hỏi những thông tin thực sự cần thiết để bảo đảm an toàn và xác định bước xử lý tiếp theo.

Sau khi lắng nghe, người lớn cần nói rõ mình sẽ làm gì, chẳng hạn lưu lại bằng chứng, báo cáo nền tảng, liên hệ nhà trường hoặc tìm sự hỗ trợ từ cơ quan chức năng. Khi biết trước điều sắp xảy ra, trẻ sẽ bớt lo sợ và cảm thấy mình vẫn được tham gia vào quá trình xử lý.

Có nên hứa giữ bí mật tuyệt đối với trẻ không?

Người lớn không nên hứa giữ bí mật tuyệt đối nếu vụ việc cần được chia sẻ để bảo vệ trẻ. Khi lời hứa bị phá vỡ, trẻ có thể cảm thấy bị phản bội và không còn muốn tìm kiếm sự giúp đỡ trong những lần sau.

Cách phù hợp hơn là nói rõ rằng thông tin chỉ được chia sẻ với những người thực sự cần biết để bảo vệ em, chẳng hạn giáo viên phụ trách, cán bộ bảo vệ trẻ em, Tổng đài 111 hoặc cơ quan công an. Thông tin không nên được kể lại cho họ hàng, hàng xóm, bạn bè hoặc những người không có vai trò xử lý vụ việc.

Có nên thu điện thoại của trẻ sau khi sự việc xảy ra không?

Thu điện thoại không nên là phản ứng đầu tiên. Với trẻ, thiết bị không chỉ là nơi xảy ra sự việc mà còn là phương tiện liên lạc với bạn bè, học tập và tìm kiếm sự hỗ trợ. Việc tước điện thoại ngay sau khi trẻ kể chuyện dễ khiến em cảm thấy mình đang bị phạt vì đã lên tiếng.

Trong một số trường hợp, việc tạm ngừng sử dụng một ứng dụng, khóa tài khoản hoặc hạn chế liên lạc là cần thiết để ngăn kẻ xâm hại tiếp tục tiếp cận. Tuy nhiên, quyết định này nên được giải thích rõ và thực hiện cùng với trẻ, thay vì áp dụng như một hình thức kỷ luật.

Thu điện thoại ngay khi trẻ vừa kể chuyện có thể khiến cánh cửa giao tiếp vừa mở ra lập tức khép lại.

PHẦN V

**TRÁCH NHIỆM CỦA GIA ĐÌNH, NHÀ TRƯỜNG VÀ
CÁC BÊN LIÊN QUAN**

Việc bảo vệ trẻ em trên không gian mạng cần có sự tham gia của nhiều bên. Gia đình không thể kiểm soát hoạt động của nền tảng; nhà trường khó theo sát trẻ sau giờ học; nền tảng không phải lúc nào cũng nhìn thấy những gì diễn ra trong các nhóm kín; còn cơ quan chức năng chỉ có thể can thiệp khi nhận được thông tin. Mỗi bên vì vậy cần thực hiện đúng phần trách nhiệm của mình và phối hợp khi sự việc xảy ra.

Trẻ em, thanh thiếu niên

Điều quan trọng nhất là nhận ra sớm dấu hiệu bất thường và tìm người hỗ trợ. Trẻ cần đặc biệt cảnh giác khi có người yêu cầu giữ bí mật với cha mẹ, đề nghị chuyển cuộc trò chuyện sang một ứng dụng riêng tư hơn hoặc tạo cảm giác gấp gáp để buộc các em phải hành động ngay.

Bên cạnh việc tự bảo vệ, trẻ cũng cần tránh trở thành một mắt xích trong chuỗi gây hại. Các em không nên chia sẻ lại nội dung làm tổn thương người khác, hòa theo những lời chế giễu trong nhóm hoặc dùng công nghệ để trêu chọc, làm nhục và cô lập bạn bè. Trong nhiều vụ bắt nạt trực tuyến, chính những người chứng kiến và bạn cùng lớp là những người quyết định sự việc sẽ dừng lại hay tiếp tục lan rộng.

Về mặt kỹ thuật, trẻ nên khai đúng độ tuổi khi tạo tài khoản, bật chế độ riêng tư và xác thực hai bước. Khi báo cáo nội dung vi phạm, các em nên cung cấp đường dẫn cụ thể để nền tảng xác định và xử lý nội dung nhanh hơn.

Cha mẹ và người chăm sóc

Nghiên cứu Disrupting Harm cho thấy có 77% người chăm sóc được khảo sát sử dụng internet hằng ngày trong khi chỉ 17% thường xuyên hướng dẫn con cách dùng mạng an toàn, nghĩa là người lớn đang có mặt trên cùng một không gian với trẻ nhưng lại ít khi thực sự tham gia vào trải nghiệm của các em.⁵

Gia đình có thể bắt đầu bằng việc cùng trẻ tạo tài khoản đúng độ tuổi, bật xác thực hai bước và rà soát các cài đặt riêng tư. Đây nên là hoạt động được thực hiện cùng trẻ để giải thích và hướng dẫn, thay vì làm thay hoặc biến thành một cuộc kiểm tra.

Cha mẹ cũng cần trò chuyện về những người bạn trên mạng của con bằng thái độ quan tâm, không tra xét. Những câu hỏi như con thường chơi với ai, người bạn ấy bao nhiêu tuổi hoặc hai người thường nói chuyện gì có thể giúp cha mẹ hiểu hơn về các mối quan hệ của trẻ mà không khiến các em cảm thấy bị theo dõi.

Các cuộc trò chuyện cũng cần diễn ra theo cả hai chiều: trẻ có đang bị ai làm phiền không và trẻ có đang tham gia làm phiền người khác không. Phần lớn gia đình chỉ chú ý đến nguy cơ con trở thành nạn nhân mà bỏ qua khả năng trẻ có thể hòa theo, chia sẻ lại hoặc trực tiếp thực hiện hành vi gây tổn thương.

⁵ Disrupting Harm in Viet Nam, 2022, tài liệu đã dẫn.

Đăng ảnh con lên mạng xã hội có làm tăng nguy cơ cho trẻ không?

Đây là câu hỏi ngày càng được đặt ra nhiều hơn kể từ khi công nghệ giả mạo hình ảnh trở nên phổ biến, và câu trả lời không phải là ngừng đăng ảnh mà là cân nhắc kỹ hơn về loại ảnh được đưa lên cùng chế độ hiển thị của chúng.

Nguy cơ này đã xuất hiện ở quy mô lớn. Năm 2026, UNICEF, ECPAT International và INTERPOL công bố kết quả nghiên cứu tại 11 quốc gia, cho thấy trong vòng một năm, ít nhất 1,2 triệu trẻ em cho biết hình ảnh của mình đã bị biến đổi thành hình deepfake mang tính chất tình dục. Vì vậy, việc cân nhắc kỹ số lượng, loại hình ảnh và mức độ công khai thông tin của trẻ là cần thiết để giảm rủi ro bị lợi dụng.

Gia đình nên hạn chế đăng công khai những tấm ảnh rõ mặt ở nhiều góc độ, ảnh mặc đồng phục có in tên trường, ảnh chụp trước cổng nhà hoặc cổng trường, cùng những thông tin cho phép người ngoài đoán được lịch sinh hoạt hằng ngày của con.

Nhà trường và giáo viên cần chuẩn bị những gì?

Nhà trường cần chuẩn bị cả hoạt động phòng ngừa lẫn quy trình xử lý. Nội dung giáo dục về an toàn trên không gian mạng nên được lồng ghép thường xuyên vào giờ sinh hoạt lớp, thay vì chỉ xuất hiện trong một buổi ngoại khóa mỗi năm.

Nhà trường cũng cần có quy trình tiếp nhận rõ ràng để học sinh biết mình có thể tìm đến ai, người tiếp nhận biết cần thực hiện những bước nào và thông tin của trẻ được bảo mật trong suốt quá trình xử lý.

Khi vụ việc xảy ra, nhà trường không nên nêu tên học sinh trước lớp, tổ chức đối chất công khai hoặc yêu cầu trẻ kể lại sự việc nhiều lần trước nhiều người. Đồng thời, nhà trường cần chuẩn bị phương án giúp trẻ trở lại lớp học, khôi phục các mối quan hệ và tránh tiếp tục bị cô lập sau khi sự việc đã được xử lý.

Doanh nghiệp và nền tảng số phải làm gì để bảo vệ trẻ em?

Từ ngày 01/7/2026, khoản 3 Điều 16 Luật An ninh mạng số 116/2025/QH15 quy định doanh nghiệp cung cấp dịch vụ trên không gian mạng có trách nhiệm triển khai biện pháp kỹ thuật và biện pháp quản lý cần thiết để phát hiện, ngăn chặn và gỡ bỏ kịp thời thông tin có nội dung xâm hại trẻ em, đồng thời phải thiết lập cơ chế và công cụ thuận tiện để người sử dụng phản ánh, tố giác.⁶

Theo thực tiễn quốc tế, nền tảng cần đặt chế độ an toàn và riêng tư làm mặc định cho tài khoản trẻ em; hạn chế khả năng người lạ chủ động liên hệ; áp dụng biện pháp xác định độ tuổi hiệu quả; cung cấp công cụ báo cáo dễ tìm, dễ sử dụng; thông báo kết quả xử lý cho người báo cáo; đồng thời nhận diện hoặc gắn nhãn phù hợp đối với nội dung do trí tuệ nhân tạo tạo ra.

Việc phản hồi kết quả báo cáo có ý nghĩa đặc biệt quan trọng. Nhiều trẻ không báo cáo vì cho rằng hành động ấy sẽ không tạo ra thay đổi nào. Một thông báo ngắn cho biết nội dung đã được tiếp nhận, gỡ bỏ hay chưa đủ căn cứ xử lý có thể giúp trẻ tin tưởng hơn vào cơ chế bảo vệ của nền tảng.

⁶ Quốc hội, Luật An ninh mạng số 116/2025/QH15, khoản 3 Điều 16 và khoản 2 Điều 25, có hiệu lực từ ngày 01/7/2026.

Cơ quan báo chí và người có ảnh hưởng cần đưa tin, lên tiếng như thế nào?

Cách một vụ việc được đưa tin có thể ảnh hưởng trực tiếp đến những tổn thương mà trẻ phải chịu đựng về sau. Cơ quan báo chí và người đưa tin không nên đăng lại nội dung gây hại, mô tả chi tiết hành vi hoặc công bố tên trường, lớp, địa phương và những đặc điểm có thể khiến người đọc suy đoán được danh tính của trẻ.

Đối với người có ảnh hưởng trên mạng xã hội, phạm vi tiếp cận lớn đi kèm với trách nhiệm hạn chế tổn thương. Một lời kêu gọi mang tính kích động có thể khiến hàng nghìn người truy tìm danh tính của trẻ, liên hệ với gia đình hoặc tiếp tục phát tán nội dung liên quan. Khi lên tiếng, người có ảnh hưởng nên hướng công chúng đến các kênh báo cáo và hỗ trợ chính thức, thay vì thúc đẩy việc truy tìm, phán xét hoặc xử lý vụ việc trên mạng.

PHẦN VI

ĐỊA CHỈ HỖ TRỢ VÀ CĂN CỨ PHÁP LÝ

Tổng đài quốc gia bảo vệ trẻ em 111

Tổng đài quốc gia bảo vệ trẻ em 111 là đầu mối tiếp nhận chính thức của Việt Nam do Cục Bà mẹ và Trẻ em thuộc Bộ Y tế quản lý, hoạt động hoàn toàn miễn phí suốt hai mươi tư giờ mỗi ngày và tất cả các ngày trong tuần.

Tổng đài tiếp nhận thông tin, tư vấn và kết nối can thiệp cho mọi vụ việc liên quan đến trẻ em trong đó có cả những vụ việc xảy ra trên môi trường mạng, và người gọi đến có thể là chính trẻ em, là cha mẹ, là thầy cô hay bất kỳ ai tình cờ phát hiện ra sự việc.

Trong nhiều trường hợp thì việc gọi tổng đài không nhằm mục đích tố giác ai cả mà chỉ đơn giản là để hỏi xem mình nên làm gì tiếp theo, và đây cũng chính là cách dùng phù hợp với những gia đình còn đang phân vân chưa biết sự việc đã đủ nghiêm trọng hay chưa.

TỔNG ĐÀI QUỐC GIA BẢO VỆ TRẺ EM

111

Miễn phí, hoạt động 24 giờ mỗi ngày

Các đầu mối hỗ trợ khác

Khi cần tư vấn hoặc khi trẻ đang bị đe dọa và cần được bảo vệ thì ngoài Tổng đài 111, gia đình có thể tìm đến nhà trường cùng cán bộ bảo vệ trẻ em cấp xã, với lưu ý rằng trong mọi trường hợp đều phải ưu tiên an toàn của trẻ và giữ kín thông tin về em.

Khi gặp nội dung xâm hại, tài khoản quấy rối hoặc tài khoản giả mạo thì kênh phù hợp nhất chính là công cụ báo cáo của nền tảng, và nếu vụ việc có liên quan đến học sinh cùng trường thì nên báo thêm cho nhà trường sau khi đã lưu lại đường dẫn cùng ảnh chụp màn hình.

Khi xuất hiện dấu hiệu xâm hại tình dục, dụ dỗ, đòi tiền hoặc phát tán hình ảnh riêng tư thì đây là những vụ việc cần báo cơ quan công an, và trong lúc chờ xử lý thì gia đình tuyệt đối không tự thương lượng với người gây hại cũng như không xóa đi bất kỳ bằng chứng nào.

Khi trẻ đang khủng hoảng tâm lý hoặc có biểu hiện muốn tự làm hại bản thân thì gia đình cần liên hệ cơ sở y tế cùng chuyên gia tâm lý, gọi Tổng đài 111 hoặc gọi cấp cứu khi cần, và điều quan trọng nhất trong khoảng thời gian ấy là tuyệt đối không để trẻ ở lại một mình.

Căn cứ pháp lý hiện hành

Luật Trẻ em số 102/2016/QH13 hiện được hợp nhất tại Văn bản hợp nhất số 108/VBHN-VPQH ngày 27/8/2025 quy định tại Điều 54 về trách nhiệm bảo vệ trẻ em trên môi trường mạng, còn Nghị định số 56/2017/NĐ-CP quy định chi tiết trình tự hỗ trợ và can thiệp, với lưu ý rằng thẩm quyền đối với một số thủ tục đã được phân định lại theo Nghị định số 147/2025/NĐ-CP.

Luật An ninh mạng số 116/2025/QH15 có hiệu lực từ ngày 01/7/2026 và thay thế cả Luật An ninh mạng số 24/2018/QH14 lẫn Luật An toàn thông tin mạng số 86/2015/QH13, trong đó Điều 16 được dành riêng để quy định về phòng, chống xâm hại trẻ em trên không gian mạng.

Về dữ liệu cá nhân thì Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025 có hiệu lực từ ngày 01/01/2026 và dành Điều 24 cho việc bảo vệ dữ liệu cá nhân của trẻ em, nội dung này được quy định chi tiết tại Nghị định số 356/2025/NĐ-CP ngày 31/12/2025, văn bản thay cho Nghị định số 13/2023/NĐ-CP trước đây.

Bên cạnh đó còn có Nghị định số 147/2024/NĐ-CP về quản lý và cung cấp dịch vụ internet, Luật Giao dịch điện tử số 20/2023/QH15 với Điều 11 về giá trị chứng cứ của thông điệp dữ liệu, cùng Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng ban hành theo Quyết định số 88/QĐ-BTTTT ngày 21/01/2025.

Về định hướng chính sách thì Chương trình bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026–2030 là khung hiện hành cho toàn bộ các hoạt động trong lĩnh vực này.⁷

⁷ Thủ tướng Chính phủ, Quyết định số 468/QĐ-TTg ngày 23/3/2026 phê duyệt Chương trình bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026–2030.

LỜI KẾT

Cẩm nang mở đầu bằng câu chuyện về một người mẹ phải mất gần một tuần mới biết con mình đang bị xâm hại. Trong suốt bảy ngày ấy, đứa trẻ đã phải tự mình đối mặt với nỗi sợ hãi ngay trong chính ngôi nhà của mình. Toàn bộ nội dung của cẩm nang được xây dựng với mong muốn rút ngắn khoảng thời gian từ khi trẻ bị đe dọa, ép buộc hoặc xâm hại trên mạng đến khi em nhận được sự giúp đỡ.

Nhận biết dấu hiệu, lưu giữ bằng chứng, báo cáo vi phạm và tìm đúng nơi hỗ trợ đều là những kỹ năng cần thiết. Tuy nhiên, người lớn chỉ có thể thực hiện các bước này khi biết điều gì đang xảy ra với trẻ. Vì vậy, trẻ cần cảm thấy đủ an toàn để kể lại sự việc với cha mẹ, thầy cô hoặc một người lớn mà em tin tưởng.

Cảm giác an toàn ấy được hình thành từ cách người lớn ứng xử với trẻ mỗi ngày. Đó có thể là một lần cha mẹ giữ bình tĩnh khi con mắc lỗi, một cuộc trò chuyện bắt đầu bằng sự quan tâm thay vì tra hỏi, hay việc tôn trọng những điều riêng tư mà trẻ đã chia sẻ. Qua những điều tưởng như rất nhỏ, trẻ dần hiểu rằng khi bị đe dọa hoặc tổn thương, em có thể tìm đến người lớn mà không sợ bị mắng, bị trách mắng hay bị đổ lỗi.

Bảo vệ trẻ em trên không gian mạng vì thế bắt đầu từ chính mối quan hệ giữa trẻ và những người lớn xung quanh. Khi tin rằng mình sẽ được lắng nghe và bảo vệ, trẻ sẽ tìm kiếm sự giúp đỡ sớm hơn. Người lớn nhờ đó có thể kịp thời ngăn hành vi xâm hại tiếp diễn, xử lý những hậu quả đã xảy ra và giúp trẻ dần ổn định trở lại.

Kết nối — Không tổn thương

Kết nối — Không một mình.