

Doxing

Doxing (hay doxxing) là gì?

Doxing là khi ai đó đưa thông tin cá nhân, riêng tư của bạn lên mạng mà không hỏi ý kiến bạn. Thông tin này có thể bao gồm họ tên đầy đủ, địa chỉ nhà, số điện thoại, nơi làm việc hoặc thậm chí thông tin liên lạc của gia đình bạn. Họ thường khuyến khích người khác sử dụng thông tin này để hù dọa, quấy rối hoặc đe dọa bạn.

Nếu việc doxing được thực hiện cho hoặc thay mặt cho một quốc gia nước ngoài, thì đây là một hình thức can thiệp của nước ngoài. Chia sẻ công khai thông tin cá nhân, riêng tư có thể gây hại đến quyền riêng tư, bảo mật và sự an toàn của người khác.

Phải làm gì nếu bạn bị doxed

Nói với gia đình và bạn bè

Nếu bạn cảm thấy thoải mái, hãy cho gia đình và bạn bè biết chuyện gì đã xảy ra, họ cũng có thể là mục tiêu của kẻ xấu. Nói họ cài đặt hồ sơ mạng xã hội của họ ở chế độ riêng tư.

Báo cáo trên nền tảng / trang web / ứng dụng nơi đã xảy ra việc doxing

Sử dụng tính năng báo cáo trên trang web, ứng dụng hoặc nền tảng nơi đã xảy ra sự việc. [Hướng dẫn về mạng xã hội](#) của Netsafe có thông tin về cách thực hiện việc này.

Báo cáo cho Netsafe

Bạn có thể báo cáo nội dung có hại cho Netsafe: [Gửi yêu cầu – Netsafe](#). Netsafe cũng có thể cung cấp cho bạn sự hỗ trợ, lời khuyên và trợ giúp của chuyên gia về an toàn trực tuyến. Gửi email đến help@netsafe.org.nz hoặc nhắn tin 'Netsafe' đến số 4282 để được hỗ trợ.

Báo cáo với Cảnh sát

Nếu bạn đang gặp nguy hiểm, hãy gọi ngay cho Cảnh sát bằng cách gọi 111.

Nếu không phải là trường hợp khẩn cấp, bạn có thể liên hệ với Cảnh sát bằng cách:

- Sử dụng [biểu mẫu](#) trực tuyến 105
- Gọi [105](#) từ bất kỳ máy điện thoại di động hoặc cố định nào, dịch vụ này miễn phí và luôn sẵn sàng 24/7 trên toàn quốc.

Biểu mẫu 105 yêu cầu bạn cung cấp một số thông tin cá nhân để giúp Cảnh sát xử lý báo cáo của bạn và làm việc tiếp với bạn. Cảnh sát chỉ sử dụng thông tin này cho **các mục đích được cho phép**.

Báo cáo cho NZSIS

Nếu bạn nghi ngờ một quốc gia nước ngoài đứng sau hành vi doxing bạn, bạn có thể báo cáo điều này với NZSIS thông qua [biểu mẫu trực tuyến](#) an toàn của họ.

Bạn không cần phải cung cấp thông tin cá nhân như tên, số điện thoại hoặc thông tin liên lạc nếu bạn không muốn. Bạn cũng có thể điền vào biểu mẫu đó bằng ngôn ngữ của bạn. Tất cả thông tin bạn cung cấp đều **được bảo mật và bảo vệ**.

Nếu bạn muốn nói chuyện với nhân viên của NZSIS, bạn có thể gọi cho họ theo số [+64 4 472 6170](#) hoặc [0800 747 224](#).

Thông tin chia sẻ với Netsafe, Cảnh sát hoặc NZSIS khi báo cáo

Khi báo cáo, bạn nên đưa ra càng nhiều thông tin chi tiết càng tốt. Cố gắng chụp màn hình hoặc lưu lại một bản sao của:

- Thông tin cá nhân, riêng tư nào đã được chia sẻ hoặc đăng tải
- Hồ sơ người dùng hoặc tài khoản của người đã chia sẻ nó (ví dụ: tên người dùng của họ)
- Ngày và giờ thông tin đã được chia sẻ hoặc đăng tải
- Tên của trang web hoặc ứng dụng nơi sự việc đã xảy ra

Làm thế nào để bảo vệ bản thân không bị doxed

Giữ an toàn trực tuyến

Hãy xem [mục Giữ an toàn trực tuyến](#) để biết thêm thông tin.

Cẩn thận khi chia sẻ thông tin trực tuyến

Kiểm tra các cài đặt về quyền riêng tư trên phương tiện truyền thông xã hội và tài khoản trực tuyến của bạn. Cài đặt hồ sơ của bạn ở chế độ riêng tư sao cho chỉ những người bạn tin tưởng mới có thể xem thông tin của bạn.

Tìm kiếm thông tin về bạn trên web

Tìm kiếm tên và thông tin cá nhân của bạn để xem thông tin nào về bạn được công khai. Xóa mọi thông tin cá nhân và riêng tư mà người khác có thể sử dụng để gây hại cho bạn, chẳng hạn như địa chỉ của bạn.

Quản lý cài đặt vị trí và gắn thẻ địa lý trên thiết bị của bạn

Điện thoại thông minh và máy ảnh có thể nhúng dữ liệu vị trí vào hình ảnh bằng cách sử dụng cài đặt vị trí của bạn. Việc này có thể được sử dụng để tìm ra thông tin cá nhân của bạn, như thông tin về nhà riêng của bạn hoặc trường học của con bạn. Cách thức tắt gắn thẻ địa lý hoặc tắt cài đặt vị trí sẽ khác nhau tùy theo thiết bị, vì vậy hãy tìm kiếm trực tuyến bằng tên thiết bị của bạn để biết hướng dẫn cụ thể.