



Bảo vệ khu vực công chống lại mạng lưới tội phạm

Tờ thông tin

Tại IBAC, một phần công việc của chúng tôi là điều tra và ngăn chặn các mạng lưới tội phạm lợi dụng thành công các cơ quan công quyền ở Victoria.

IBAC là cơ quan của Victoria hoạt động độc lập nhằm chống tham nhũng và giám sát lực lượng cảnh sát. Chúng tôi luôn sẵn sàng để ngăn chặn và vạch trần tham nhũng trong khu vực công và hành vi sai trái của cảnh sát, với mục tiêu tổng thể là tăng cường tính liêm chính trong tiểu bang của chúng ta.

Một phần quan trọng trong công việc của chúng tôi là hành động chống lại mối đe dọa từ các nhóm tội phạm có tổ chức đang cố gắng phát triển mối quan hệ trong khu vực công. Họ làm điều này để truy cập thông tin hạn chế, làm giả hồ sơ hoặc gây ảnh hưởng đến các quyết định, mà có thể giúp họ tiến hành các hoạt động bất hợp pháp và giúp họ tránh bị phát hiện.

Nhận diện mạng lưới tội phạm

Mạng lưới tội phạm là nhóm gồm hai người trở lên cùng nhau gây ra các tội ác và vi phạm nghiêm trọng.

Các nhóm tội phạm có tổ chức này nhằm vào các nhân viên khu vực công và cố gắng xây dựng các mối quan hệ có thể giúp họ mở rộng các hoạt động bất hợp pháp và tránh bị cơ quan thực thi pháp luật phát hiện.

Nếu bạn làm việc trong khu vực công, bạn có thể là mục tiêu

Điều tra của chúng tôi cho thấy các nhóm tội phạm có tổ chức nhắm vào nhân viên khu vực công ở mọi cấp độ.

Cho dù bạn là nhân viên của hội đồng thành phố, nhân viên của bộ hay làm việc trong cơ quan thi hành pháp luật, bạn cần nhận thức được nguy cơ của mạng lưới tội phạm.

Việc trình báo mọi hoạt động đáng ngờ cho IBAC sẽ giúp chúng ta giữ cho khu vực công không bị tội phạm có tổ chức tấn công.

Các Câu hỏi Thường gặp

Hỏi: Điều gì khiến các tổ chức trong khu vực công dễ bị tấn công?

Đáp: Nếu tổ chức của bạn có quyền truy cập vào thông tin hoặc vật thể có thể có giá trị đối với các nhóm tội phạm có tổ chức thì bạn có thể trở thành mục tiêu.

Các tổ chức có nhiều khả năng trở thành mục tiêu nhất là những tổ chức có:

- quyền ra quyết định và quản lý, bao gồm các tổ chức giám sát các ngành an ninh, xây dựng, quy hoạch, rượu bia và cờ bạc

- truy cập vào thông tin nhạy cảm hoặc các chi tiết về thi hành pháp luật
- truy cập vào cơ sở dữ liệu lớn về nhận diện danh tính với thông tin nhận diện cá nhân có thể dẫn đến hành vi trộm cắp danh tính, đe dọa và tống tiền nhân chứng, hoặc có thể được bán cho các nhóm tội phạm khác
- kiểm soát tài sản hoặc hàng hóa có giá trị bán lại cao.

Hỏi: Bạn có thể bảo vệ tổ chức của mình khỏi mạng lưới tội phạm bằng cách nào?

Đáp:

1. Hãy ưu tiên việc bảo mật. Tiến hành đánh giá nguy cơ, thường xuyên thực hiện kiểm toán ngẫu nhiên và áp dụng các biện pháp bảo vệ thông tin có giá trị cao.
2. Xác định mối quan hệ với các nhóm tội phạm. Thực hiện chính sách cho người lao động khai báo các mối quan hệ; khiến việc này trở thành bắt buộc trong quá trình tuyển dụng và sử dụng lao động; và xác định hậu quả đối với việc không tuân thủ.
3. Thực hiện kiểm tra kỹ lưỡng trước khi tuyển dụng. Kiểm tra nhân viên dựa trên mức độ tiếp cận và độ nhạy cảm; thường xuyên giám sát các kiểm tra an ninh; và tăng cường kiểm tra các vị trí có khả năng tiếp cận cao hơn

Khi sử dụng các đại lý tuyển dụng bên thứ ba, hãy tuân thủ các quy trình mua sắm phù hợp và tiến hành thẩm định để đảm bảo họ tuân thủ các quy trình tuyển chọn dựa trên thành tích và có các nguyên tắc đạo đức nghề nghiệp.

Hỏi: Những dấu hiệu nào có thể cho thấy đồng nghiệp có liên quan đến tội phạm?

Đáp: Có một số dấu hiệu có thể cho thấy ai đó có liên quan đến tội phạm. Ví dụ: người đó có thể:

- thể hiện sự giàu có không giải thích được
- hỏi xin thông tin không phải là một phần trong công việc của họ
- tìm cách truy cập vào các hệ thống không phải là một phần trong công việc của họ
- làm thêm giờ hoặc giờ làm việc bất thường
- không nghỉ phép.

Hỏi: Bạn có thể tự bảo vệ mình khỏi mạng lưới tội phạm bằng cách nào?

Đáp:

1. Tránh mọi hành vi mạo hiểm có thể khiến cá nhân bạn bị mạng lưới tội phạm tấn công, bao gồm cả việc dính líu đến tài chính hoặc mắc nợ.
2. Hãy thận trọng khi sử dụng các nền tảng mạng xã hội vì tội phạm có thể nhắm vào bạn thông qua các kênh này. Không sử dụng mạng xã hội để truyền đạt thông tin nhạy cảm về tổ chức của bạn, không nhấp vào các tin nhắn hoặc liên kết đáng ngờ từ những người bạn không quen biết và hãy cảnh giác khi chấp nhận yêu cầu kết bạn từ những người bạn không quen biết.
3. Không cung cấp bất kỳ thông tin nào về vai trò, quy trình, hệ thống hoặc thông tin bạn nắm giữ liên quan đến việc làm của mình cho bất kỳ ai không làm việc tại tổ chức của bạn. Từ chối mọi đề nghị được trả tiền để cung cấp loại thông tin này cho bất kỳ ai.
4. Cân nhắc bất kỳ mối quan hệ nào đã có từ trước mà có thể khiến bạn rơi vào tình thế phải thỏa hiệp vì có chung lợi ích. Khai báo tất cả các xung đột lợi ích thực tế, tiềm ẩn hoặc cảm nhận được với chủ lao động của bạn.

Nghĩa vụ của bạn là giúp bảo vệ khu vực công chống lại tội phạm có tổ chức.

Nếu bạn làm việc trong khu vực công và:

- bạn được một người có liên quan đến một nhóm tội phạm có tổ chức tiếp cận
- hoặc nếu bạn có thông tin rằng một nhóm tội phạm có tổ chức có liên quan đến khu vực công

...bạn có thể trình báo vấn đề này một cách an toàn cho IBAC.



Điền vào mẫu đơn trực tuyến bảo mật để trình báo tại www.ibac.vic.gov.au



Nếu bạn gặp khó khăn khi truy cập mẫu đơn trực tuyến, hãy gọi cho chúng tôi theo số **1300 735 135** để được hỗ trợ thêm.



Nếu bạn cần trợ giúp về dịch thuật, hãy gọi Dịch vụ Phiên dịch và Thông dịch theo số **13 14 50** hoặc truy cập www.ibac.vic.gov.au/mylanguage

