

Cảnh báo hành vi gian lận thương mại công nghệ cao xuyên biên giới

17:16 22/05/2026

Đây là cảnh báo được nhiều chuyên gia an ninh mạng đưa ra tại Vietnam Security Summit 2026, với chủ đề “Bảo vệ tương lai số trong thế giới hậu lượng tử và AI”, diễn ra ngày 22/5 tại Hà Nội.

Cụ thể, các chuyên gia nhận định, trí tuệ nhân tạo (AI) không chỉ làm thay đổi phương thức tấn công mạng truyền thống, mà còn trở thành công cụ hỗ trợ các hành vi gian lận thương mại xuyên biên giới. Các đối tượng có thể sử dụng deepfake để giả mạo khuôn mặt, giọng nói doanh nghiệp, tạo website và ứng dụng giả giống thương hiệu thật nhằm lừa người dùng cung cấp thông tin tài khoản, thanh toán hoặc tải phần mềm chứa mã độc.

Phát biểu tại hội nghị, Thiếu tá Trần Trung Hiếu, Phó Giám đốc Trung tâm An ninh mạng quốc gia kiêm Giám đốc Trung tâm VNCERT cho rằng, tội phạm mạng đang chuyển dịch mạnh từ các hình thức phát tán mã độc thông thường sang khai thác AI để thực hiện hành vi lừa đảo, giả mạo thương hiệu và chiếm đoạt dữ liệu trên quy mô lớn.

Theo ông Hiếu, nhiều cuộc tấn công hiện không chỉ gây thiệt hại tài chính mà còn ảnh hưởng trực tiếp đến niềm tin của người tiêu dùng trong môi trường số.



Toàn cảnh sự kiện Vietnam Security Summit 2026. Ảnh: HB

Tại hội nghị, ban Tổ chức nhận định, AI đang tạo ra tác động kép đối với lĩnh vực an toàn thông tin. Một mặt, công nghệ này hỗ trợ phát hiện nguy cơ, tự động hóa giám sát và phân tích dữ liệu nhanh hơn. Tuy nhiên, ở chiều ngược lại, AI cũng bị lợi dụng để tạo ra các chiến dịch lừa đảo (phishing), giả mạo thương hiệu và lừa đảo trực tuyến với mức độ tinh vi cao hơn trước.

Ông Ivo Gajdica, Trưởng bộ phận Dịch vụ An ninh mạng (EmbedIT) cảnh báo, nhiều rủi ro hiện nay đến từ rò rỉ dữ liệu và các hình thức giả mạo nằm ngoài khả năng giám sát của đội ngũ an ninh nội bộ. Theo chuyên gia này, nhiều doanh nghiệp chỉ phát hiện sự cố khi dữ liệu đã bị phát tán hoặc thương hiệu bị lợi dụng để thực hiện hành vi lừa đảo.

Ở lĩnh vực tài chính - ngân hàng, áp lực bảo vệ dữ liệu và ngăn chặn gian lận số cũng gia tăng mạnh khi các tổ chức đẩy nhanh chuyển đổi số nhưng vẫn phải duy trì hoạt động liên tục và đáp ứng yêu cầu tuân thủ.

Các chuyên gia cũng cho rằng, mô hình phòng thủ truyền thống không còn đủ hiệu quả trước các cuộc tấn công ứng dụng AI và hình thức tấn công zero-day. Xu hướng mới hiện nay là chuyển sang các kiến trúc bảo mật chủ động như: Zero Trust, Cloud Detection & Response và hệ thống phát hiện giả mạo theo thời gian thực.

Tại sự kiện, nhiều doanh nghiệp công nghệ đã giới thiệu các giải pháp nhận diện deepfake, chống rò rỉ dữ liệu, phát hiện ứng dụng giả mạo và bảo mật AI nhằm hỗ trợ doanh nghiệp giảm nguy cơ gian lận thương mại trên môi trường số.

Tuấn Ngọc