

Bộ Công an cảnh báo nguy cơ đánh cắp dữ liệu cá nhân khi sử dụng ‘game lậu’

16:20 29/10/2026

Theo Cục An ninh mạng, Bộ Công an, việc sử dụng “game lậu” sẽ tiềm ẩn nguy cơ bị cài mã độc, đánh cắp mật khẩu, dữ liệu cá nhân, tài khoản trò chơi, mạng xã hội và thông tin tài chính. Thậm chí, một số ứng dụng có thể yêu cầu quyền truy cập không cần thiết, như: Đọc thông báo, danh bạ, tệp hoặc trợ năng, tạo điều kiện theo dõi và thu thập dữ liệu.

Cụ thể, theo Cục An ninh mạng, Bộ Công an, qua theo dõi nhiều nhóm Facebook liên quan đến “game lậu” đã thu hút hàng nghìn đến hàng chục nghìn thành viên, với tần suất đăng bài cao. Một số nhóm thường xuyên chia sẻ thông tin về trò chơi miễn phí, bản chỉnh sửa hoặc máy chủ ngoài hệ thống phát hành chính thức.

Cục An ninh mạng cho hay, “game lậu” thường được dùng để chỉ trò chơi bị sao chép, chỉnh sửa, phát hành trái phép hoặc máy chủ riêng chưa được đơn vị có quyền cho phép. Các nội dung quảng bá thường nhấn mạnh lợi ích như chơi miễn phí, tặng vật phẩm, mở tính năng VIP hoặc nạp ít nhận nhiều để thu hút người chơi.



Cơ quan Cảnh sát điều tra, Công an tỉnh Quảng Ninh khởi tố vụ án, khởi tố bị can đối với đối tượng làm giả game online. Ảnh: conganquangninh.gov.vn

Việc tải tệp APK, EXE hoặc phần mềm từ nguồn không rõ ràng tiềm ẩn nguy cơ bị cài mã độc, đánh cắp mật khẩu, dữ liệu cá nhân, tài khoản trò chơi, mạng xã hội và thông tin tài chính. Một số ứng dụng có thể yêu cầu quyền truy cập không cần thiết như: Đọc thông báo, danh bạ, tệp hoặc trợ năng, tạo điều kiện theo dõi và thu thập dữ liệu.

Bên cạnh đó, người chơi còn có thể mất tiền khi nạp vào máy chủ không minh bạch. Dịch vụ có thể đột ngột ngừng hoạt động, xóa nhân vật hoặc đóng kênh hỗ trợ mà không hoàn trả tiền. Khi thiếu thông tin về đơn vị vận hành và cơ chế giải quyết khiếu nại, việc yêu cầu bồi hoàn cũng gặp nhiều khó khăn.

Các đối tượng xấu có thể lợi dụng tâm lý thích chơi miễn phí, muốn lên cấp nhanh và nhận ưu đãi lớn để dẫn dụ người chơi truy cập website lạ, tham gia nhóm chat hoặc tải phần mềm bên ngoài kênh chính thức. Sau đó, chúng có thể yêu cầu tắt cảnh báo bảo mật, cấp quyền không cần thiết, đánh cắp thông tin đăng nhập hoặc lôi kéo nạp tiền vào các gói VIP, vật phẩm và chương trình đua top. Một số máy chủ có thể đóng cửa hoặc đổi tên, khiến người chơi khó xác định bên chịu trách nhiệm. Đây là những nguy cơ cần cảnh giác.

Cục An ninh mạng khuyến cáo, người dùng cần ưu tiên tải trò chơi từ cửa hàng ứng dụng và kênh phát hành chính thức; không mở tệp APK, EXE không rõ nguồn gốc, không tắt cảnh báo bảo mật hoặc cấp quyền truy cập bất thường.

Đồng thời, không sử dụng chung mật khẩu giữa nhiều dịch vụ, không cung cấp mã xác thực cho người khác và cân nhắc kỹ trước khi nạp tiền vào máy chủ không rõ đơn vị vận hành. Khi phát hiện dấu hiệu lừa đảo hoặc mã độc, cần ngừng giao dịch, bảo vệ tài khoản và thông báo cho cơ quan chức năng để được hướng dẫn xử lý.

Tuấn Ngọc