

Cảnh giác thủ đoạn lừa đảo trực tuyến gia tăng trong dịp nghỉ hè

15:27 30/05/2026

Lực lượng Công an tỉnh Lâm Đồng đề nghị phụ huynh tăng cường quản lý, hướng dẫn con em sử dụng internet an toàn; thường xuyên nhắc nhở học sinh nâng cao ý thức cảnh giác trước các thủ đoạn lừa đảo trên không gian mạng trong thời gian nghỉ hè.



Công an phường Xuân Trường - Đà Lạt tuyên truyền cho học sinh về các thủ đoạn lừa đảo trực tuyến. Ảnh: Nguyễn Luân

Bước vào kỳ nghỉ hè năm 2026, nhu cầu sử dụng internet, mạng xã hội và các nền tảng trực tuyến của học sinh, sinh viên tăng cao. Đây cũng là thời điểm các đối tượng lừa đảo trên không gian mạng đẩy mạnh hoạt động với nhiều phương thức, thủ đoạn ngày càng tinh vi nhằm chiếm đoạt tài sản và đánh cắp thông tin cá nhân.

Nhiều chiêu trò nhắm vào học sinh, thanh thiếu niên

Theo lực lượng Công an, thời gian gần đây xuất hiện nhiều hình thức lừa đảo trực tuyến nhắm vào học sinh, thanh thiếu niên thông qua mạng xã hội và các ứng dụng trực tuyến.

CẢNH BÁO CÁC THỦ ĐOẠN LỪA ĐẢO TRỰC TUYẾN NHẪM VÀO HỌC SINH TRONG DỊP HÈ

THỦ ĐOẠN LỪA ĐẢO PHỔ BIẾN	HƯỚNG DẪN PHÒNG CHỐNG CHO PHỤ HUYNH & HỌC SINH
1. TUYỂN CTV ONLINE "VIỆC NHẸ LƯƠNG CAO" Lưu ý: Không tin vào lời mời gọi kiếm tiền nhanh!	1. TĂNG CƯỜNG QUẢN LÝ VÀ NHẮC NHỞ CON EM
2. NHẬN QUÀ TẶNG MIỄN PHÍ, QUAY VÒNG TRÚNG THƯỞNG Lưu ý: Không chia sẻ thông tin cá nhân!	2. KHÔNG TRUY CẬP ĐƯỜNG LINK LẠ, KHÔNG TẢI ỨNG DỤNG LẠ
3. YÊU CẦU CUNG CẤP OTP, TÀI KHOẢN NGÂN HÀNG Lưu ý: Tuyệt đối không cung cấp OTP!	3. KHÔNG THAM GIA HỘI NHÓM KHÔNG RÕ NGUỒN GỐC
	4. KHI PHÁT HIỆN LỪA ĐẢO, LIÊN HỆ CÔNG AN PHƯỜNG Số điện thoại: 02633.593.381

BẢO VỆ TRẺ EM TRÊN KHÔNG GIAN MẠNG LÀ TRÁCH NHIỆM CỦA TOÀN XÃ HỘI.

CÔNG AN PHƯỜNG XUÂN TRƯỜNG - ĐÀ LẠT

Các thủ đoạn lừa đảo trực tuyến dịp hè. Ảnh: Nguyễn Luân

Một trong những thủ đoạn phổ biến là giả danh tuyển cộng tác viên online với những lời mời gọi hấp dẫn như “việc nhẹ lương cao”, “kiếm tiền tại nhà”, chỉ cần thực hiện các nhiệm vụ đơn giản như thả tim, xem video, bình luận hoặc chốt đơn hàng để nhận hoa hồng.

Ban đầu, các đối tượng thường chuyển cho nạn nhân một khoản tiền nhỏ để tạo lòng tin. Sau đó, chúng yêu cầu tiếp tục chuyển tiền nhằm “nâng cấp nhiệm vụ”, “gia tăng lợi nhuận” rồi chiếm đoạt toàn bộ số tiền đã giao dịch. Nhiều học sinh do thiếu kinh nghiệm và kỹ năng nhận diện rủi ro trên môi trường mạng đã trở thành nạn nhân của thủ đoạn này.

Bên cạnh đó, các đối tượng còn lợi dụng tâm lý yêu thích trò chơi trực tuyến của giới trẻ để thực hiện hành vi lừa đảo thông qua các chương trình tặng quà game miễn phí, cung cấp vật phẩm hiếm hoặc mời tham gia các cuộc thi bình chọn trực tuyến. Các đường link lạ được gửi kèm thường chứa mã độc nhằm đánh cắp tài khoản Facebook, Zalo, Gmail và nhiều tài khoản cá nhân khác.

Sau khi chiếm quyền sử dụng tài khoản mạng xã hội, các đối tượng tiếp tục giả danh chủ tài khoản để nhắn tin vay mượn tiền người thân, bạn bè hoặc thực hiện các hành vi vi phạm pháp luật khác.

Ngoài ra, tình trạng giả danh cơ quan chức năng, nhà mạng, trường học để gọi điện thông báo liên quan đến học bổng, tài khoản vi phạm hoặc yêu cầu xác minh thông tin cá nhân cũng đang diễn biến phức tạp. Thông qua đó, các đối tượng dụ dỗ nạn nhân cung cấp mã OTP, mật khẩu đăng nhập hoặc thông tin tài khoản ngân hàng nhằm chiếm đoạt tài sản.

Cảnh giác chiêu trò lừa đảo đặt phòng, du lịch trực tuyến

Mùa hè cũng là thời điểm nhu cầu du lịch, nghỉ dưỡng tăng mạnh. Lợi dụng điều này, các đối tượng lừa đảo đã lập website, fanpage giả mạo khách sạn, homestay, khu nghỉ dưỡng uy tín với hình ảnh bắt mắt, thông tin đầy đủ và quảng cáo rộng rãi trên mạng xã hội để tạo lòng tin.

Quá trình tư vấn thường được thực hiện rất chuyên nghiệp, từ báo giá, gửi hình ảnh phòng, xác nhận lịch lưu trú đến giới thiệu các chương trình ưu đãi hấp dẫn nhằm thúc đẩy khách hàng chuyển khoản đặt cọc hoặc thanh toán trước.

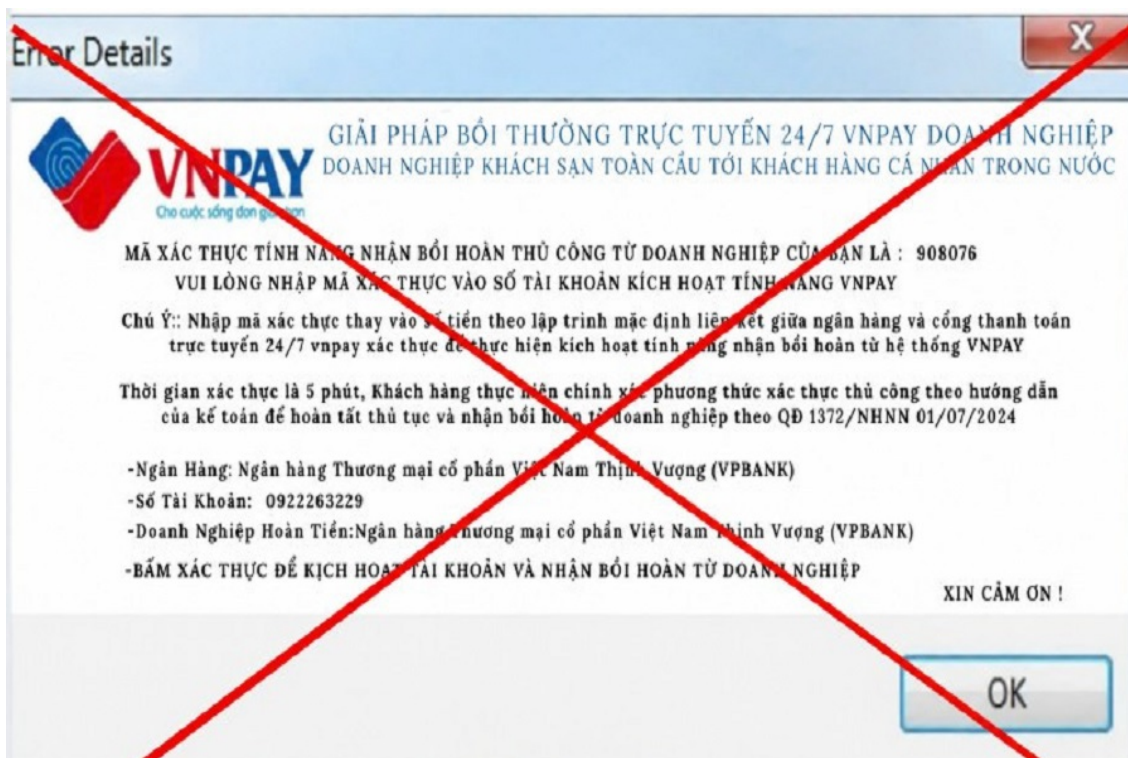
Sau khi nhận được tiền, các đối tượng tiếp tục thông báo giao dịch bị lỗi, sai nội dung chuyển khoản hoặc hệ thống chưa ghi nhận thanh toán, từ đó yêu cầu khách hàng chuyển tiền nhiều lần để được hoàn tiền hoặc xác nhận giao dịch.

Thậm chí, các đối tượng còn giả danh nhân viên chăm sóc khách hàng, kế toán hoặc bộ phận hỗ trợ thanh toán điện tử để tiếp tục dẫn dụ nạn nhân thực hiện thêm các giao dịch khác nhằm chiếm đoạt số tiền lớn hơn.

Đáng chú ý, các đối tượng thường tạo áp lực về thời gian, yêu cầu thao tác khẩn cấp trong vài phút khiến người dân mất bình tĩnh, chủ quan và dễ sập bẫy.

Tăng cường quản lý con em, chủ động phòng ngừa lừa đảo

Trước tình hình trên, lực lượng Công an khuyến cáo người dân cần nâng cao cảnh giác khi tham gia các hoạt động trên không gian mạng; tuyệt đối không cung cấp mã OTP, mật khẩu đăng nhập, thông tin tài khoản ngân hàng cho người lạ dưới bất kỳ hình thức nào.



Hình ảnh giả mạo thông báo hoàn tiền, kích hoạt “VNPay du lịch” do các đối tượng lừa đảo tạo dựng nhằm chiếm đoạt tài sản của người dân. Ảnh: Nguyễn Luân

Người dân không nên truy cập các đường link không rõ nguồn gốc, không tải các ứng dụng lạ và không tin vào những lời mời gọi kiếm tiền dễ dàng trên internet.

Đối với nhu cầu đặt phòng, du lịch trực tuyến, người dân nên ưu tiên sử dụng website chính thức, ứng dụng uy tín hoặc liên hệ trực tiếp với cơ sở lưu trú để xác minh thông tin trước khi chuyển tiền; tuyệt đối không chuyển khoản nhiều lần theo hướng dẫn của người lạ với các lý do như “kích hoạt hoàn tiền”, “mở khóa giao dịch” hay “xác minh tài khoản”.

Đặc biệt, lực lượng Công an đề nghị phụ huynh tăng cường quản lý, quan tâm và hướng dẫn con em sử dụng internet an toàn trong thời gian nghỉ hè; thường xuyên tuyên truyền, nhắc nhở học sinh nâng cao ý thức cảnh giác, kỹ năng nhận diện các thủ đoạn lừa đảo trên không gian mạng.

Khi phát hiện dấu hiệu nghi vấn liên quan đến hành vi lừa đảo trực tuyến, người dân cần nhanh chóng trình báo cơ quan Công an gần nhất để được hướng dẫn, hỗ trợ xử lý kịp thời, hạn chế thiệt hại về tài sản và thông tin cá nhân.

Hoàng Phương (t/h)