

Mua sắm cuối năm: Khẩu quyết "3 Không - 3 Nhanh" đối phó bẫy lừa đảo Deepfake

10:01 29/11/2025

Trong giai đoạn cao điểm mua sắm cuối năm, người tiêu dùng Việt Nam đối mặt với làn sóng tấn công của tội phạm mạng, sử dụng trí tuệ nhân tạo (AI) và Deepfake để giả mạo, chiếm đoạt tài sản. Tại tọa đàm của Hiệp hội An ninh mạng Quốc gia (NCA), các chuyên gia đã phát đi cảnh báo đỏ và đưa ra khẩu quyết "3 Không - 3 Nhanh" để người dân có thể tự trang bị "khiên 3 lớp" bảo vệ mình trên không gian mạng.



Giải pháp bảo vệ người dùng dựa trên mô hình "Khiên 3 lớp": Pháp lý - công nghệ - kỹ năng.

Ông Vũ Duy Hiền, Phó Tổng Thư ký NCA cho biết, tội phạm mạng đang hoạt động mạnh nhất, tận dụng triệt để AI và Deepfake. Các bẫy lừa thường bắt đầu từ những hành động nhỏ như một cú click hoặc một mã QR, có thể dẫn đến mất toàn bộ tài chính chỉ trong vài giây.

Có một nghịch lý là chưa bao giờ việc thanh toán lại tiện lợi đến vậy, nhưng tài sản lại dễ bị đánh cắp nhanh chóng. Các hình thức lừa đảo hiện nay nhắm vào tâm lý và cảm xúc, với những kịch bản tinh vi như:

Thao túng cảm xúc: Tội phạm sử dụng Deepfake để giả mạo gương mặt, giọng nói người thân hoặc mạo danh công an, shipper. Kẻ gian đọc vanh vách thông tin đơn hàng bị lộ lọt, khiến nạn nhân tin sái cổ và sập bẫy.

Đại diện MoMo tiết lộ, hình thức lừa phổ biến là dụ người dùng cài mã độc để chiếm quyền điều khiển thiết bị hoặc thao túng tâm lý khiến người dùng tự chuyển tiền.

Các chuyên gia đồng tình rằng, kỹ năng của người dùng là chốt chặn quan trọng nhất, vì an toàn không đến từ may mắn mà đến từ sự hiểu biết. Ông Vũ Ngọc Sơn (NCA) đã đưa ra khẩu quyết đơn giản, dễ nhớ để phòng chống lừa đảo, dựa trên mô hình chiến lược "Khiên 3 lớp" (Pháp lý - Công nghệ - Kỹ năng):

Ở nhóm "3 Không", người dùng phải từ bỏ sự tin tưởng tuyệt đối, ngay cả khi nhìn thấy video call mặt người thân, vì đó có thể là Deepfake. Tiếp theo, tuyệt đối không cài bất kỳ ứng dụng nào từ liên kết lạ, bởi hành động này đồng nghĩa với việc giao toàn bộ quyền kiểm soát điện thoại cho hacker. Cuối cùng, người dùng phải giữ vững "chốt chặn" cuối cùng là không chuyển tiền khi chưa xác thực, vì mọi kịch bản lừa đảo đều hướng đến bước này.

Ở nhóm "3 Nhanh", người dùng cần phải hành động nhanh chóng. Khi nhận thông tin đáng ngờ về trúng thưởng hay bị khóa tài khoản, phải nhanh tra cứu ngay qua các kênh chính thống. Nếu bị đối tượng đe dọa hoặc thao túng tâm lý qua điện thoại, hãy nhanh ngắt kết nối (vì công an không làm việc qua Zalo hay yêu cầu chuyển tiền). Cuối cùng, hãy nhanh báo cáo ngay cho cơ quan chức năng hoặc ngân hàng khi phát hiện bị lừa, tránh tự ý tìm kiếm các dịch vụ "lấy lại tiền lừa đảo" trên mạng vì đó lại là một cái bẫy thứ hai.

Về phía nền tảng, MoMo cho biết, họ áp dụng giải pháp kỹ thuật thời gian thực để phát hiện mã độc và dấu hiệu bất thường, thậm chí khóa chiều "cash-out" của tài khoản nghi ngờ để ngăn tẩu tán tài sản. Đại diện TikTok Shop cũng cho biết đã xóa 420.000 video có nội dung lừa đảo trong năm 2024, với 97% là do AI của nền tảng tự động phát hiện.

Bên cạnh đó, TS Phan Thế Thắng (Ủy ban Cạnh tranh Quốc gia) lưu ý, theo Luật Bảo vệ quyền lợi người tiêu dùng 2023, các KOLs và KOCs phải thông báo rõ ràng cho người tiêu dùng nếu nội dung quảng cáo được tài trợ, tránh cung cấp thông tin sai lệch gây nhầm lẫn.

Các chuyên gia đồng tình rằng, chỉ khi hành lang pháp lý đủ mạnh, công nghệ đủ thông minh và mỗi người dân tự trang bị cho mình "vaccine số" về kỹ năng, chúng ta mới có thể thực sự "an tâm mua sắm" trên không gian mạng và giảm thiểu thiệt hại từ tội phạm Deepfake.

Tâm An(t/h)