

Cảnh giác với thủ đoạn lừa đảo trực tuyến Quishing qua mã QR code

08:51 14/09/2025

Trong thời đại công nghệ số, mã QR ngày càng phổ biến trong thanh toán, đăng nhập dịch vụ hay tiếp cận thông tin. Tuy nhiên, điều này cũng đang bị tội phạm mạng lợi dụng để thực hiện hành vi lừa đảo.

Một cú quét mã QR tưởng chừng vô hại có thể trở thành “cánh cửa” để đối tượng đánh cắp dữ liệu cá nhân, chiếm quyền truy cập tài khoản ngân hàng và thậm chí chiếm đoạt tài sản. Thủ đoạn này được gọi là Quishing – viết tắt của “QR code phishing”, tức lừa đảo trực tuyến qua mã QR.



Cảnh giác với thủ đoạn lừa đảo trực tuyến Quishing qua mã QR code (ảnh minh họa)

Theo công an tỉnh Lào Cai, kịch bản Quishing thường diễn ra như sau: đối tượng tạo mã QR chứa đường link giả mạo, dẫn đến các trang web có giao diện giống hệt ngân hàng, ví điện tử, email hoặc dịch vụ trực tuyến. Sau đó, mã QR này được gắn vào email, tin nhắn, poster, tờ rơi hay bảng quảng cáo nơi công cộng.

Khi người dùng mất cảnh giác quét mã, họ sẽ bị điều hướng đến trang giả mạo và bị yêu cầu nhập thông tin cá nhân, mật khẩu, mã OTP. Ngay lập tức, dữ liệu rơi vào tay kẻ gian hoặc thiết bị của nạn nhân bị cài mã độc mà không hề hay biết.

Các chiêu thức Quishing phổ biến gồm: Dán đề mã QR giả tại bến xe, quán ăn, điểm thanh toán công cộng; Gửi mã QR kèm email, tin nhắn giả mạo ngân hàng, công ty vận chuyển, cơ quan nhà nước; Sử dụng trang trung gian để thu thập dữ liệu trước khi chuyển hướng sang trang web thật, khiến người dùng khó phát hiện.

Người dân cần cảnh giác trước các dấu hiệu đáng ngờ như: email, tin nhắn lạ thúc giục quét mã ngay lập tức; mã QR xuất hiện trên tờ rơi, bảng quảng cáo không rõ nguồn gốc; trang web sau khi quét yêu cầu đăng nhập tài khoản, cung cấp mật khẩu hay mã OTP.

Để phòng ngừa Quishing, cơ quan chức năng khuyến cáo: Người dùng không quét mã QR không rõ nguồn gốc, đặc biệt tại nơi công cộng có dấu hiệu dán chồng; Kiểm tra kỹ đường dẫn, chỉ truy cập các địa chỉ chính thức có giao thức bảo mật <https://>; Sử dụng ứng dụng quét QR uy tín có chức năng cảnh báo; Cập nhật phần mềm bảo mật thường xuyên; Bật xác thực hai lớp để bảo vệ tài khoản.

Cũng theo Công an tỉnh Lào Cai, mỗi cá nhân cần trở thành “người dùng thông minh”, tỉnh táo trước những cú quét mã QR tưởng chừng đơn giản. Trang bị kiến thức an toàn thông tin, thận trọng khi chia sẻ dữ liệu cá nhân và chủ động tuyên truyền cho người thân, bạn bè sẽ góp phần tạo dựng môi trường số an toàn, lành mạnh, ngăn chặn các thủ đoạn lừa đảo ngày càng tinh vi.

Hải Minh