Cách Nhận Biết Mã QR Có An Toàn Không Trước Khi Mở (Hướng Dẫn Chống Quishing)

Quishing là lừa đảo qua mã QR. Tìm hiểu các dấu hiệu nguy hiểm trước khi quét và những gì cần kiểm tra trước khi nhấn Mở.

Tác giả: Lubor Šimůnek · Ngày đăng: August 23, 2026 · Bảo mật

Phiên bản trực tuyến: https://appstoryo.com/vi/blog/qr-code-safe-quishing-guide



Quishing là gì?

Quishing là hình thức lừa đảo (phishing) sử dụng mã QR. Kẻ tấn công tạo ra một mã QR mà khi quét sẽ dẫn đến trang web độc hại được thiết kế để đánh cắp thông tin đăng nhập, cài đặt phần mềm độc hại hoặc hiển thị trang thanh toán giả. Thuật ngữ này kết hợp giữa 'QR' và 'phishing', và mối đe dọa này đang phát triển nhanh chóng vì mọi người thường tin tưởng mã QR mà không suy nghĩ.

Tại sao mã QR có rủi ro đặc biệt

Với liên kết thông thường, bạn có thể di chuột qua để xem URL trước khi nhấp. Nhưng với mã QR, bạn không thể thấy đích đến cho đến khi máy quét giải mã nó — và nhiều ứng dụng camera mở trình duyệt ngay lập tức mà không hiển thị địa chỉ. Khoảnh khắc đó đủ để trang web độc hại bắt đầu theo dõi thiết bị của bạn.

Mã QR cũng hoàn toàn vượt qua bộ lọc thư rác: bộ lọc tìm kiếm văn bản đáng ngờ hoặc URL độc hại đã biết, nhưng hình ảnh mã QR trông hoàn toàn vô hại. Đó là lý do tại sao email lừa đảo ngày càng thay thế các siêu liên kết cũ bằng mã QR, đặc biệt trong các cuộc tấn công nhắm vào nhân viên doanh nghiệp.

Trong cuộc sống thực, quishing xuất hiện dưới dạng nhãn dán trên các mã hợp lệ ở máy tính tiền đỗ xe, thực đơn nhà hàng giả, thông báo giao hàng lừa đảo trong hộp thư, và trạm sạc công cộng giả yêu cầu

'quét để thanh toán'.

Dấu hiệu nguy hiểm TRƯỚC KHI quét

- **Nhãn dán trên mã gốc.** Nhãn dán QR dán lên một mã QR khác là thủ thuật thay thế điển hình. Nhẹ nhàng nhấc góc lên — nếu bong ra, đừng quét.
- **Ngôn ngữ khẩn cấp trên tờ rơi lạ.** 'Quét ngay để nhận giải thưởng' hoặc 'Bưu kiện của bạn bị giữ — quét để đặt lại lịch giao hàng' là chiến thuật gây áp lực tâm lý.
- **Email hoặc thư không yêu cầu.** Liên lạc bất ngờ từ ngân hàng, công ty giao hàng hoặc cơ quan chính phủ sử dụng mã QR làm lời kêu gọi hành động chính là dấu hiệu cảnh báo mạnh mẽ.

Những gì cần kiểm tra SAU KHI quét và TRƯỚC KHI mở

- **Tên miền có khớp với kỳ vọng không?** Nếu bạn quét mã QR tại ngân hàng, URL phải nằm trên tên miền chính thức.
- **Có phải là dịch vụ rút gọn URL không?** Các dịch vụ như bit.ly hoặc tinyurl.com ẩn đích đến thực sự. Sử dụng dịch vụ mở rộng URL để biết địa chỉ thực trước khi truy cập.
- **Tên miền bị sai chính tả hoặc giả mạo.** Chú ý paypa1.com (số 1 thay cho chữ L) hoặc g00gle.com (số 0 thay cho chữ O). Đọc kỹ từng ký tự.
- **Tên miền phụ đáng ngờ.** login.secure.amazon-giaohang-vn.com có vẻ hợp lệ, nhưng tên miền thực là amazon-giaohang-vn.com, không phải amazon.com.

QR Code Reader Without Ads giúp như thế nào

QR Code Reader Without Ads hiển thị toàn bộ URL trước khi mở bất cứ thứ gì, cho bạn thời gian kiểm tra liên kết trước khi hành động. Nếu địa chỉ có vẻ đáng ngờ, đơn giản là đừng nhấn 'Mở'. Ứng dụng lưu lịch sử quét cục bộ trên thiết bị của bạn, không thu thập dữ liệu và không hiển thị quảng cáo. Có sẵn trên App Store và Google Play bằng cách tìm kiếm 'QR Code Reader Without Ads'.

Tải QR Code Reader Without Ads miễn phí cho iOS hoặc Android — không quảng cáo, không theo dõi và hoạt động hoàn toàn ngoại tuyến.

Trích dẫn: Lubor Šimůnek (2026). *Cách Nhận Biết Mã QR Có An Toàn Không Trước Khi Mở (Hướng Dẫn Chống Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/vi/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.