QR코드 열기 전 안전 여부 확인하는 방법 (퀴싱 가이드)

퀴싱은 QR코드를 이용한 피싱 공격입니다. 스캔 전 위험 신호와 열기 전 확인해야 할 사항을 알아보세요.

작성자: Lubor Šimůnek · 게시일: August 23, 2026 · 보안

온라인 버전: https://appstoryo.com/ko/blog/qr-code-safe-quishing-guide



퀴싱이란 무엇인가?

퀴싱은 QR코드를 악용한 피싱 사기입니다. 공격자가 만든 QR코드를 스캔하면 자격 증명을 훔치거나 악성 소프트웨어를 설치하거나 가짜 결제 페이지를 표시하는 악성 사이트로 연결됩니다. 'QR'과 'phishing(피싱)'을 결합한 용어로, 사람들이 QR코드를 거의 의심 없이 신뢰하기 때문에 빠르게 확산되고 있습니다.

QR코드가 특별한 위험을 가지는 이유

일반 링크는 클릭하기 전에 커서를 올려 URL을 확인할 수 있습니다. 하지만 QR코드는 스캐너가 해독할 때까지 목적지를 볼 수 없으며, 많은 카메라 앱은 주소를 보여주지 않고 즉시 브라우저를 엽니다. 그 짧은 순간으로도 악성 사이트는 기기 추적을 시작하기에 충분합니다.

QR코드는 스팸 필터도 완전히 우회합니다. 필터는 의심스러운 텍스트나 알려진 악성 URL을 찾지만, QR코드 이미지는 완전히 무해해 보입니다. 그래서 피싱 이메일은 특히 기업 공격에서 하이퍼링크 대신 QR코드를 사용하는 경우가 늘고 있습니다.

현실에서 퀴싱은 주차 요금 기기의 정규 코드 위에 붙인 스티커, 위조 식당 메뉴, 우편함에 투입된 택배 사기 안내문, '결제를 위해 스캔'을 요구하는 가짜 공공 충전소 등에서 나타납니다.

스캔 전 확인할 위험 신호

- 원본 코드 위의 스티커. 다른 QR코드 위에 붙은 스티커는 전형적인 교체 수법입니다. 모서리를 살짝 들어보세요 — 벗겨진다면 스캔하지 마세요.
- 낯선 전단지의 긴박한 언어. '지금 스캔해서 경품 받기' 또는 '택배가 보류 중 — 스캔해서 재배송 신청'은 심리적 압박 전술입니다.
- 요청하지 않은 이메일이나 편지. 은행, 배송 회사, 정부 기관에서 왔다고 주장하며 QR코드를 주요 행동 유도 수단으로 사용하는 예상치 못한 연락은 강력한 경고 신호입니다.

스캔 후 열기 전 확인할 사항

- 도메인이 예상과 일치하나요? 은행에서 QR코드를 스캔했다면 URL은 공식 도메인이어야 합니다.
- **URL** 단축기가 사용되었나요? bit.ly나 tinyurl.com 같은 서비스는 실제 목적지를 숨깁니다. URL 확장 서비스를 사용해 방문 전에 실제 주소를 확인하세요.
- 철자가 틀리거나 유사한 도메인. paypa1.com(L 대신 숫자 1)이나 g00gle.com(O 대신 숫자 0)에 주의하세요.
- 의심스러운 서브도메인. login.secure.amazon-delivery-kr.com은 정당해 보이지만 실제 도메인은 amazon-delivery-kr.com이며 amazon.com이 아닙니다.

QR Code Reader Without Ads의 도움

QR Code Reader Without Ads는 무엇을 열기 전에 전체 URL 미리보기를 표시하여 링크를 확인하고 결정할 시간을 줍니다. URL이 의심스러우면 '열기'를 탭하지 않으면 됩니다. 앱은 기기에 로컬 스캔 기록을 보관하며 데이터를 수집하지 않고 광고도 표시하지 않습니다. App Store 또는 Google Play에서 'QR Code Reader Without Ads'를 검색하세요.

iOS 또는 Android에서 **QR Code Reader Without Ads** 앱을 무료로 다운로드하세요 — 광고도, 추적도 없으며 완전히 오프라인으로 작동합니다.

인용 형식: Lubor Šimůnek (2026). *QR코드 열기 전 안전 여부 확인하는 방법 (퀴싱 가이드)*. AppStoryo, lapnito.cz s.r.o..
https://appstoryo.com/ko/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.