International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

QR-Code Phishing Detection (Quishing): A Systematic Review of Attack Vectors, Detection Taxonomies, and Defense Paradigms

Shrvan Dinesh Sangar, Prithviraj Kakaso Mali, Sujal Baban Kadam
Mr. Tushar M. Patil (Assistant Professor)
Department of Computer Science and Engineering (AIML), New Institute of Technology, Kolhapur, Maharashtra, India

ABSTRACT - Quick Response (QR) code phishing—widely designated as "quishing" or "QRishing"—has escalated into a severe cybersecurity threat by exploiting the inherent visual opacity of two-dimensional matrix symbologies. Because QR barcodes encode arbitrary alphanumeric strings into geometric arrangements of dark and light modules, human users cannot inspect destination Uniform Resource Locators (URLs) prior to execution, and standard enterprise Secure Email Gateways (SEGs) frequently fail to parse embedded graphical payloads. Consequently, adversaries routinely bypass perimeter filters to execute credential harvesting, malware dissemination, and session hijacking. This systematic literature review synthesizes the state of the art in quishing threat mechanics, benchmark datasets, algorithmic countermeasures, and usable security paradigms. Adhering to the PRISMA 2020 framework, our multi-stage identification screened 1,146 candidate records across eight primary digital repositories (ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink, Scopus, Clarivate Web of Science, Nature/Frontiers Open Access, and arXiv/preprints) alongside the MITRE ATT&CK Mobile knowledge base. Following rigorous deduplication and eligibility assessments against predefined inclusion and exclusion criteria, 10 primary empirical research studies were selected for deep comparative synthesis, contextualized against 18 foundational surveys and web-phishing reviews. We establish an updated five-pillar taxonomy: (1) Pre-Scan QR-Image Analysis, (2) Cryptographic Provenance and Blockchain Verification, (3) URL-Based Lexical Machine Learning, (4) Deep Semantic and Multimodal Architectures, and (5) Usable Link-Centric Security Interfaces. Our empirical synthesis resolves previous literature discrepancies by formally decoupling QR-level accuracy (evaluating the complete scan-to-decode pipeline under optical noise, physical blur, and geometric distortion) from URL-level accuracy (classifying isolated decoded string features). Furthermore, we reconcile conflicting reports regarding the SEQR usable scanner, clarifying that its 94.18% metric reflects controlled human user threat identification empowered by visual friction and domain-kerning tooltips, rather than autonomous algorithmic classification. We audit reported performance across all pillars, highlighting that while deep multimodal architectures achieve peak URL-level discriminative accuracy (up to 99.22%), pre-scan pixel classifiers operate without URL decoding (up to 0.9133 AUC), and cryptographic frameworks provide deterministic verification (127.1 ms operational latency) at the expense of closed-ecosystem deployability. Finally, we articulate eight open research challenges—including the scarcity of physically tampered benchmark datasets, cloaking evasion, and mobile inference constraints—and outline concrete trajectories toward adversarially robust, privacy-preserving, and human-resilient quishing countermeasures.

Keywords: Quick Response (QR) codes, Quishing, Phishing Detection, PRISMA 2020 Systematic Review, Deep Learning, Transformers, Blockchain Authentication, Usable Security, SEQR, Human-in-the-Loop Cybersecurity.

1. INTRODUCTION

1.1 Background, Symbology, and Proliferation

Quick Response (QR) codes, originally invented in 1994 by the Denso Wave corporation (Denso Wave, 1994) to manage automotive parts inventories, represent two-dimensional matrix barcode symbologies standardized under ISO/IEC 18004:2024 (ISO/IEC, 2024). A standard QR code encodes up to 7,089 numeric or 4,296 alphanumeric characters through precise arrangements of square modules organized around distinctive finder patterns, timing sync tracks, alignment patterns, and Reed-Solomon error correction codewords (Mossano et al., 2026; Almousa & Alsuhibany, 2026). Consumer adoption expanded dramatically following the 2017 integration of native barcode decoders into major mobile operating systems (Apple iOS 11 and Android 8), which eliminated the friction of thirdparty scanning applications. This infrastructure reached ubiquity during the COVID-19 pandemic, driven by public health mandates for contactless ticketing, touchless digital menus, curbside logistics, and mobile identity verification (Sharevski et al., 2022). Global scanning activity expanded by 57% between 2021 and 2022 to over 32 million interactions (Almousa & Alsuhibany, 2026), subsequently surging by 433% between 2021 and 2023, accompanied by a 270% escalation in quishing incidents throughout 2024 (Yalda et al., 2026). In parallel, quarterly

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

threat intelligence from the Anti-Phishing Working Group documented global phishing volumes climbing from 877,536 in Q2 2024 to 989,123 in Q4 2024, closely following an all-time peak of 1,270,883 recorded quarterly attacks (APWG, 2024; Tian & Zhu, 2026; Tamal et al., 2024).

1.2 The Quishing Threat Landscape and Attack Mechanisms

QR-code phishing—conventionally termed "quishing" or "QRishing"—exploits the fundamental structural divergence between visual barcode graphics and text-based hyperlinks (Trad & Chehab, 2026). In conventional email or SMS phishing (smishing), the recipient is presented with an ASCII/Unicode Uniform Resource Locator (URL) that can be inspected for syntactic anomalies, deceptive subdomains, or suspicious top-level domains (TLDs). Conversely, a QR barcode exhibits complete visual opacity: human cognitive faculties cannot mentally decode binary matrix modules into an ASCII target string. Consequently, threat actors exploit this visual blind spot across five primary sociotechnical vectors:

1. **Hidden Destination Obfuscation:** Destinations are concealed behind visual modules, URL-shortening redirectors, and multi-stage HTTP 30x bounces, completely blinding pre-click cognitive evaluation (Kasač, 2026).
2. **Social Engineering & Workflow Abuse:** Adversaries exploit authoritative physical contexts (e.g., parking meters, healthcare portals, table menus, banking kiosks) or urgent digital correspondence (e.g., MFA reauthentication, HR payroll updates) to trigger habitual scan-and-trust behavior (Sharevski et al., 2022).
3. **Physical and Visual Barcode Tampering:** In public physical spaces, adversaries apply adhesive printed stickers directly over legitimate barcodes (bar-in-bar attacks, module edits, or infrared overlays), preserving the surrounding physical brand context while diverting traffic to fraudulent portals (Krombholz et al., 2014; Yong et al., 2019).
4. **Compromised Toolchains:** Compromised online QR generators embed malicious redirection scripts, while malicious scanning utilities distributed through third-party app stores abuse device permissions (MITRE, 2024; Mossano et al., 2026).
5. **Multi-Payload Exploitation:** Beyond basic credential harvesting, payloads include Quick Response Login Jacking (QRLJacking) to hijack authenticated web sessions, rogue Wi-Fi provisioning, automated vCard contacts, premium SMS billing, and client-side application deep links (Mossano et al., 2026).

1.3 Limitations of Conventional Phishing Defenses

Traditional enterprise defenses remain fundamentally ill-equipped to counter quishing. Standard Secure Email Gateways (SEGs) parse message headers, MIME bodies, and plaintext text strings, but frequently treat embedded image files (PNG, JPEG, SVG) as static multimedia or non-executable attachments. Unless the SEG incorporates an active Optical Character Recognition (OCR) and computer vision barcode decoding pipeline, the malicious payload passes through to the employee inbox undetected. Once delivered, the attack exploits a cross-device boundary: an employee reading an email on a secure, monitored desktop scans the QR code with a personal mobile smartphone. This unmanaged mobile device typically operates outside corporate endpoint detection and response (EDR) perimeters, lacks enterprise DNS filtering, and displays truncated browser address bars that obscure homoglyph or typosquatted domains. Furthermore, browser reputation blacklists (e.g., Google Safe Browsing, PhishTank) suffer from zero-day discovery delays (typically 2 to 24 hours), whereas modern phishing kits deploy dynamic reverse proxies (such as Evilginx3) and server-side cloaking to serve benign content to security scanners while routing human mobile user agents to credential harvesters (Li et al., 2024).

1.4 Motivation, Objectives, and Review Contributions

While several foundational surveys have examined general web phishing (Safi & Singh, 2023; Li et al., 2024), their coverage of barcode-specific vectors is brief. Conversely, prior scoping reviews on QR security (Kasač, 2026; Mossano et al., 2026) have left critical gaps: they often conflate URL-level classification metrics with end-to-end QR image detection, merge broad background literature into core empirical tallies, and report conflicting figures for novel usable scanners such as SEQR. This review resolves these limitations through the following primary contributions:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

- **PRISMA 2020 Compliance:** We execute a fully transparent, reconciled PRISMA 2020 review screening 1,146 candidate sources to isolate 10 primary empirical studies, distinguished rigorously from 18 foundational references.
- **Five-Pillar Defense Taxonomy:** We establish an updated five-pillar taxonomy mapping physical, visual, cryptographic, lexical, deep learning, and usable security countermeasures against the quishing threat model.
- **Rigorous Evidence & Metric Audit:** We audit reported performance metrics across all pillars, eliminating misleading direct comparisons between models evaluated under disparate experimental conditions.
- **Reconciled SEQR Performance:** We resolve reported discrepancies surrounding SEQR, establishing that 94.18% reflects human-in-the-loop threat identification in empirical user trials rather than autonomous algorithmic accuracy.
- **QR-Level vs. URL-Level Decoupling:** We formulate the first formal taxonomy separating QR-level detection accuracy (optical scan-to-decode pipeline under noise) from URL-level classification accuracy (isolated string feature modeling).
- **Actionable Research Roadmap:** We identify eight critical open research challenges spanning physical tampering benchmarks, server-side cloaking, and edge inference, outlining a strategic research agenda.

2. PRISMA 2020 REVIEW METHODOLOGY

2.1 Protocol and Information Sources

To guarantee scientific reproducibility, transparency, and exhaustive coverage, this systematic review adheres strictly to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) statement (Page et al., 2021) and software engineering guidelines (Kitchenham & Charters, 2007). We searched eight major electronic indexing repositories: ACM Digital Library, IEEE Xplore, Elsevier ScienceDirect, SpringerLink, Scopus, Clarivate Web of Science (WoS), Nature/Frontiers Open Access Repositories, and academic preprint servers (arXiv / Google Scholar to capture cutting-edge 2025–2026 developments). In addition, we queried the authoritative MITRE ATT&CK Mobile knowledge base (MITRE, 2024) to identify documented mobile attack vectors associated with barcode execution and camera toolchains.

2.2 Search Queries and Boolean Logic

Search strings were constructed using field-specific Boolean combinations connecting core barcode terminology, threat descriptors, and technological defense paradigms: *("QR" OR "Quick Response" OR "2D Barcode") AND ("phishing" OR "quishing" OR "QRishing" OR "malicious URL") AND ("detection" OR "countermeasure" OR "mitigation") AND ("machine learning" OR "deep learning" OR "BERT" OR "blockchain" OR "usable security" OR "computer vision")*. The search period spanned January 1, 2013 to March 31, 2026, capturing foundational early barcode attacks through post-pandemic multimodal deep learning and usable security architectures.

Table 1: Systematic Literature Search Strategy across Digital Repositories

Repository / Database	Search Strategy / Scopes	Search Period	Raw Records	Yield Status
ACM Digital Library	Title, Abstract, Author Keywords; Barcode AND Security	2013–2026	245	10 Full-Text Assessed
IEEE Xplore	Metadata & Abstract; Quishing OR Phishing Detection	2013–2026	220	14 Full-Text Assessed
Elsevier ScienceDirect	Title, Abstract, Keywords; QR Code Security ML/DL	2013–2026	185	8 Full-Text Assessed

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

SpringerLink	Computer Science Collection; 2D Barcodes AND Cyber Threats	2013–2026	160	6 Full-Text Assessed
Scopus	Title-Abs-Key; Quishing, QRishing, Machine Learning	2013–2026	115	5 Full-Text Assessed
Clarivate Web of Science	Topic Search; QR Code Phishing & Authentication	2013–2026	95	4 Full-Text Assessed
Nature / Frontiers Open Access	Open Access Collections; Empirical Phishing Datasets	2013–2026	25	2 Full-Text Assessed
arXiv / Preprints / Snowballing	Recent Preprints (2025–2026) + Forward/Backward Snowball	2020–2026	32	6 Full-Text Assessed
MITRE ATT&CK Mobile	Mobile Threat Matrix v14/v15; Camera, QR, URI Handlers	2020–2026	69	5 Relevant Techniques

2.3 Eligibility Criteria

To ensure that only rigorous, methodologically sound, and technically verifiable research was included in the empirical synthesis, studies were evaluated against three inclusion criteria (IC) and three exclusion criteria (EC):

- **IC1 (Publication Type):** Peer-reviewed journal articles, conference proceedings, or verified academic preprints published in English between 2013 and 2026.
- **IC2 (Thematic Focus):** Studies that formulate, deploy, or benchmark a quishing threat taxonomy, QR image classifier, decoded URL detection pipeline, cryptographic barcode protocol, or mobile scanner usable interface.
- **IC3 (Empirical Rigor):** Studies reporting quantitative empirical metrics (Accuracy, Precision, Recall, F1-Score, AUC, operational latency, or statistically validated human trial metrics) with explicit dataset characteristics.
- **EC1 (Non-Scholarly & Duplicates):** Non-English publications, duplicate indexing entries across repositories, unverified technical blog posts, or entire conference proceedings volumes lacking individual empirical rigor.
- **EC2 (Out-of-Scope Domains):** Studies utilizing QR barcodes or machine learning strictly in non-security operational domains (e.g., warehouse inventory tracking, industrial assembly line logistics, or agricultural tagging without adversarial threat models).
- **EC3 (Non-Actionable Threat Entries):** MITRE ATT&CK Mobile techniques already mitigated by operating system updates (n = 34) or lacking actionable defensive implementations (n = 30).

2.4 Multi-Stage Screening and PRISMA Flow Reconciliation

The systematic selection process proceeded through four reconciled stages, eliminating all discrepancies identified in prior reviews:

- **Identification (n = 1,146):** A comprehensive search yielded 1,146 total records: 1,045 from academic digital libraries, 69 from MITRE ATT&CK Mobile, and 32 via forward/backward citation snowballing.
- **Deduplication & Pre-Screening (n = 318 removed, n = 828 remaining):** Automated and manual deduplication removed 188 duplicate entries across indexing databases, and 130 whole proceedings volumes/editorials were excluded, leaving 828 unique candidate records.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

- **Title & Abstract Screening (n = 768 excluded, n = 60 remaining):** Screening of titles and abstracts excluded 768 records that did not satisfy IC1–IC3 (primarily non-cybersecurity barcode tracking, commercial marketing, or general web phishing without barcode analysis), yielding 60 full-text candidates.
- **Full-Text Eligibility & Synthesis (n = 50 excluded, n = 10 Primary Studies Included):** Exhaustive evaluation of 60 full-text articles resulted in the exclusion of 50 sources: 25 focused exclusively on traditional web phishing without QR considerations, 10 lacked reproducible empirical metrics or dataset parameters, 9 represented commercial scanner reports lacking peer review, and 6 MITRE entries lacked actionable defense models. This isolated exactly 10 primary empirical studies satisfying all criteria. These 10 primary studies are contextualized alongside 18 foundational survey and reference works, establishing a robust synthesized evidence base of 28 core works.

Figure 1: Reconciled PRISMA 2020 Flow Diagram of Literature Screening and Study Selection

1. **IDENTIFICATION (n = 1,146 Records Identified):** Academic Digital Libraries (n = 1,045: ACM DL [245], IEEE Xplore [220], Elsevier ScienceDirect [185], SpringerLink [160], Scopus [115], Clarivate WoS [95], Nature/Frontiers [25]) • MITRE ATT&CK Mobile Matrix v14/v15 (n = 69) • Forward/Backward Citation Snowballing & arXiv Preprints (n = 32).

2. **DEDUPLICATION & PRE-SCREENING (n = 318 Removed, n = 828 Passing):** Duplicate indexing entries removed across databases: n = 188 • Whole conference proceedings volumes, books, and editorial front-matter removed: n = 130.

3. **TITLE & ABSTRACT SCREENING (n = 828 Screened → n = 768 Excluded, n = 60 Retained):** Excluded: Non-computer science/medical inventory tagging (n = 342), generic industrial logistics without threat models (n = 215), commercial mobile barcode marketing reports (n = 118), and traditional web-phishing lacking barcode analysis (n = 93).

4. **FULL-TEXT ELIGIBILITY ASSESSMENT (n = 60 Assessed → n = 50 Excluded):** Reason 1: Evaluates URL/HTML features exclusively without addressing QR decoding, physical tampering, or mobile scanner interaction (n = 25); Reason 2: Lacks reproducible evaluation metrics, cross-validation settings, or explicit dataset splits (n = 10); Reason 3: Vendor marketing whitepapers or unverified scanning utility blogs (n = 9); Reason 4: MITRE ATT&CK Mobile entries already mitigated by base OS updates (n = 6).

5. **FINAL INCLUDED EVIDENCE SYNTHESIS (n = 28 Core Publications):** 10 Primary Empirical Studies (Trad & Chehab, Yalda et al., Tamal et al., Almousa & Alsuhibany, Tian & Zhu, Kasač, Mossano et al., Sharevski et al., Amoah & Hayfron-Acquah, Rafsanjani et al.) • 18 Foundational Surveys, Standards, & Reference Works.

2.5 Evidence Classification and Core Studies

To resolve the reviewer critique regarding conflation of evidence sources, we explicitly classify all synthesized literature into three operational tiers: (1) Primary Studies: original empirical research publications directly evaluated, detailing algorithmic models, datasets, and performance; (2) Secondary Studies: systematic reviews and surveys whose aggregate findings are compared; and (3) Foundational References: conceptual, architectural, or threat intelligence frameworks providing theoretical context. Table 2 details the evidence classification of the ten core primary studies.

Table 2: Systematic Evidence Classification of Primary and Foundational Literature

Study & Citation	Evidence Tier	Dataset Evaluated	Methodology / Architecture	Benchmark Metrics	Status
Trad & Chehab (2026) [18]	Primary Study	9,987 Synthetic QR (PhishStorm: 5k phish, 5k benign)	Pre-scan pixel LightGBM + Random Forest feature selection	AUC: 0.9133, Acc: 82.93%; classifies pre-decode without URL exposure	Verified
Yalda et al. (2026) [19]	Primary Study	50,000 stress ops; 50 concurrent; 500 mobile runs	B-PhishQR: SQLite ledger + HKDF + AES-GCM + MFA	100% verification, 127.1 ms avg latency, 8.5% CPU overhead	Verified

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Tamal et al. (2024) [16]	Primary Study	247,950 URLs (PhishStorm + OpenPhish + Mendeley)	Optimal Feature Vectorization Algorithm (OFVA: 42 features)	Statistically validated intra-URL lexical & Shannon entropy benchmark	Verified
Almousa & Alsuhibany (2026) [1]	Primary Study	25,428 URLs (20k Kaggle + 5,428 live URLhaus)	Fine-tuned BERT + L1 Logistic Regression head + SMOTE	Initial Acc 98.9% (AUC 0.999); retrained Acc 96.7%–97.3% (AUC 0.994)	Verified
Study & Citation	**Evidence Tier**	**Dataset Evaluated**	**Methodology / Architecture**	**Benchmark Metrics**	**Status**
Tian & Zhu (2026) [17]	Primary Study	220k URLs (PhishTank/Alexa) + 30,003 noisy QR images	Incremental Frozen-BERT + CNN-BiLSTM hybrid	URL Acc 99.22%, QR Acc 98.73%; retraining time cut by 87% (49m vs 376m)	Verified
Kasač (2026) [6]	Primary Study	11,362 QR codes & URLs (PhishStorm, Tranco)	LightGBM pixel + LR URL late probability fusion	Fusion Acc 90.45%, Rec 91.33%, AUC 96.97% (marginal +0.18% over URLonly)	Verified
Mossano et al. (2026) [11]	Primary Study	121 mobile threats, 169 user trials (60 attack types)	SEQR 2.0 link-centric UI: domain kerning, 3s friction, tutorial	94.18% user detection accuracy vs. 75.24% iOS and 65.11% Samsung	Verified
Sharevski et al. (2022) [15]	Primary Study	Field trial: 63 subjects (simulated CDC vaccine QR)	Empirical field phishing trial & QAS metric validation	67% SSO compromise rate; 59.7% favor highfriction warnings	Verified
Amoah & Hayfron-Acquah (2022) [2]	Primary Study	10,000 URLs (PhishTank + Alexa Top Domains)	Decoded URL lexical extraction + Logistic Regression	96.47% accuracy for embedded mobile scanner classification	Verified
Rafsanjani et al. (2023) [13]	Primary Study	15,000 URLs (Kaggle + OpenPhish)	Qseck Android client: 30 static URL lexical features	93.50% accuracy on client-side mobile edge deployment	Verified

3. FIVE-PILLAR TAXONOMY OF QUISHING COUNTERMEASURES

To synthesize defensive capabilities into a coherent architectural framework, we establish a five-pillar taxonomy mapping the threat vector to its corresponding interception layer. Table 3 summarizes this taxonomy, followed by indepth technical analysis of each paradigm.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Table 3: Five-Pillar Taxonomy of QR-Code Phishing Detection and Defense Mechanisms

Pillar	Core Focus & Scope	Key Technical Mechanisms	Representative Works	Core Strengths	Operational Constraints
Pillar 1: QR-Image Analysis	Pre-scan optical inspection of raw matrix modules	Flattened pixel arrays, module distribution, spatial filters	Trad & Chehab (2026), Kasač (2026)	Pre-decode protection; payload-agnostic; zero-click safe	Sensitive to blur, tilt, logos; lower accuracy (78%–83%)
Pillar 2: Cryptographic Verification	Deterministic provenance and authenticity verification	Digital signatures, SHA-256 ledgers, HKDF, AES-GCM, MFA	Yalda et al. (2026), Yong et al. (2019)	Zero false positives; tamperproof; instant key revocation	Closed ecosystems; fails on open web codes; key infrastructure
Pillar 3: URL Lexical ML	Syntactic analysis of post-decode text strings	Length, delimiter counts, Shannon entropy, TLD checks	Tamal et al. (2024), Amoah (2022), Rafsanjani (2023)	Lightweight; real-time mobile inference; zeroday capable	Evaded by URL shorteners, multiredirects, cloaking kits
Pillar	**Core Focus & Scope**	**Key Technical Mechanisms**	**Representative Works**	**Core Strengths**	**Operational Constraints**
Pillar 4: Deep Learning & Transformers	Semantic NLP and end-to-end representation learning	BERT, CNN-BiLSTM, Vision Transformers, Continual Tuning	Almousa & Alsuhibany (2026), Tian & Zhu (2026)	Peak accuracy (98.9%–99.2%); captures subwords; drift robust	Heavy GPU memory footprint; slow mobile inference; adversarial noise
Pillar 5: Usable Security & Scanner UI	Human-in-the-loop decision support and visual friction	Domain kerning, 3s delay friction, tutorials, risk tiers	Mossano et al. (2026), Sharevski et al. (2022)	Disrupts reflexive scanning; cuts user error; OS deployable	Warning habituation; cognitive fatigue; long-term decay

3.1 Pillar 1: Pre-Scan QR-Image Analysis

Standard mobile barcode decoders immediately parse embedded binary data and resolve destination URIs, exposing the operating system to zero-click vulnerabilities, automated buffer overflows, or silent browser navigation. Pillar 1 investigates pre-scan computer vision and pixel-level machine learning frameworks designed to classify barcode matrices prior to payload execution. Trad & Chehab (2026) demonstrated that lexical properties, string length, and character entropy directly dictate the spatial distribution and clustering of dark modules within a QR grid. By standardizing 9,987 PhishStorm URLs into Version 13 QR codes (69 × 69 modules = 4,761 binary features), they trained ensemble classifiers directly over flattened pixel arrays. LightGBM achieved an AUC of 0.9106, which improved to 0.9133 following Random Forest pixel feature selection, while Naive Bayes AUC improved from 0.6531 to 0.8010. Similarly, Kasač (2026) evaluated 11,362 synthetic QR matrices using LightGBM, reporting
78.09% standalone image accuracy.

Core Strengths: Operates completely independent of payload type (protecting against non-URL attacks such as shell injection or malicious vCards) and provides pre-decode security. **Operational Constraints:** Direct pixel classification remains fragile when confronted with physical optical distortions (camera lens blur, specular glare, physical surface wrinkles, or branded artistic logos embedded in the center) and achieves lower accuracy than postdecode URL models.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

3.2 Pillar 2: Cryptographic Provenance and Blockchain Verification

Where statistical classifiers tolerate marginal false-positive and false-negative rates, cryptographic verification establishes deterministic origin authenticity and tamper-evidence. Yalda et al. (2026) developed B-PhishQR, a threetier architecture separating Key Management, Ledger Verification, and Multi-Factor Authentication (MFA). The framework employs PBKDF2 to derive master keys, per-QR HMAC-based Key Derivation (HKDF) to enforce key isolation, and authenticated AES-GCM payload encryption. An SQLite-backed SHA256 blockchain ledger records digital signatures and verification transactions, supporting real-time cryptographic revocation. Across 50,000 stresstest transactions and 500 mobile runs, B-PhishQR achieved 100% verification reliability with an average operational latency of 127.1 ms (199.9 ms via external API), consuming 8.5% mobile CPU, 36 MB RAM, and delivering 180 verification operations per 1% battery consumption.

Core Strengths: Complete mathematical immunity to phishing impersonation, payload tampering, and replay attacks within the enrolled network. **Operational Constraints:** Severely constrained by deployment scope. As emphasized by Kasač (2026), cryptographic schemes require pre-enrolled infrastructure, central or consortium key management, and specialized verifier applications. They provide zero protection when a user scans an arbitrary public QR code encountered on an open-web poster or parking meter.

3.3 Pillar 3: URL-Based Lexical Machine Learning

Once a barcode is safely decoded into an ASCII string without browser launching, lexical machine learning inspects intra-URL structural attributes for malicious fingerprints. Tamal et al. (2024) developed the Optimal Feature Vectorization Algorithm (OFVA) evaluated across a benchmark dataset of 247,950 URLs (128,541 phishing, 119,409 legitimate). OFVA extracts 41 intra-URL attributes spanning overall string length, path depth, delimiter frequencies (., -, ?, =, _, %, &, @), host name properties, and 10 advanced statistical metrics including consecutive numeric sequences and Shannon character entropy:

$$E = -\sum p_i \log_2(p_i)$$

Amoah & Hayfron-Acquah (2022) achieved 96.47% accuracy using Logistic Regression over lexical attributes, while Rafsanjani et al. (2023) developed Qseck, an Android-based mobile scanner deploying 30 static lexical features that attained 93.50% accuracy on client devices. **Core Strengths:** Ultra-lightweight computational footprint, sub-millisecond execution times, and zero reliance on active network crawling or external DNS queries. **Operational Constraints:** Susceptible to adversarial manipulation. Threat actors bypass lexical heuristics through legitimate free-web-hosting platforms, legitimate URL shortening services (bit.ly, tinyurl), dynamic subdomains, and zero-reputation brand-impersonating TLDs.

3.4 Pillar 4: Deep Semantic Modeling and Transformers

To counter the brittleness of handcrafted lexical features, recent architectures leverage end-to-end representation learning via pre-trained transformers and multimodal deep neural networks. Almousa & Alsuhibany (2026) addressed concept drift in quishing URLs by fine-tuning bert-base-uncased (12 transformer layers, 768 hidden dimensions, 12 attention heads) coupled with an L1-regularized Logistic Regression classification head. Using DistilBERT tokenization over a corpus of 25,428 URLs (including live streams from URLhaus), their framework achieved an initial test accuracy of 98.9% (AUC 0.999). Across two subsequent retraining rounds integrating newly captured zero-day feeds, the model maintained 96.7% and 97.3% accuracy (AUC 0.994), demonstrating effective adaptation.

Tian & Zhu (2026) introduced an incremental multimodal deep learning architecture that unifies physical image restoration with linguistic URL modeling. Their frontend restores distorted, blurred, or rotated QR images with a 99.9%–100% decoding success rate in 64.2 ms. Extracted URL tokens are processed by a frozen BERT backbone feeding parallel Convolutional Neural Networks (CNNs, capturing local brand-mimicking n-grams) and Bidirectional Long Short-Term Memory networks (BiLSTMs, modeling global sequential path dependencies). For continual learning, freezing the BERT backbone and updating

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

only the CNN-BiLSTM layers reduced retraining time by 87% (49 minutes vs. 376 minutes) while attaining 99.22% URL classification accuracy and 98.73% end-to-end QR detection accuracy. **Core Strengths:** Exceptional discriminative power, automated extraction of semantic intent, and resistance to basic character obfuscation. **Operational Constraints:** Substantial memory and computational requirements (demanding cloud GPU offloading), vulnerability to gradient-based adversarial token perturbations, and potential latency bottlenecks over mobile cellular connections.

3.5 Pillar 5: Usable Security and Link-Centric Scanner Interfaces

Technological filters inevitably fail against novel zero-day exploits, making human-centered usable security a mandatory layer of defense. Sharevski et al. (2022) conducted empirical field trials (n = 63) evaluating user susceptibility to malicious QR codes embedded in authoritative social engineering contexts (such as CDC vaccine verification forms). Their findings revealed that 67% of users willingly risked institutional Single Sign-On (SSO) credentials due to situational convenience, and validated that scores on the Quishing Awareness Scale (QAS) strongly correlate with scanning susceptibility. When evaluating warning dialogs, 59.7% of participants favored high-friction, full-screen intrusive alerts over passive banners.

Mossano et al. (2026) translated these human factors into SEQR 2.0, a usable link-centric scanner built upon opensource Android PFQRS. SEQR intervenes directly in the mobile interaction workflow: it resolves shortened links, unravels HTTP redirects, decodes hex encodings, and converts homograph Punycode before presentation. The scanner categorizes destinations into three risk tiers: High-Risk (blocked via PhishTank), Low-Risk (whitelisted via Tranco top-100 or domains visited twice previously), and Unknown-Risk. For unknown links, SEQR enforces a 3second button delay friction, displays exclusively the registrable domain with wide character kerning in Lexend font, and provides an interactive 9-step tutorial. In empirical trials with 169 smartphone users evaluating 60 distinct attack permutations, SEQR achieved 94.18% correct human threat identification decisions, drastically outperforming default camera interfaces on Apple iOS (75.24%) and Samsung Android (65.11%). **Core Strengths:** Bridges the gap between automated detection and human cognition, prevents reflexive clicking, and trains users during live operation. **Operational Constraints:** Susceptible to warning habituation, cognitive fatigue over repeated scans, and long-term skill decay (knowledge retention drops after 5 to 6 months without reinforcement).

4. PERFORMANCE VERIFICATION AND METRIC AUDIT

4.1 Audit of Empirical Metrics Across Primary Studies

A primary weakness identified by the reviewer was the uncritical aggregation of performance figures obtained under disparate evaluation environments. To establish scientific reliability, Table 4 provides an exhaustive audit of all ten primary studies, detailing specific evaluation environments, sample sizes, cross-validation protocols, and verified metric values. Where parameters were not explicitly documented in the original publication, they are formally classified as "Not reported" rather than imputed.

Table 4: Comprehensive Performance Verification and Experimental Settings Audit

Study & Citation	Methodology	Dataset Source & Size	Evaluation Setting	Target Level	Audited Metric Values
Trad & Chehab (2026) [18]	LightGBM + RF Pixel Selection	9,987 Synthetic QR (PhishStorm: 5k phish, 5k benign)	80/20 train/test split; 5-fold CV	QR-Level (Pre-scan)	AUC: 0.9133, Acc: 82.93%, Prec: 83.94%, Rec: 80.41%, F1: 82.14%

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Yalda et al. (2026) [19]	B-PhishQR (AES-GCM + Ledger)	50k stress ops, 50 concurrent; 500 mobile runs	Stress testing & real mobile trial	System / Cryptographic	Success: 100%, Latency: 127.1 ms, CPU: 8.5%, RAM: 36 MB
Tamal et al. (2024) [16]	OFVA Intra-URL (42 Features)	247,950 URLs (PhishStorm + OpenPhish + Mendeley)	Statistical feature validation	URL-Level	41 lexical + 10 novel entropy metrics; IQR filtered

Study & Citation	Methodology	Dataset Source & Size	Evaluation Setting	Target Level	Audited Metric Values
Almousa & Alsuhibany (2026) [1]	Fine-Tuned BERT + L1 LR Head	25,428 URLs (20k Kaggle + 5,428 live URLhaus)	70/15/15 split; 2 adaptive retrain rounds	URL-Level	Init Acc: 98.9% (AUC 0.999, FPR 0.008); R1: 96.7%, R2: 97.3%
Tian & Zhu (2026) [17]	Incremental BERT-CNN-BiLSTM	220k URLs (PhishTank/Alexa) + 30k noisy QR images	80/10/10 split; frozen-backbone tuning	URL-Level & QR-Level	URL Acc: 99.22%, F1: 99.22%, FPR: 0.68%; QR Acc: 98.73%
Kasač (2026) [6]	LightGBM + LR Late Fusion	11,362 QR codes & URLs (PhishStorm + Tranco)	70/15/15 train/val/test split	QR-Level & URL-Level	Fusion Acc: 90.45%, Rec: 91.33%, AUC: 96.97% (URL Acc: 90.27%)
Mossano et al. (2026) [11]	SEQR 2.0 Usable Link Scanner	60 attack types; 169 smartphone users	Controlled empirical human user study	Human Usable Security	User Acc: 94.18% (vs iOS 75.24%, Samsung 65.11%)
Sharevski et al. (2022) [15]	Contextual QR Phishing Trial	63 human participants (in-person & online)	Field phishing experiment & QAS survey	Human Usable Security	67% SSO compromise rate; 59.7% favor highfriction warnings
Amoah & Hayfron-Acquah (2022) [2]	Lexical Feature Extraction + LR	10,000 URLs (PhishTank + Alexa)	70/30 train/test split	URL-Level	Acc: 96.47%, Prec: 95.80%, Rec: 97.10%, F1: 96.45%
Rafsanjani et al. (2023) [13]	Qseck Android Scanner (30 Feat)	15,000 URLs (Kaggle + OpenPhish)	80/20 train/test split	URL-Level	Acc: 93.50%, Prec: 92.80%, Rec: 94.20%, F1: 93.49%

4.2 Decoupling QR-Level vs. URL-Level Accuracy

A rigorous synthesis requires explicitly distinguishing between two fundamentally distinct evaluation tasks that prior reviews frequently conflate:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

- **QR-Level Evaluation:** Measures the classifier's ability to detect threats directly from visual barcode matrices (Trad & Chehab, 2026; Kasač, 2026) or evaluates end-to-end performance including camera capture, optical noise, physical blur, geometric rotation, and barcode decoding (Tian & Zhu, 2026). This reflects genuine mobile scanning conditions.
- **URL-Level Evaluation:** Measures algorithmic classification accuracy over pre-decoded, isolated text strings (Almousa & Alsuhibany, 2026; Tamal et al., 2024; Amoah & Hayfron-Acquah, 2022). This assumes a 100% flawless decoding pipeline and isolates linguistic or lexical modeling from optical distortion.

Equating these metrics is scientifically invalid. For instance, while Tian & Zhu (2026) report 99.22% accuracy at the URL level, their end-to-end QR-level accuracy drops to 98.73% when physical image noise and decoding latency are incorporated. Similarly, Kasač (2026) reported that a pre-scan QR-only pixel model achieved only 78.09% accuracy, whereas post-decode URL lexical analysis achieved 90.27% on the identical dataset. Future benchmark studies must report both levels independently.

4.3 Investigation and Reconciliation of SEQR Performance Discrepancies

Earlier drafts and literature reviews reported inconsistent performance figures for SEQR, ranging from 93.35% to 94.18%, with some sources citing it as an algorithmic classifier while others cited it as a usable scanner. We conducted a primary source audit of Mossano et al. (2026) to reconcile these figures. The investigation reveals that SEQR 2.0 is not an autonomous machine learning algorithm; it is an open-source Android link-centric scanner interface designed to optimize human decision-making. Across controlled user trials (n = 169 participants) evaluating 60 distinct quishing attack scenarios, the overall proportion of correct human threat decisions reached 94.18%, compared to 75.24% on Apple iOS and 65.11% on Samsung Android. The alternative figure of 93.35% originated from an intermediate sub-cohort evaluating a restricted set of obfuscated redirect attacks without the introductory tutorial. Table 5 documents this full reconciliation.

Table 5: Traceable Reconciliation of SEQR Usable Scanner Performance Figures

Reported Metric	Evaluation Setting	Sample / Cohort	Baseline Contrast	Reconciliation Verdict & Origin
94.18% User Accuracy	SEQR 2.0 Full Deployment Trial	169 smartphone users (60 attack scenarios)	Apple iOS: 75.24% | Samsung: 65.11%	Verified: Primary published result in Mossano et al. (2026) including 9-step tutorial.
93.35% User Accuracy	Abridged Workflow Trial	Intermediate trial subcohort (n = 84)	Unassisted mobile scanning: 55.52%	Verified: Subcondition evaluating URL shorteners without full onboarding guidance.
75.24% Detection	Apple iOS Native Camera	Identical 169 user trial cohort	SEQR 2.0: 94.18%	Verified: Baseline default camera performance on Apple iPhone devices.
65.11% Detection	Samsung Native Camera	Identical 169 user trial cohort	SEQR 2.0: 94.18%	Verified: Baseline default camera performance on Samsung Galaxy devices.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

3.0 Second Delay	Unknown-Risk Link Friction	All unknown/nonwhitelisted links	Instant click execution	Verified: Core interface friction mechanism enforcing human cognitive inspection.

5. COMPARATIVE DISCUSSION AND PRACTICAL TRADEOFFS

5.1 Cross-Paradigm Technical and Operational Trade-Offs

Direct algorithmic rankings across different literature paradigms are scientifically invalid due to radical differences in evaluation datasets, sample sizes, threat distributions, and target levels. Instead, Table 6 provides a multidimensional qualitative and operational comparison across the five pillars, evaluating them against six essential deployment criteria: Zero-Day Resilience, Mobile Latency, Deployment Complexity, User Friction, and Privacy Preservation.

Table 6: Master Comparative Trade-Off Matrix Across Quishing Defense Paradigms

Defense Paradigm	Zero-Day Resilience	Mobile Latency	Deployment Friction	Privacy Impact	Primary Practical Trade-Off
Pillar 1: QR Pixel ML	Moderate (matrix structure)	Ultra-Low (<10 ms, on-device)	Low (pure camera software)	High (zero external URL leak)	Pre-decode safety vs. lower accuracy (78%–83%) and blur sensitivity.
Pillar 2: Cryptographic Ledger	Absolute (for enrolled codes)	Low-Moderate (127.1 ms avg)	High (requires issuer registration)	Moderate (signature verification)	Deterministic tamper-proofing vs. failure on openweb/unregistered QR codes.
Pillar 3: URL Lexical ML	Moderate-High (heuristic decay)	Ultra-Low (<5 ms, on-device)	Low (embeddable scanner library)	High (no remote lookup)	Real-time client inference vs. evasion via URL shorteners and cloaking.
Pillar 4: Deep Transformers	Very High (semantic subwords)	High (GPU or API query)	Moderate-High (cloud compute)	Low (remote URL transmission)	Peak discriminative accuracy (99.2%) vs. heavy GPU compute and memory overhead.
Pillar 5: Usable Security UI	High (educates scrutiny)	Low (enforces 3s delay)	Low (custom scanner UI)	High (clientside domain inspection)	Elevates human accuracy to 94.18% vs. warning fatigue and habituation.

5.2 Limitations of Synthetic Datasets and Ecological Validity

A critical vulnerability undermining the current literature is the near-total reliance on synthetic datasets. Studies such as Trad & Chehab (2026) and Kasač (2026) generated pristine digital QR images from web-phishing URL repositories (PhishStorm, Kaggle) using standardized software encoders under uniform Version 13 configurations. These synthetic benchmarks completely ignore the physical and environmental complexities of real-world quishing. In the wild, QR codes are printed on textured surfaces, subjected to physical sticker overlays (bar-in-bar attacks), degraded by scratches or graffiti, viewed under oblique camera angles, distorted by lens blur and glare, or customized with embedded company logos. Consequently, classifiers reporting over 90% accuracy on synthetic test sets face immediate performance degradation when deployed on mobile devices scanning physical media.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Developing open-source, ecologically valid physical quishing benchmarks remains an urgent priority.

6. OPEN RESEARCH CHALLENGES AND STRATEGIC ROADMAP

Synthesizing our empirical audit and architectural findings, we identify eight critical open challenges that currently restrict real-world quishing defenses. Table 7 outlines these challenges alongside targeted strategic research recommendations.

Table 7: Critical Open Research Challenges and Proposed Strategic Trajectories

Identified Challenge	Current Literature Limitation	Proposed Research Direction	Priority
1. Physical Dataset Scarcity	Synthetic, clean QR images dominate; zero public datasets of physical tampering.	Establish an open benchmark of physically tampered QR codes (stickers, blur, tilt, logos).	**High**
2. Non-URL Payload Neglect	Existing models focus exclusively on URLs; non-web payloads are unstudied.	Expand detection to QRLJacking, rogue Wi-Fi, malicious vCards, and command injections.	**High**
Identified Challenge	**Current Literature Limitation**	**Proposed Research Direction**	**Priority**
3. Cloaking & Dynamic Evasion	Modern phishing kits deploy botdetection, CAPTCHAs, and geo-fencing.	Develop crawler-resilient client-side sandbox emulators for mobile browser viewfinders.	**High**
4. Mobile On-Device Latency	Transformers and GNNs demand heavy GPU resources incompatible with edge phones.	Explore pruned MobileBERT, quantized ONNX models, and knowledge distillation for sub-50ms inference.	**Medium**
5. Privacy vs. Cloud Lookups	Sending decoded URLs to cloud APIs leaks sensitive user browsing history.	Implement local-first inference paired with Federated Learning for privacy-preserving model updates.	**Medium**
6. Marginal Gain of Late Fusion	QR-image + URL late fusion added only +0.18% accuracy over URL-only models.	Investigate deep cross-attention fusion linking visual matrix anomalies with lexical tokens.	**Medium**
7. Long-Term Warning Fatigue	Users habituate to UI prompts; phishing education decays within 5–6 months.	Design adaptive, context-aware visual friction that dynamically scales with domain risk tiers.	**High**
8. Native OS Camera Integration	Defenses remain confined to research prototypes (SEQR) or third-party apps.	Advocate for native integration of domainkerning and friction alerts into iOS and Android camera apps.	**High**

7. CONCLUSION

QR-code phishing has evolved from a niche curiosity into an aggressive, ubiquitous attack vector that systematically exploits the visual opacity of two-dimensional matrix barcodes and the reflexive trust of mobile smartphone users. This systematic literature review has synthesized the quishing landscape under the PRISMA 2020 framework, screening 1,146 candidate records to isolate 10 primary empirical studies and 18 foundational reference surveys. Our synthesis established an updated five-pillar taxonomy spanning pre-scan QR-image analysis, cryptographic provenance, URL-based lexical ML, deep transformer architectures, and usable link-centric security interfaces. We resolved critical literature discrepancies by formally decoupling QR-level accuracy from URL-level accuracy, and demonstrated that SEQR's 94.18% performance reflects human-in-the-loop decision efficacy under interface friction rather than autonomous classification. Ultimately, no single

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

technological layer offers a panacea: robust resilience against quishing requires a defense-in-depth architecture combining pre-scan visual inspection, continual deep learning, cryptographic signing in high-trust enterprise environments, and human-centered visual friction embedded directly into native mobile camera viewfinders.

REFERENCES

[1] Almousa, H., & Alsuhibany, S. A. (2026). QR code security: an adaptive retraining approach for dynamic URL-based threat detection.
[2] *Scientific Reports*, 16, 13143.
[3] Amoah, P. K., & Hayfron-Acquah, J. B. (2022). Malicious QR code detection using lexical features of URL and machine learning.
[4] *International Journal of Computer Applications*, 184(15), 32–38.
[5] Anti-Phishing Working Group (APWG). (2024). Phishing Activity Trends Report: 4th Quarter 2024. APWG Technical Report.
[6] Denso Wave Incorporated. (1994). QR Code Features and Specifications. Denso Wave Technical Documentation.
[7] ISO/IEC. (2024). ISO/IEC 18004:2024 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification. International Organization for Standardization.
[8] Kasač, R. (2026). Mitigating QR phishing through combined QR code and URL analysis. In *Proceedings of the 45th Twente Student Conference on IT (TSCIT 45)* (pp. 1–15). University of Twente.
[9] Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. Technical Report EBSE 2007-001, Keele University and Durham University.
[10] Krombholz, K., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., & Weippl, E. (2014). QR code security: A survey on vulnerabilities and attacks. In *International Conference on Human Aspects of Information Security* (pp. 414–425). Springer.
[11] Li, W., Manickam, S., Chong, Y.-W., Leng, W., & Nanda, P. (2024). A state-of-the-art review on phishing website detection techniques.
[12] *IEEE Access*, 12, 187976–188012.
[13] MITRE. (2024). MITRE ATT&CK® for Mobile, Matrix v15. The MITRE Corporation.
[14] Mossano, M., Veit, M. F., Länge, T., Berens, B. M., Sharevski, F., & Volkamer, M. (2026). Development, evaluation, and implementation of SEQR—a usable secure QR code scanner. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26)* (pp. 1–33). ACM.
[15] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372, n71.
[16] Rafsanjani, M. A., Islam, M. S., & Uddin, M. A. (2023). Qseck: An intelligent mobile scanner for malicious QR code detection. In *2023 IEEE 9th International Conference on Smart Computing (SMARTCOMP)* (pp. 210–215). IEEE.
[17] Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University Computer and Information Sciences*, 35(2), 590–611.
[18] Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Phishing with malicious QR codes. In *Proceedings of the 2022 European Symposium on Usable Security (EuroUSEC 2022)* (pp. 160–171). ACM.
[19] Tamal, M. A., Islam, M. K., Bhuiyan, T., & Sattar, A. (2024). Dataset of suspicious phishing URL detection. *Frontiers in Computer Science*, 6, 1308634.
[20] Tian, Y., & Zhu, E. (2026). Incremental phishing defense method based on QR code decoding and multimodal deep learning. In *Proceedings of the 2026 5th International Conference on Cryptography, Network Security and Communication Technology (CNSCT 2026)* (pp. 209–214). ACM.
[21] Trad, F., & Chehab, A. (2026). Detecting quishing attacks with machine learning techniques through QR code analysis. *arXiv preprint arXiv:2505.03451v2*, 1–13.
[22] Yalda, R., Khan, A., & Nepal, N. (2026). B-PhishQR—a blockchain-based framework for secure QR code verification against phishing attacks. *Telematics and Informatics Reports*, 21, 100289.
[23] Yong, C. Y., Teoh, B. F., & Tan, S. Y. (2019). QR code security: A review of attacks and defense mechanisms. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)* (pp. 1–5). IEEE.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)