Kajian Penipuan Social Engineering dalam Logistik E-Commerce: Studi Kasus QRIS dan *Airwaybiil* Paket di Indonesia

Analysis of Social Engineering Fraud in Indonesia's E-Commerce Logistics: Case Study of QRIS and Package Airwaybill

gairah sinulingga
Sekolah Tinggi Ilmu Ekonomi Manajemen Bisnis Indonesia
Jl. Komjen Pol. M. Jasin (Akses UI) No. 89, Kelapa Dua Cimanggis, Depok 16951
Telp. 021 – 87716339, 87716556, Fax. 021 – 87721016
e-mail:gslingga12@gmail.com

Abstrak

Fenomena penyalahgunaan nomor resi airwaybill (AWB) paket logistik oleh penipu penipuan digital dengan modus pengembalian dana melalui QRIS palsu menjadi perhatian serius dalam ekosistem logistik dan pembayaran digital di Indonesia. Modus ini memanfaatkan teknik social engineering untuk meyakinkan korban bahwa mereka akan menerima pengembalian dana, padahal QRIS yang disediakan justru menarik dana dari rekening digital korban. Penelitian ini bertujuan mengkaji modus operandi, kelemahan sistem, serta mitigasi teknis dan perilaku berdasarkan literatur nasional dan internasional. Hasil studi menunjukkan bahwa QR code phishing (quishing) menjadi bentuk social engineering yang semakin canggih dan efektif. Mitigasi efektif membutuhkan integrasi sistem deteksi berbasis teknologi serta peningkatan literasi digital pengguna.

Kata Kunci: QRIS, social engineering, logistik, phishing, quishing, keamanan digital

Abstract

The misuse of airwaybill (AWB) tracking numbers for logistics packages by digital fraudsters through fake refunds via QRIS has become a serious concern within the logistics and digital payment ecosystems in Indonesia. This modus operandi exploits social engineering to convince victims they will receive a refund, while, in reality, the provided QR code withdraws funds from their digital accounts. This study aims to examine methods, system vulnerabilities, and technical and behavioral mitigation strategies, based on the national and international literature. The results indicate that QR code phishing (quishing) is becoming increasingly sophisticated and effective as a form of social engineering. Effective mitigation requires integrating technology-based detection systems and improving users' digital literacy.

Keywords: QRIS, social engineering, logistics, phishing, quishing, digital security.

.

1. PENDAHULUAN

Dalam beberapa tahun terakhir, metode pembayaran digital seperti QRIS telah menjadi standar nasional di Indonesia, didorong oleh kemudahan dan efisiensinya. Namun, perkembangan ini juga menciptakan ruang baru bagi modus penipuan berbasis teknologi. Salah satu modus terbaru adalah penyalahgunaan informasi pengiriman *airwaybill* ("**AWB**") untuk mengelabui konsumen bahwa paket mereka bermasalah, tertukar dan sebagainya.

Selanjutnya Penipu kemudian menawarkan pengembalian dana melalui QRIS palsu. Korban diminta memindai QRIS yang disediakan oleh penipu, yang ternyata mengarahkan pada proses tarik dana ke rekening penipu.

Perkembangan e-commerce dan digitalisasi layanan logistik telah meningkatkan kenyamanan konsumen dalam bertransaksi. Namun, inovasi ini juga membuka celah bagi tindakan kriminal seperti social engineering dan penipuan digital. Salah satu modus baru yang teridentifikasi adalah penyalahgunaan nomor AWB paket logistik oleh *fraudster* untuk menipu konsumen dengan iming-iming pengembalian dana melalui QRIS palsu (*QR payment*), padahal QRIS tersebut memicu penarikan dana dari rekening digital korban. Kasus ini menjadi nyata di Indonesia, dan belum banyak dieksplorasi secara sistematis dalam literatur ilmiah logistik dan keamanan digital.

Social engineering sendiri merupakan teknik manipulasi psikologis di mana penipu menipu korban untuk mengungkapkan informasi atau mengambil tindakan yang merugikan, termasuk pengungkapan PIN, kode OTP, atau akses rekening sebagai akibat *scan* QRIS palsu. Fenomena ini sejajar dengan jenis serangan "*quishing*" yang memanfaatkan QR Code untuk *phishing* dan pencurian data finansial pengguna. Perusahaan logistik sudah saatnya menerapkan Undang-Undang Pelindungan Data Pribadi pelanggan, demi keamanan dan kenyaman pelanggan.

2. TINJAUAN PUSTAKA

Perkembangan *social engineering* merupakan teknik manipulasi psikologis di mana penipu menipu korban untuk memberikan informasi atau melakukan tindakan merugikan. QR code *phishing* atau *quishing* adalah variasi baru dari teknik ini, dengan memanfaatkan kepercayaan publik terhadap kode QR sebagai alat transaksi aman. Kajian oleh Geisler & Pöhn (2024) menunjukkan bahwa desain profesional QR code palsu sangat mudah menipu pengguna awam. Di sisi lain, studi AI *Based QR Code Fraud Detection System* (2025) mengusulkan sistem deteksi berbasis *machine learning* untuk menilai keabsahan QR code secara *real-time* sebelum diproses pengguna.

Penipuan Digital dan *Social Engineering*

Social engineering adalah bentuk serangan di mana penipu memanipulasi psikologi korban hingga memberikan akses atau data sensitif mereka (mis. kredensial perbankan). Teknik ini terus berkembang bersama digitalisasi, termasuk via *QR code phishing* yang dikenal sebagai *quishing*. Data AWB yang diperoleh Penipu berisikan data antara lain nama lengkap, alamat lengkap, nomor telepon, jenis dan jumlah barang, berat dan dimensi barang, nilai barang, jenis layanan pengiriman, dan biaya pengiriman. Data ini yang digunakan penipu untuk menyakin pelanggan bahwa mereka karyawan perusahaan logistik.

Risiko Sistem Pembayaran QRIS

QRIS sebagai standar pembayaran digital di Indonesia mempermudah transaksi, namun juga menjadi target eksploitasi. Studi nasional menyoroti pemalsuan *barcode* QRIS sebagai tindakan fraud yang memerlukan penanganan lebih serius dari *stakeholder* sesuai dengan amanat dari undang-undang pelindungan konsumen.

Fraud dalam Logistik

Fraud dalam logistik bisa muncul dalam bentuk manipulasi AWB, manipulasi data pengiriman, dan pencurian barang atau dana. Penelitian pada salah satu perusahaan besar menunjukkan bahwa lemahnya pengawasan internal membuka celah kecurangan operasional, yang bisa diperluas ke konteks penipuan pelanggan melalui AWB yang dimanipulasi.

Penelitian internasional di bidang deteksi penipuan digital menegaskan pentingnya model deteksi *real-time* menggunakan *machine learning* atau AI untuk mengidentifikasi pola transaksi yang mencurigakan sebelum terjadi kerugian besar. Saat ini sudah banyak aplikasi fraud detetion management (FDM) yang dapat digunakan.

Salah satu fitur yang dapat digunakan untuk mendetesi awal terjadinya penipuan adalah dengan mengaktifkan parameter lokasi dan kordinat alamat tujuan pengiriman paket. Artinya jika sistem mendeteksi transaksi yang dilakukan pelanggan bukan di lokasi tujuan pengiriman yang tertera pada paket maka FDM akan memberikan *alert* indikasi fraud, melalui sistem berupa informasi transaksi tidak sesuai dengan parameter dan harus segera ditindak lanjuti unit kerja terkait. Misalnya langsung mengkonfirmasi ke pelanggan, apakah benar melakukan transaksi tersebut. Hal mana dapat mengurangi terjadinya kerugian bagi pelanggan dan perusahaan juga terhindar dari risiko reputasi karena isu terjadinya penyalahagunaan data pelanggan.

Quishing dan Mitigasi

Penelitian lain menyebut ancaman *quishing* (QR phishing) sebagai masalah di era digital, di mana QR code yang tampak sah bisa dialihkan ke tautan palsu untuk mencuri data atau menginisiasi penarikan dana tanpa persetujuan korban. Penelitian kuantitatif nasional menunjukkan mitigasi ancaman ini melibatkan faktor *behavioral* dan awareness pengguna serta mekanisme autentikasi yang lebih aman.

3. METODE PENELITIAN

Penelitian Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan studi kasus berbasis fenomena nyata yang terjadi di Indonesia. Data diperoleh melalui studi literatur nasional dan internasional, dokumentasi media terpercaya, serta analisis pendekatan mitigasi dari penelitian sebelumnya. Fokus utama penelitian adalah identifikasi pola penipuan, kelemahan sistem logistik dan pembayaran, serta mitigasi berbasis teknologi dan perilaku pengguna.

Jenis penelitian: kualitatif deskriptif dengan pendekatan kasus nyata penipuan AWB + QRIS.
Pendekatan:

1) Studi dokumen kasus penipuan digital dan AWB palsu di Indonesia
2) Analisis literatur jurnal nasional dan internasional terkait *fraud* digital dan logistik
3) Analisis *sosial engineering* dalam konteks logistik dan pembayaran QRIS

Sumber data:

1) Publikasi jurnal, dan studi empiris
2) Laporan kasus pada beberrpa media nasional terkait modus penipuan AWB + QRIS.

4. HASIL DAN PEMBAHASAN

Hasil kajian menemukan bahwa modus penipuan AWB dan QRIS ini bergantung pada tiga faktor utama: (1) manipulasi psikologis korban melalui pesan personal dan mendesak, (2) penggunaan QRIS palsu yang tampak sah, dan (3) kelemahan verifikasi sistem logistik dan literasi digital korban. Studi Geisler & Pöhn mengonfirmasi bahwa pengguna lebih mudah tertipu oleh *QR code* ketimbang tautan biasa karena asosiasi positif terhadap kode QR. Sementara itu, teknologi berbasis AI dapat dimanfaatkan untuk membuat sistem yang secara otomatis menganalisis *payload* QRIS sebelum pengguna melakukan *scan* dan pembayaran.

Hasil dan Temuan Utama

Modus Operandi
Fraudster menghubungi konsumen dengan informasi paket tertahan atau bermasalah, lalu menawarkan pengembalian dana melalui QRIS. Konsumen diminta menscan QRIS tersebut, yang ternyata merupakan QRIS palsu yang terhubung dengan rekening penipu. Akibatnya, dana konsumen ditarik dari rekening tanpa persetujuan.

Kelemahan Keamanan
Konsumen terlalu percaya pada tautan pesan instan/pesan teks QRIS yang dipindai tidak diverifikasi oleh sistem logistik resmi. Kurangnya literasi keamanan digital membuat pengguna rentan *social engineering*.

Keterkaitan dengan *Social Engineering*
Kasus ini selaras dengan literatur *social engineering* yang menyatakan bahwa penipu memanfaatkan ketidaktahuan dan kepercayaan korban untuk memperoleh akses atau informasi sensitif.

Upaya Mitigasi
Penelitian mitigasi *quishing* menunjukkan bahwa kesadaran pengguna dan autentikasi kuat (mis. autentikasi ganda, sistem verifikasi QRIS

resmi) dapat membantu mengurangi risiko penipuan semacam ini.

Implikasi Operasional Logistik
Kasus QRIS palsu berdampak pada kepercayaan konsumen terhadap layanan logistik serta memunculkan beban reputasi bagi perusahaan logistik. Integrasi sistem pembayaran perlu dilengkapi dengan mekanisme verifikasi resmi yang aman dan terhubung langsung ke *backend* perusahaan untuk mencegah tautan palsu.

Peran Edukasi dan Literasi Digital
Penguatan literasi digital konsumen menjadi strategi mitigasi penting, karena banyak serangan *social engineering* hanya berhasil karena kelemahan *awareness* pengguna.

Teknologi Deteksi Fraud
Penggunaan AI dan analisis data dalam sistem pembayaran dan logistik dapat membantu mengidentifikasi pola transaksi abnormal sebelum dana ditarik atau terjadi kerugian besar, sesuai dengan tren literatur internasional deteksi fraud.

5. KESIMPULAN

Penipuan dengan modus AWB dan QRIS palsu merupakan evolusi dari *social engineering* di era digital yang mengancam ekosistem logistik dan transaksi elektronik. Perusahaan logistik dan *platform* pembayaran perlu mengembangkan sistem verifikasi QRIS berbasis AI serta meningkatkan literasi keamanan digital kepada konsumen. Diperlukan kolaborasi antara *regulator*, penyedia jasa logistik, *platform* e-commerce, dan otoritas keamanan siber untuk meminimalisir dampak fraud digital ini.

Penipuan AWB logistik yang dikombinasikan dengan *social engineering* melalui QRIS palsu merupakan fenomena baru yang meresahkan konsumen dan perusahaan logistik di Indonesia. Kajian terhadap literatur dan kasus menunjukkan perlunya:

1) sistem verifikasi QRIS yang aman dan resmi,
2) peningkatan literasi keamanan digital masyarakat,
3) integrasi teknologi deteksi fraud dalam ekosistem logistik dan pembayaran digital.

6. SARAN

Berdasarkan hasil kajian di atas, maka penelitian ini merekomendasikan beberapa saran strategis sebagai berikut:

1) Perusahaan logistik saatnya memperkuat tata kelola keamanan data dan sistem komunikasi Pelanggan.
2) *Platform e-Commerce* beperan aktif juga dalam memperkuat ekosistem transaksi digital yang aman.
3) Penyedia layanan pembayaran berbasis QRIS dapat meningkatkan transparansi fungsi QRIS melalui notifkasi pra-transaki yang menjelaskan suatu transaksi pembayran atau penarikan dana.
4) Regulator di bidang sistem pembayaran dan pelindungan konsumen dengan meningkatkan literasi keamanan transaksi digital sebagai tindakan pencegahan.
5) Untuk pelanggan jangan terlampau cepat percaya jika mendapat tawaran pengembelain dana karena paket tertukar sebaiknya hubungan terlebih dahulu seller untuk memastikannya.

DAFTAR PUSTAKA

1. *AI-Based QR Code Fraud Detection System*. (2025). International Journal of Innovative Research in Science, Engineering and Technology.
2. Baruadi, R., Puluhulawa, M. R., & Swarianata, V. (2024). *Tinjauan Penipuan dengan Motif Pemalsuan Barcode QRIS dari Aspek Penanggulangan Berdasarkan Hukum Pidana Indonesia*. Jurnal Terang.
3. Destyarini, N., Al Ghozali, F., & Rois, M. (2022). *Legal Protection Quick Response Code as a Payment System*. ICOHETECH Proceedings.
4. Geisler, F. & Pöhn, D. (2024). Hooked: *A Real-World Study on QR Code Phishing*. Arxiv preprint arxiv:2407.16230.
5. Jurnal Paradoks. (2023). *Perilaku Pengguna dalam Menghadapi Ancaman Quishing*. Jurnal Fakultas Ekonomi dan Bisnis, UMI.

6. MetroTVNews. (2024). *Marak Penipuan Logistik, Jangan Asal Klik dan Scan QRIS*. https://www.metrotvnews.com
7. Mutemi, A. (2024). *E-Commerce Fraud Detection Based on Machine Learning*. SciOpen.
8. Pradana, N. N. (2025). *Deteksi Transaksi Mencurigakan Menggunakan Decision Tree dan Logistic Regression. JMA* – Jurnal Media Akademik.
9. Rully Andika, P., Nuraliah Ali, N., & Sangalang, R. S. (2025). *Fraud Crime in Banking Using Social Engineering and Trickery Techniques*. Eduvest – Journal of Universal Studies.
10. Sheed Iseal & Michael Halli. (2025). *AI-Powered Fraud Detection in Digital Payment Systems*. (ResearchGate).
11. Singkeruang, A. W. T. F. (2025). *Mitigating the Risk of Quishing Threats (QR Phishing) using Security Behavior Intentions Scale*. Jurnal Paradoks.
12. Wikipedia. (2024). *Phishing*. https://en.wikipedia.org/wiki/Phishing
13. *https://atmbersama.com/news/baru-pake-qris-tuntas-waspada-ini-modus-penipuan-yang-sering-terjadi*