The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

Investigation of a Courier Brand Impersonation Scam: A Case Study of the CDEK Delivery Fraud

[1] Amal Mammadov
[1] Independent Cybersecurity Researcher and Security Operations Practitioner Vilnius, Lithuania

Received: 18th Nov 2025 | Received Revised Version: 28th Nov 2025 | Accepted: 27th Dec 2025 | Published: 15th Jan 2026

Volume 08 Issue 01 2026 | Crossref DOI: 10.37547/tajet/Volume08Issue01-10

Abstract

Courier-related phishing and impersonation scams have become a persistent threat, exploiting user trust in logistics providers and the rapid growth of e-commerce. This article presents a detailed case study of a delivery scam that impersonated the international courier company CDEK. The investigation reconstructs the full attack chain, beginning with initial social engineering via telephone contact and continuing through the use of a fraudulent web domain designed to harvest sensitive information. Technical artifacts including domain registration details, TLS certificate misuse, web content structure, and interaction flow are analyzed to illustrate how attackers combine psychological manipulation with low-cost technical infrastructure. The study highlights common weaknesses in user awareness, brand protection, and domain abuse monitoring that enable such scams to succeed. Based on the findings, practical detection indicators and mitigation recommendations are proposed for security teams, domain registrars, and end users. The case demonstrates how real-world incident investigations can contribute actionable insights into modern phishing operations and complement existing academic research on social engineering and online fraud (Cloudflare, 2025; Let's Encrypt, 2021).

Keywords: phishing, social engineering, brand impersonation, online fraud, domain abuse, cybersecurity investigation

Cite This Article: Mammadov, A. (2026). Investigation of a Courier Brand Impersonation Scam: A Case Study of the CDEK Delivery Fraud. The American Journal of Engineering and Technology, 8(01), 71–77. https://doi.org/10.37547/tajet/Volume08Issue01-10

1. Introduction

Social engineering remains one of the most effective techniques used by cybercriminals, particularly when combined with brand impersonation and time-sensitive narratives. Courier and delivery services are frequently abused in such campaigns, as users are conditioned to expect shipment notifications and to act quickly to avoid perceived losses or delays. While large-scale phishing campaigns have been widely studied, smaller, targeted scams often receive less attention despite their effectiveness (Verizon, 2025; Anti-Phishing Working Group, 2025).

From a psychological standpoint, these scams typically combine authority, urgency, and scarcity cues to drive compliance, often overriding technical warning signs (Cialdini, 2006; Hadnagy, 2018; Mitnick & Simon, 2002). Phishing research also shows that brand impersonation and payment-flow mimicry remain durable patterns over time (Jakobsson & Myers, 2006).

This article documents and analyzes a real-world scam impersonating the courier company CDEK. Unlike purely theoretical analyses, the investigation is based on direct interaction with the scam infrastructure and focuses on practical indicators observable by defenders.

The goal is to contribute practitioner-driven insights into how such scams are constructed, how victims are guided through the deception process, and how similar attacks may be detected or disrupted earlier.

2. Materials and Methods

The investigation followed a qualitative case study methodology based on direct observation and technical analysis. No automated exploitation or unauthorized access was performed.

The following methods were applied:

- • Manual interaction with the scam workflow as a potential victim.
- • Open-source intelligence (OSINT) analysis of the fraudulent domain, including WHOIS data and DNS records (Daigle, 2004; Internet Corporation for Assigned Names and Numbers, n.d.).
- • Inspection of TLS certificate metadata and hosting characteristics (Cloudflare, 2025; Let's Encrypt, 2021).
- • Visual and structural analysis of the scam website to assess impersonation techniques.
- • Review of publicly available information regarding the legitimate CDEK service for comparison.

• No personal data belonging to third parties was collected or retained during the investigation. The analysis is limited to artifacts voluntarily exposed by the attackers during the scam process.

3. Results

3.1. Initial Social Engineering Phase

The scam began with a phone call claiming to represent a delivery issue requiring immediate user action. The attacker leveraged urgency and authority, instructing the victim to visit a provided website to resolve the problem. This approach reduced skepticism and shifted the interaction from voice to web-based deception.

The fraudulent page presented to the victim is shown in Figure 1.

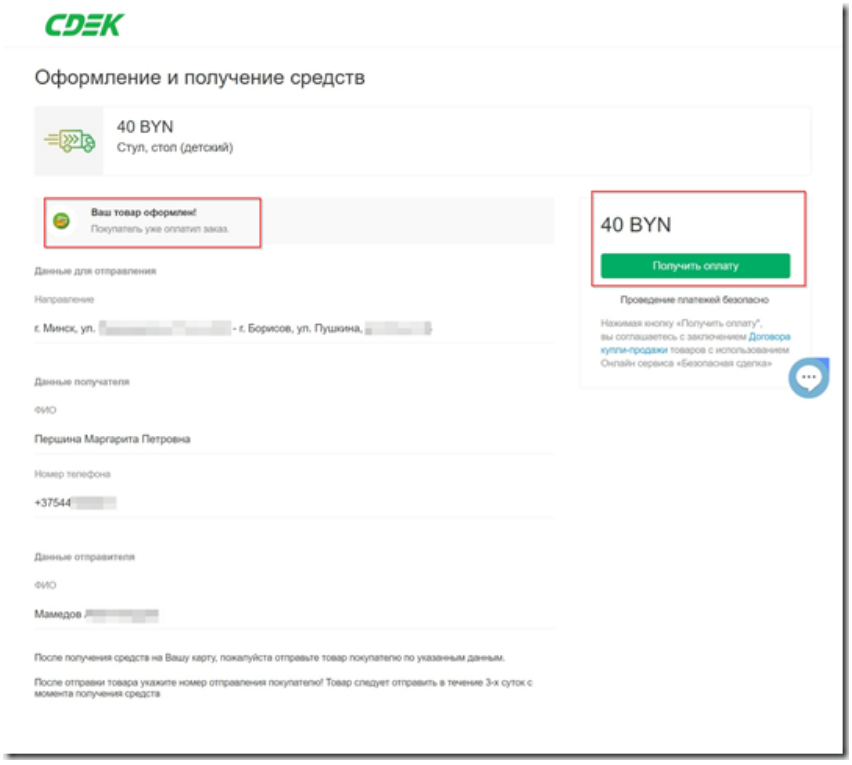

Figure 1. Fraudulent courier delivery page impersonating the CDEK service and prompting the user to proceed with payment confirmation.

3.2. Fraudulent Domain and Infrastructure

The provided website closely resembled legitimate courier tracking pages. Domain analysis revealed recently registered infrastructure with no historical reputation, a common characteristic of short-lived phishing campaigns. The domain name incorporated courier-related keywords to enhance credibility while avoiding direct trademark duplication.

Despite the use of HTTPS and a padlock icon (Figure 2), the domain was unrelated to the legitimate CDEK infrastructure (Let's Encrypt, 2021).

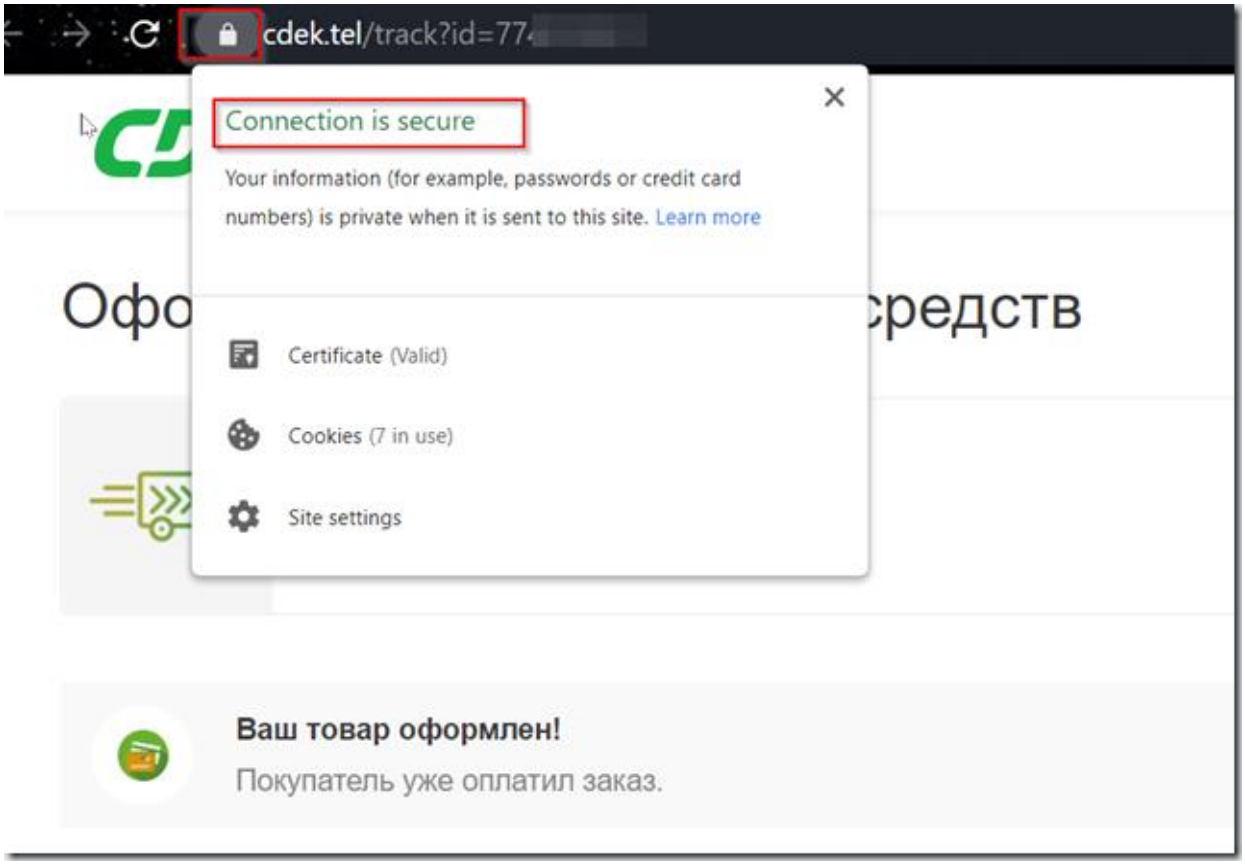

Figure 2. Browser view of the fraudulent domain using HTTPS, visually mimicking a legitimate courier service website.

TLS certificates were valid and issued by a trusted certificate authority, demonstrating how attackers exploit automated certificate issuance to increase perceived legitimacy (Cloudflare, 2025; Let's Encrypt, 2021).

Certificate inspection revealed differences between the legitimate service and the fraudulent site, as illustrated in Figure 3 and Figure 4

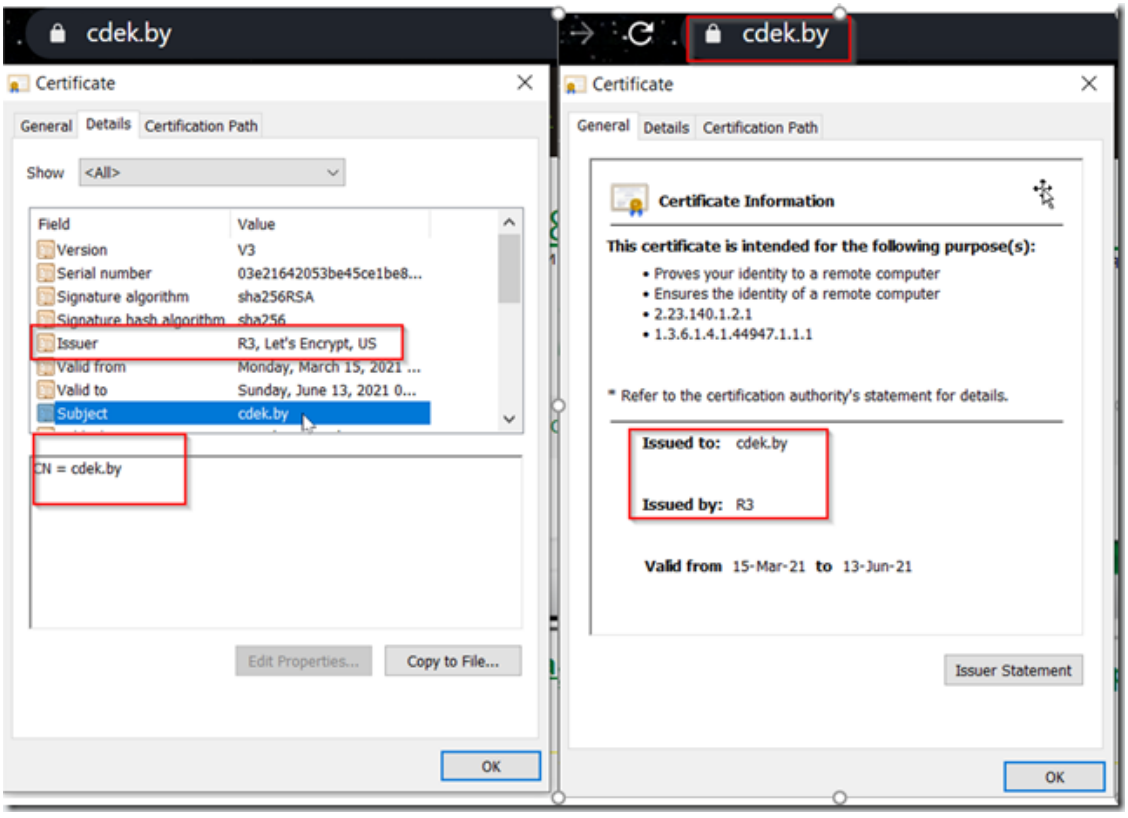

Figure 3. TLS certificate details of the legitimate CDEK domain compared with the fraudulent domain.

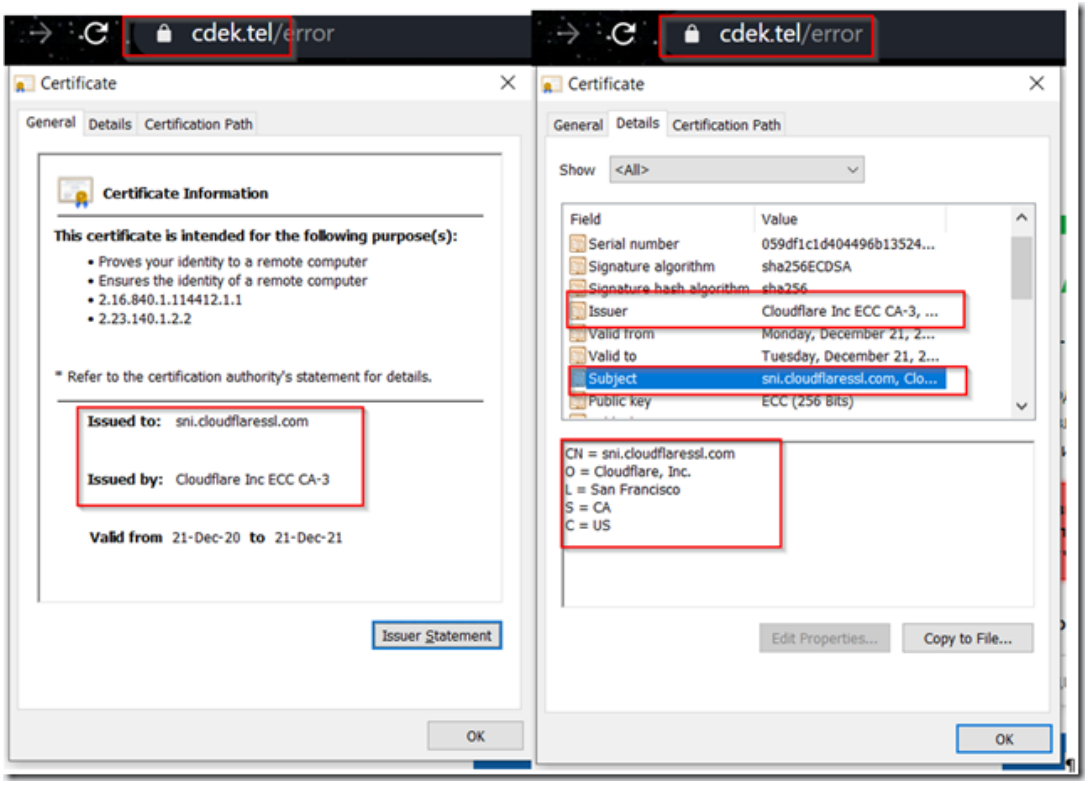

Figure 4. TLS certificate issued via Cloudflare SSL for the fraudulent domain, illustrating third-party certificate termination.

3.3. Website Structure and User Flow

The fraudulent site guided users through a minimal interaction flow, requesting confirmation of delivery details. Visual elements, logos, and language were consistent with logistics branding, reinforcing trust. The absence of advanced backend functionality suggested that the primary objective was credential or data harvesting rather than service simulation. As shown in Figure 5, the fraudulent form requests sensitive card information, including the card verification code (CVC), which is unnecessary for receiving a payment.

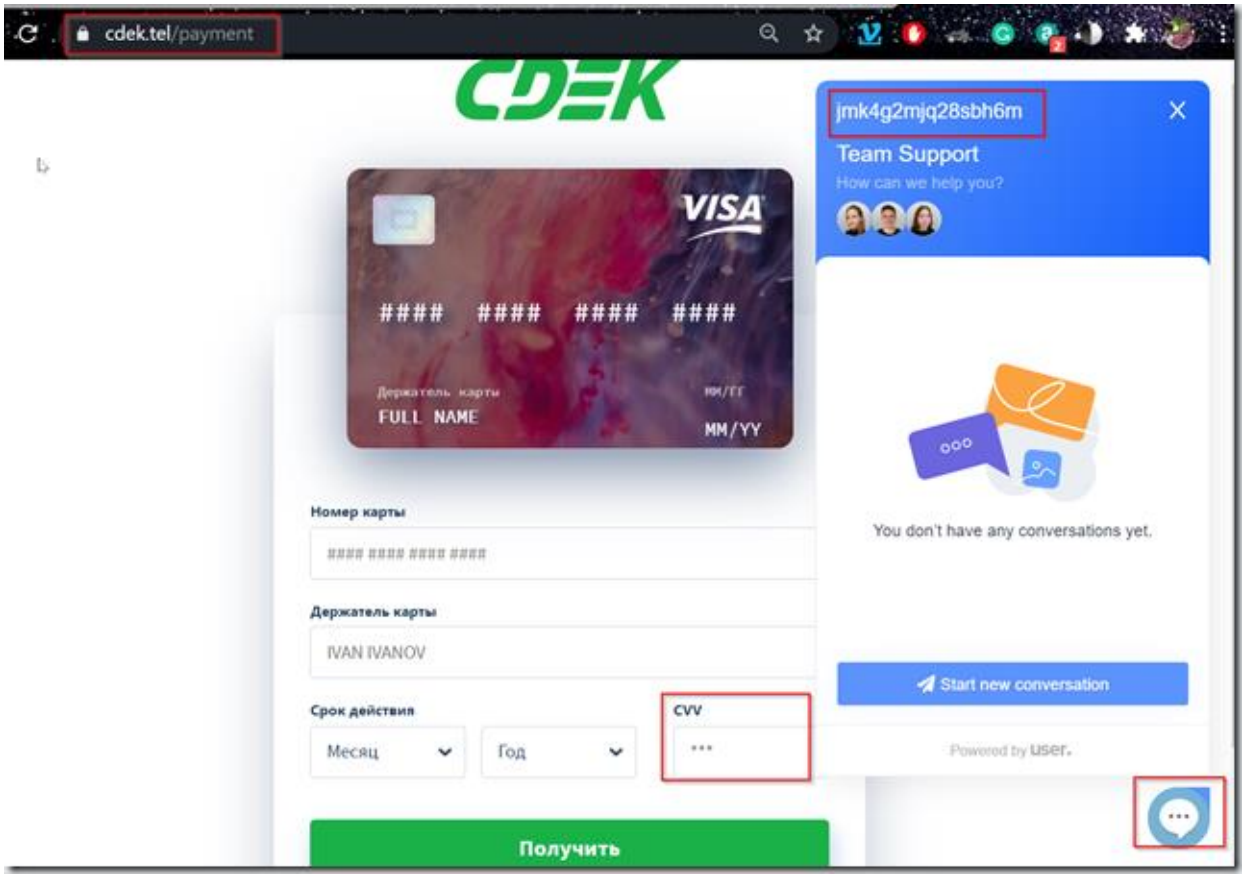

Figure 5. Fraudulent payment form requesting full card details, including the CVC code, under the pretext of receiving funds.

3.4. Indicators of Malicious Activity

Several red flags were identified during the investigation:

- • Recently registered domain with privacy-protected ownership
- • Generic hosting infrastructure inconsistent with enterprise courier platforms
- • Simplified web logic lacking integration with real shipment systems
- • Pressure-driven messaging emphasizing urgency

These indicators are consistent with patterns observed in other delivery-related phishing campaigns. At this stage, the attackers attempt to determine the card balance in order to maximize the amount withdrawn (Figure 6).

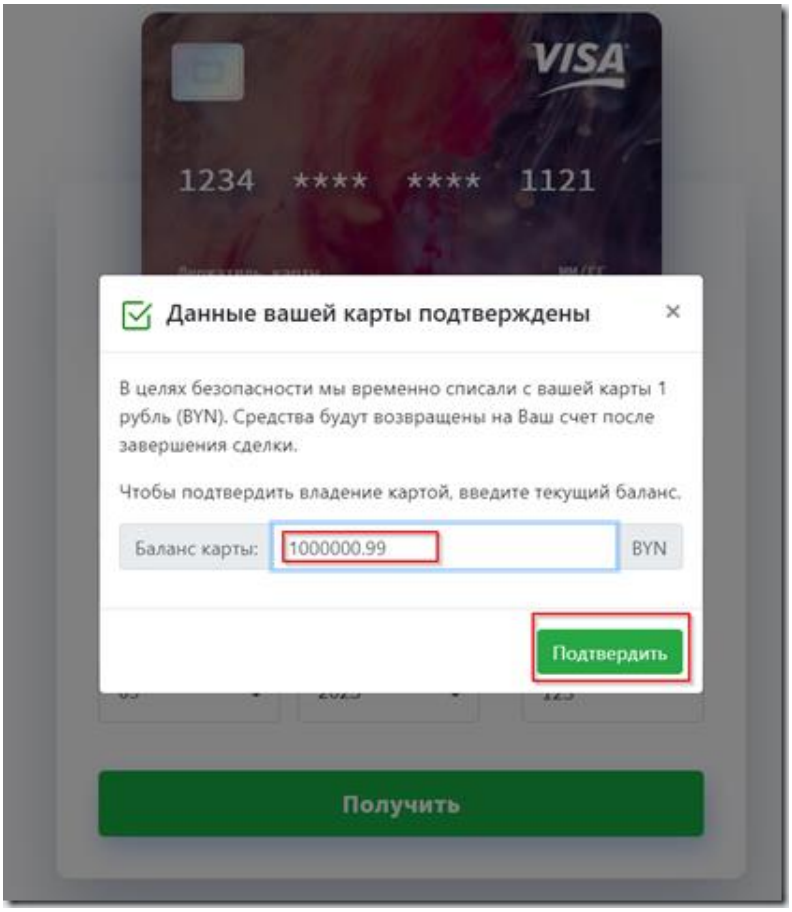

Figure 6. Fraudulent page requesting the victim's card balance under the pretext of a security verification step.

The final stage of the scam attempts to bypass two-factor authentication through a fake 3-D Secure page (Figure 7) (EMVCo, n.d.).

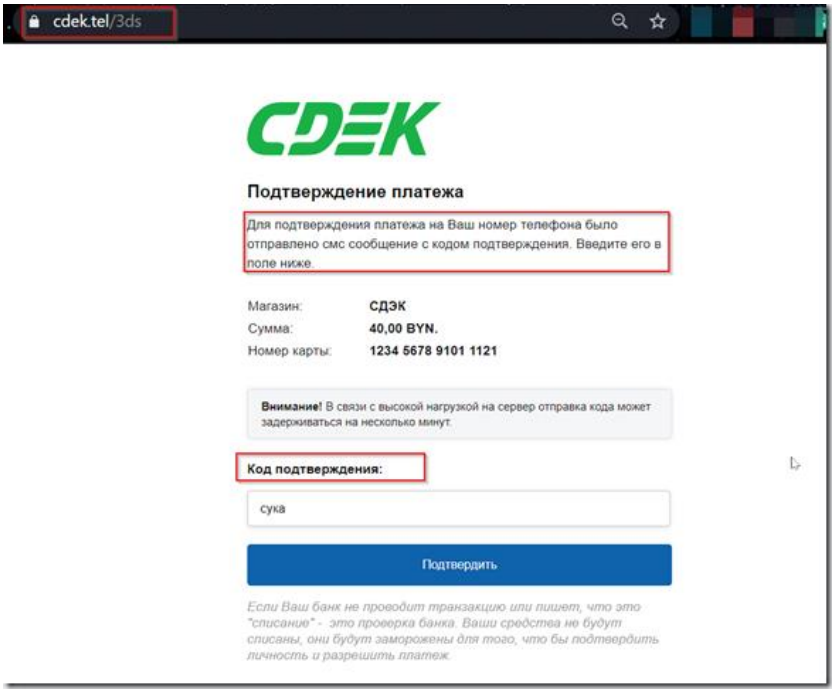

Figure 7. Fake 3-D Secure authentication page designed to capture one-time SMS verification codes.

4. Discussion

The case highlights how effective social engineering does not require advanced technical sophistication. By combining minimal infrastructure costs with carefully crafted psychological pressure, attackers can achieve high success rates. The use of valid TLS certificates and visually convincing branding continues to undermine user trust in traditional security indicators such as HTTPS (Cloudflare, 2025; Let's Encrypt, 2021).

From a defensive perspective, this investigation underscores the importance of brand monitoring, rapid domain takedown processes, and user education focused on behavioral cues rather than technical symbols alone. Security teams should consider integrating domain age, hosting reputation, and contextual analysis into phishing detection workflows.

5. Conclusions

This article demonstrates that small-scale, targeted courier impersonation scams remain a significant threat vector. Through a step-by-step investigation of a CDEK-themed scam, the study provides practical insights into attacker methodology and observable indicators. Practitioner-led case studies such as this can complement academic research by grounding theoretical models in real-world attacker behavior.

Future work may involve comparative analysis across multiple courier scams or quantitative assessment of detection effectiveness based on the identified indicators.

Declarations

Funding: This research received no external funding.

Data Availability Statement: No datasets were generated or analyzed during this study. All observations are derived from publicly accessible information and direct interaction with scam infrastructure.

Conflicts of Interest: The author declares no conflicts of interest.

Author Contributions: Conceptualization,

investigation, analysis, and writing were performed by the author.

Disclaimer: The views expressed in this article are solely those of the author and do not represent any organization or employer.

References

1. Anti-Phishing Working Group. (2025, August 28). P*hishing Activity Trends Report, 2nd Quarter 2025. h*ttps://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf
2. CDEK. (n.d.). *Отслеживание отправлени*й [Shipment tracking]. https://www.cdek.ru/ru/tracking/
3. Cialdini, R. B. (2006). Infl*uence: The psychology of persuasion (Rev.* ed.). Harper Business.
4. Cloudflare. (2025, January 15). C*loudflare SSL/TLS*. https://developers.cloudflare.com/ssl/
5. Daigle, L. (2004). *WHOIS Protocol Specification (RFC 3912).* Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc3912
6. EMVCo. (n.d.). E*MV® 3-D Secure*. https://www.emvco.com/emv-technologies/3-d-secure/
7. Hadnagy, C. (2018). S*ocial engineering: The science of human hacking (2*nd ed.). Wiley.
8. Internet Corporation for Assigned Names and Numbers. (n.d.). IC*ANN Lookup.* https://lookup.icann.org/
9. Jakobsson, M., & Myers, S. (2006). Phishi*ng and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley. https://doi*.org/10.1002/0470086106
10. Let's Encrypt. (2021, February 12). *About Let's Encry*pt. https://letsencrypt.org/about/
11. Mitnick, K. D., & Simon, W. L. (2002). The a*rt of deception: Controlling the human element of security. Wiley.*
12. Verizon. (2025). *2025 Data Breach Investigations Re*port. https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf