Click, Trust, Lose: An Analysis of Social Engineering Vulnerabilities in Uzbekistan

Nurulloh Amirmamatov[1]

Amity University in Tashkent, Tashkent, Uzbekistan
nurulloh.amirmamatov@s.amity.edu

Abstract. Social engineering—the psychological manipulation of people into actions that compromise their own security—has become a dominant cyber-threat in rapidly digitalising economies. This paper analyses the forms social engineering has taken in Uzbekistan, drawing on documented incidents and direct observation. Four recurring attack patterns are identified and organised into a taxonomy: the self-propagating Trojan file (and its newer bot mini-app variant), fake-prize phishing that clones domestic payment brands, a patient trust-building long-con, and the fraudulent security call. We show that these patterns separate into two groups: attacks that depend on intercepting a one-time SMS code, which have been substantially blunted by the introduction of mandatory OneID transaction verification, and attacks that exploit curiosity and emotional investment, which no single regulatory measure can patch. A light conceptual model formalises the exponential, self-replicating spread of the Trojan pattern. We argue that Uzbekistan's elevated exposure reflects the timing of its digital transition—convenience arriving ahead of protective infrastructure and user literacy—rather than any unique deficiency, and we outline a layered set of technical and educational countermeasures.

Keywords: Social Engineering · Phishing · Cybersecurity · OneID · Trojan Malware · Digital Literacy

1 Introduction

A message arrives from a friend on Telegram carrying a file. A day later, that same file has been sent from the victim's own account to every contact they have, the account is locked, and it may already be deleted. This sequence captures the essence of a social-engineering attack: the technical payload is secondary to the manipulation of trust that delivers it.

Social engineering is the psychological manipulation of people into performing actions they would not normally take, such as surrendering credentials or installing malicious software. The tactic is ancient—its emblem, the Trojan horse, lends its name to the modern "Trojan file"—yet its core mechanism of disguise, trust, and exploitation remains effective. In Uzbekistan, this manipulation has taken several increasingly sophisticated forms as digital banking and social media

 Online ISSN: 2348–3326 DOI: 10.21276/MATRIX.2026.9.1.3

adoption have accelerated. This paper documents those forms, organises them into a taxonomy, explains why the country has become fertile ground for them, and assesses which countermeasures actually work. The contribution is a structured, evidence-informed account of a fast-moving regional threat landscape, together with a simple model of why the most resilient attacks persist.

2 Related Work

Defending against social engineering sits at the intersection of data protection, network security, and machine-learning-based detection. Work on securing data in distributed systems addresses the confidentiality guarantees that attackers seek to subvert once they obtain account access [4], while research on secure communication channels for connected devices speaks to protecting the transport layer that credential-theft attacks ultimately target [3]. On the detection side, discriminative feature-selection methods for high-dimensional data underpin modern fraud- and phishing-classification systems by isolating the signals that separate malicious from benign activity [5], and deep-neural-network approaches developed for predictive monitoring demonstrate how anomalous behaviour can be flagged before damage occurs [6]. Adaptive, learning-based control of networked systems further illustrates how defences can respond dynamically to evolving threats [1], and hybrid artificial-intelligence models for analysing transaction records under uncertainty are directly relevant to detecting the fraudulent transfers these scams attempt [2]. The present work complements this technical literature with a human-centred analysis of the specific attack patterns observed in Uzbekistan.

3 Methodology

The study follows an observational, case-based approach. Four attack patterns were identified from publicly reported incidents and from first-hand encounters, then characterised along three dimensions: the form of trust exploited, the technical mechanism of compromise, and the dependence (or not) on a one-time SMS verification code. Quantitative context is drawn from reported national cybercrime statistics. The patterns are then grouped by their susceptibility to existing regulatory safeguards, and the most resilient pattern is formalised with a simple propagation model.

3.1 A Taxonomy of Attack Patterns

Figure 1 summarises the four patterns and the two groups into which they fall.

Pattern 1 – The Trojan file. A file with an emotionally charged name such as *Sud_qarori.apk* (“court verdict”) or *Sen_bilan_rasmlar.apk* (“pictures with you”) arrives from a friend’s account. The names are chosen to provoke curiosity

Online ISSN: 2348–3326 DOI: 10.21276/MATRIX.2026.9.1.3

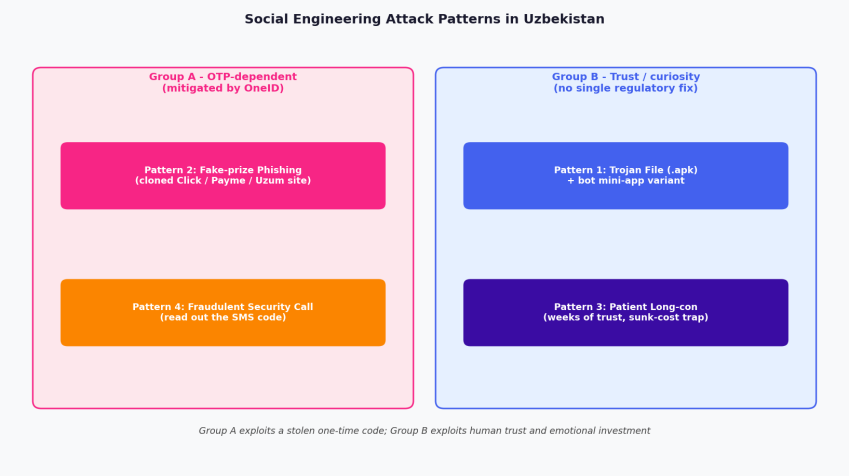

Fig. 1: Taxonomy of the four observed social-engineering patterns. Group A depends on a stolen one-time code; Group B exploits human trust and emotional investment.

or panic. Opening the file grants the attacker access to the victim's Telegram, which then automatically forwards the same file to every contact—turning each victim into an unwitting distributor and enabling exponential spread. A newer variant skips the file entirely: a Telegram bot's mini-app requests the user's phone number the moment it opens, which can be sufficient to hijack the session and propagate the bot's link before the original account is deleted.

Pattern 2 – Fake-prize phishing. The victim receives a message or call announcing a cash prize, cashback, or lottery win. The accompanying link leads to a counterfeit site that clones the branding of major Uzbek financial platforms such as Click, Payme, and Uzum, often using a near-identical domain (for example, *uzum.uz.co* in place of *uzum.uz*). To "claim" the prize, victims enter their card number, expiry date, and the one-time SMS code—emptying rather than enriching their account.

Pattern 3 – The patient long-con. A stranger with a sympathetic profile opens casual conversation on Instagram, Facebook, or TikTok with no immediate request, cultivating a relationship over weeks. The eventual ask is framed as a large reward—such as a lucrative appointment or a multi-million payout—contingent on a comparatively "small" upfront fee for taxes or delivery. After sustained emotional investment, that fee can feel reasonable: the mechanism is closer to sunk-cost reasoning than to panic.

Pattern 4 – The fraudulent security call. A caller posing as bank security warns that an unauthorised transfer is in progress and asks the victim to read out

Online ISSN: 2348–3326
DOI: 10.21276/MATRIX.2026.9.1.3

the SMS code that just arrived "to stop it"—the very code that authorises the attacker's transfer. Victims comply precisely because they believe they are protecting themselves.

3.2 Conceptual Propagation Model

The Trojan pattern is distinctive because each compromise generates further compromises. If each infected account forwards the payload to its contacts and a fraction act on it, the number of compromised accounts grows multiplicatively:

$$N(t) = N_0 \, R^t, \tag{1}$$

where N_0 is the initial number of compromised accounts, t indexes propagation rounds, and R is the average number of new compromises produced per infected account. When $R > 1$ the population of victims grows exponentially until it saturates the reachable contact graph; the self-replication shown in Fig. 2 is what distinguishes Pattern 1 from the others. Crucially, R for this pattern is governed by human curiosity, not by any single transaction safeguard, which is why regulatory fixes aimed at the payment step leave it largely untouched.

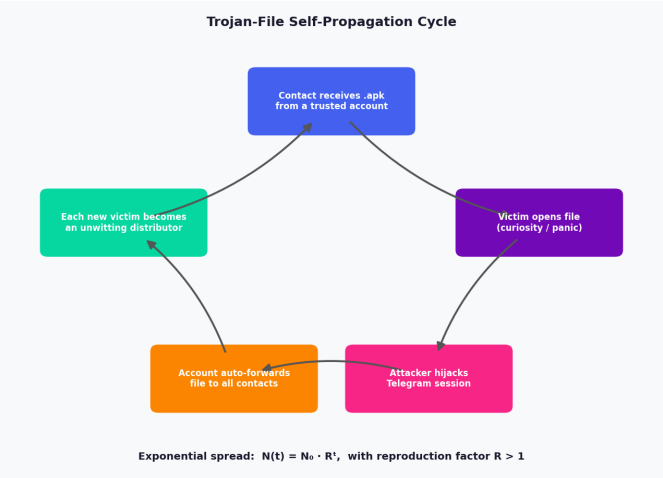

Fig. 2: Self-propagation cycle of the Trojan-file pattern, with reproduction factor $R > 1$.

4 Results and Discussion

4.1 Two Groups, Two Fates

Although the four patterns differ in disguise, they separate cleanly. Patterns 2 and 4 both depend on capturing a one-time SMS code, and both have lost

Online ISSN: 2348–3326
DOI: 10.21276/MATRIX.2026.9.1.3

much of their effectiveness since OneID-based verification became mandatory for bank transfers: a single intercepted code is no longer sufficient to authorise a transfer. Patterns 1 and 3, by contrast, never rely on intercepting a code; they exploit curiosity and emotional investment, which no single regulatory measure can patch. The distinction matters: a technical safeguard can close one door, but while human trust remains exploitable, attackers simply knock on another.

4.2 Why Uzbekistan, Why Now

The most convincing explanation for Uzbekistan's exposure is timing rather than technological deficiency. Digital banking and social media expanded faster than the systems meant to protect them, and the country has not yet had time to build societal "immunity." Earlier-digitalising countries weathered comparable waves and adapted through stronger regulation and more security-literate users; Uzbekistan is traversing that same learning curve later and faster. Reported figures underline the scale: cybercrime rose by more than 6,700% between 2019 and 2024 and, by 2024, accounted for nearly half of all reported criminal cases [7]. Figure 3 visualises this trajectory. OneID is itself part of the catch-up: before it, verifying identity for a transfer relied on weaker checks—often just a phone number or SMS code—precisely what Patterns 2 and 4 exploited.

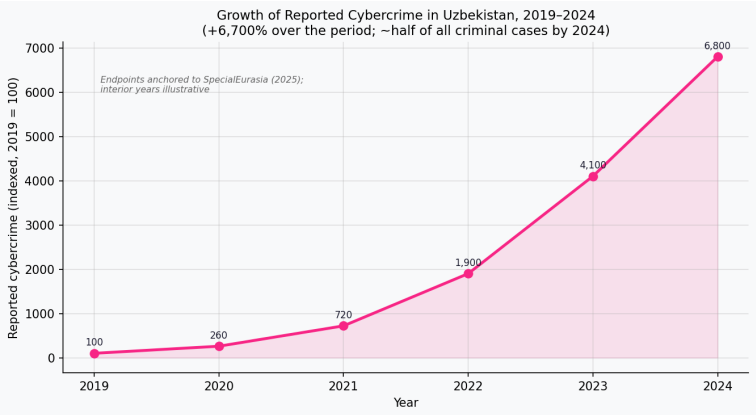

Fig. 3: Indexed growth of reported cybercrime in Uzbekistan, 2019–2024. Endpoints are anchored to the reported +6,700% increase [7]; intermediate years are illustrative.

4.3 Countermeasures

Uzbekistan has already begun building immunity. Multi-factor authentication via OneID is now mandatory for bank transfers, and public-awareness campaigns

Online ISSN: 2348–3326 DOI: 10.21276/MATRIX.2026.9.1.3

warn against sharing verification codes or opening suspicious links and files; the effect on Patterns 2 and 4 is visible. The remaining two patterns are harder to legislate away. Because the Trojan file spreads through curiosity rather than a stolen code, OneID does not impede it, and platform-side recourse is limited. Durable defence therefore requires a different kind of progress: encouraging users to enable Telegram's own two-factor authentication, never to install an `.apk` received in chat, and to recognise when a stranger's friendliness escalates too quickly. On the technical side, machine-learning detection—feature-selection-based phishing classifiers [5], neural anomaly detection [6], and AI-based transaction analysis [2]—offers a complementary layer that can flag malicious links, files, and transfers before a human is deceived.

5 Conclusion

Social engineering succeeds not because people are careless but because it targets human instincts—curiosity, trust, fear, and patience. The attack patterns documented here are not unique to Uzbekistan; every fast-digitalising economy meets the same wave sooner or later, and the country's present vulnerability is better read as the cost of rapid digitalisation than as a sign of weakness. The OTP-dependent patterns are already fading under OneID, but the Trojan file and the slow-built con will recede only as the first ones did: through time, awareness, and enough people learning—before it costs them—what these patterns look like. Combining mandatory multi-factor verification with sustained digital-literacy efforts and machine-learning-based detection offers the most credible path to lasting immunity.

References

1. Chaudhary, N., Ather, D., Kler, R., Dubey, R., Saxena, U., Singh, G.: Adaptive qos-aware routing for iot networks using deep reinforcement learning. In: 2025 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM). pp. 1–5. IEEE (2025)
2. Hussein, T.M., Rakhmatilla, T., Ather, D., Khan, R.L., Sarkar, T., Rakhra, M.: A neutrosophic-ai model for spatiotemporal analysis of land parcel transactions. International Journal of Neutrosophic Science (IJNS) **27**(1) (2026)
3. Jain, V., Ather, D., Hamid, A.B.A., Sharma, R.R., Talipova, G., Manteghi, G.: Secure arduino-based lifi communication for iot sensor networks. In: 2025 Optical Communication, Photonics, Telecommunications, and Intelligent Machine Applications (OPTIMA). pp. 189–194. IEEE (2025)
4. Jain, V., Jain, S., Ather, D., Manteghi, G., Hamid, A.B.A.: Securing patient data in distributed healthcare systems. In: Revolutionizing Metabolic Medicine With Artificial Intelligence, pp. 391–410. IGI Global Scientific Publishing (2026)
5. Kumari, N., Ather, D., Buhari, A., Agarwal, V., Verma, A.: A multi-objective hybridized metaheuristic optimization technique for discriminative feature selection from high-dimensional data. In: 2026 5th International Conference on Innovative Practices in Technology and Management (ICIPTM). pp. 1–8. IEEE (2026)

 Online ISSN: 2348–3326 DOI: 10.21276/MATRIX.2026.9.1.3

6. Saxena, U., Singh, G., Chaudhary, N., Ather, D., Kler, R., Dubey, R.: Iot-driven predictive maintenance in industrial systems using deep neural networks. In: 2025 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM). pp. 1–6. IEEE (2025)
7. SpecialEurasia OSINT Team: Rising cybercrime alarms uzbekistan's national security. SpecialEurasia (2025), https://www.specialeurasia.com/2025/06/03/cybercrimes-uzbekistans/

 Online ISSN: 2348–3326 DOI: 10.21276/MATRIX.2026.9.1.3