Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Қылмыстық құқық. Қылмыстық процесс / Criminal law. Criminal procedure/ Уголовное право. Уголовный процесс

Scientific article
IRSTI 10.77.51
https://doi.org/10.32523/2616-6844-2026-156-3-188-200

Navigating the Legal Gaps: Phishing, Vishing, and the Emerging Landscape of Online Fraud in Kazakhstan

N.S. Temirbolat[1], S.Sh. Urkumbay*[2], R.A. Alshurazova[3]

[1,2]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3]M. Auezov South Kazakhstan University, Shymkent, Kazakhstan

(e-mail: [1]nuraishamail@gmail.com, [2]urkumbay_sulushash@live.kaznu.kz, [3]rau-0708@mail.ru)

Abstract. Phishing, vishing, and broader forms of online fraud pose significant threats to Kazakhstan's citizens, yet existing legislative and policy frameworks do not comprehensively address these increasingly sophisticated tactics. This article undertakes a comparative legal analysis of Kazakhstani legal documents, including the Penal Code, the Law «On Personal Data and Their Protection», and other relevant regulations, to examine how such crimes are defined and codified. The findings reveal that while fraud statutes broadly accommodate certain dimensions of cyber deception, explicit references to phishing and vishing remain absent or insufficiently developed, leaving enforcement agencies to interpret modern social engineering schemes through traditional legal provisions. Similarly, national cybersecurity strategies, such as the «Cyber Shield of Kazakhstan», recognise social engineering as a growing threat but fail to offer targeted measures for mitigating it. The article argues that these omissions, combined with the dynamic nature of cybercrime, create enforcement ambiguities. By highlighting critical gaps and ambiguities in current legislation, this analysis underscores the need for an updated legal framework capable of keeping pace with evolving cybercriminal methodologies, ultimately ensuring more robust protection for both individuals and institutions.

Keywords: phishing, vishing, online fraud, Kazakhstan, legal framework

Received: 14.02.2025. Accepted: 12.05.2026. Available online: 30.09.2026.

***corresponding author**

Н.С. Темірболат[1], С.Ш. Үркүмбай*[2], Р.А. Альшуразова[3]
[1,2]Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
[3]М. Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан
(e-mail: [1]nuraishamail@gmail.com, [2]urkumbay_sulushash@live.kaznu.kz, [3]rau-0708@mail.ru)

Құқықтық тетіктерді қарастыру: фишинг, вишинг және Қазақстандағы онлайн алаяқтықтың қалыптасып келе жатқан көрінісі

Аңдатпа. Фишинг, вишинг және онлайн алаяқтықтың өзге де түрлері Қазақстан азаматтарына елеулі қатер төндіруде, алайда қолданыстағы заңнамалық және саяси тетіктер бұл барған сайын күрделеніп келе жатқан әдістерге жеткілікті дәрежеде көңіл бөлмейді. Берілген мақалада салыстырмалы құқықтық талдау жүргізіліп, Қазақстан Республикасының Қылмыстық кодексі, «Жеке деректер және оларды қорғау туралы» заңы және өзге де тиісті нормативтік-құқықтық актілер қарастырылады. Бұл талдау аталған қылмыстардың заңнамада қалай анықталып, кодификацияланатынын айқындауға бағытталған. Зерттеу нәтижелері көрсеткендей, алаяқтыққа қатысты жалпы ережелер кибералаяқтықтың кейбір қырларын қамтығанымен, фишинг пен вишингке нақты сілтемелер жетіспейді немесе жеткіліксіз қарастырылған. Соның салдарынан құқық қорғау органдары заманауи әлеуметтік инженерия схемаларын дәстүрлі құқықтық нормалар аясында түсіндіруге мәжбүр. Сонымен қатар, Қазақстанның Киберқауіпсіздік тұжырымдамасы (Киберқалқасы) сияқты ұлттық киберқауіпсіздік стратегияларында әлеуметтік инженерияның өсіп келе жатқан қаупі мойындалғанымен, оны нақты болдырмауға арналған мақсатты шаралар жүйесі ұсынылмаған. Мақалада осы олқылықтар киберқылмыстың қарқынды дамып отырған сипаты аясында құқық қолдануда екіұштылық туғызатыны айтылып, қазіргі заңнамадағы басты тетіктер мен түсініксіздіктер атап көрсетіледі. Соның нәтижесінде, кибералаяқтықтың өзгермелі әдістеріне ілесіп отыратын жаңартылған құқықтық базаның қажеттігі нақты дәлелденеді.

Түйін сөздер: фишинг, вишинг, онлайн алаяқтық, Қазақстан, құқықтық база

Н.С. Темірболат[1], С.Ш. Үркүмбай*[2], Р.А. Альшуразова[3]
[1,2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[3]Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан
(e-mail: [1]nuraishamail@gmail.com, [2]urkumbay_sulushash@live.kaznu.kz, [2]rau-0708@mail.ru)

Рассмотрение правовых пробелов: фишинг, вишинг и формирующееся поле онлайн-мошенничества в Казахстане

Аннотация. Фишинг, вишинг и другие формы онлайн-мошенничества представляют существенные угрозы для граждан Казахстана, однако существующие законодательные и политические рамки не в полной мере учитывают эти всё более изощрённые методы. В данной статье проводится сравнительный правовой анализ казахстанских нормативных документов, включая Уголовный кодекс, закон «О персональных данных и их защите» и другие релевантные нормативно-правовые акты, с целью выяснить, каким образом данные преступления определены и закреплены в законодательстве. Результаты

показывают, что, хотя нормы о мошенничестве в целом охватывают некоторые аспекты цифрового обмана, чётких формулировок, касающихся фишинга и вишинга, по-прежнему не хватает или они развиты недостаточно, вынуждая правоохранительные органы интерпретировать современные схемы социальной инженерии в рамках традиционных правовых положений. Аналогичным образом, национальные стратегии кибербезопасности, такие как «Киберщит Казахстана», признают растущую угрозу социальной инженерии, однако не предлагают адресных мер по её предотвращению. В статье утверждается, что подобные пробелы, усугубляемые динамичным характером киберпреступности, ведут к правоприменительным неопределённостям. Указывая на ключевые недостатки и противоречия в текущем законодательстве, данное исследование подчёркивает необходимость обновлённой законодательной базы, способной поспевать за эволюционирующими методами киберпреступников и обеспечивать более надёжную защиту для граждан и организаций.

Ключевые слова: фишинг, вишинг, онлайн-мошенничество, Казахстан, правовая база

Introduction

The internet and cybercrimes are a global phenomenon and are as ubiquitous as consumer and business access to the technology it is performed on. There are a variety of sophisticated ploys used by fraudsters to deceive unsuspecting victims of their personal and financial information, which may result in stolen identities, bank account takeovers, redirection of mail, and appropriated loans. Fraudsters regularly change locations to evade detection, operate in a legal grey area, and seek small amounts of money [1]. Internet fraud and cybercrimes manifest in a myriad of different ways, including scam calls, emails, and text messages [2].The worldwide cost of cybercrime has risen from $445 billion in 2014 to $608 billion in 2017. In 2017, it was disclosed that cybercrime impacted a total of 978 million individuals across 20 different nations [3]. According to data from the legal statistics and special records committee of the General Prosecutor's Office, Kazakhstan experienced a 70.6 percent rise in internet fraud in 2020. Over the first 11 months of 2019, 7,000 fraud incidents were documented, whereas the figure for the corresponding period in 2021 reached 12,000 [4].

Despite a wealth of literature on cyberfraud globally, there has been scant research into the internet fraud landscape, specifically phishing in Kazakhstan. It is also essential to note that research and features of phishing prevalent in other states may not be directly applicable to the Republic of Kazakhstan. However, due to the lack of literature on Kazakhstan, it is important to understand how the practices of phishing are dealt with in other countries. It is our hope that this work will shed light on phishing in Kazakhstan and fill the gap of research which exists. Therefore, it is appropriate to outline the aim of this study. In this article, a comparative legal analysis of the primary legal frameworks, policy documents, and regulatory provisions in Kazakhstan that address such crimes is undertaken, examining how current statutes define phishing and other forms of online fraud. By situating the discussion within the broader context of the nation's cybersecurity policies, the efficacy of existing legal instruments in deterring would-be fraudsters has been scrutinised.

Literature review

It is necessary here to clarify exactly what is meant by phishing. Phishing is a form of cyberattack where a fraudster uses social engineering tactics to steal someone's identity, deceive victims into revealing sensitive information, and obtain identifying information, banking and payment card data, and passwords. Phishing often involves sending fake emails, texts, and phone calls that imitate legitimate online platforms such as banks, auctions, or payment websites. These emails direct visitors to a fraudulent webpage that is skilfully crafted to resemble the authentic login page of the legitimate site [5]. Phishing emails, texts, and phone calls may result in significant financial losses for those who are deceived by the messages. Moreover, they pose challenges for the institutions whose brands are being imitated by the fraudsters [6].

There has been a wealth of research into phishing globally, and an affluence of government statistical reports. For example, in 2022 in the United States alone, the IC3 (FBI's Internet Crime Complaint Center) received 800,944 complaints of internet fraud, with potential total losses amounting to over $10.2 billion (FBI, 2023). According to the same report, the most common victims by age group were persons aged 60+ with a total of $3.1 billion in losses from internet fraudsters, and the most common internet crime type was phishing (Receiving unsolicited communication via email, text, or phone from a seemingly reputable company asking for personal, financial, or login information), totalling 300,497 victims and $52,089,159 in 2022 alone [7].

In the United Kingdom, there were 4.5 million fraud offences reported in the Telephone-operated Crime Survey for England and Wales (TCSEW) for the year ending March 2022, marking a 25% rise from the previous year ending March 2020 (ONS, 2022). 50 percent of TCSEW respondents said they may have received a phishing email, SMS, or social media message (ONS, 2022). 54% of those who received phishing communications were targeted by fraudsters impersonating delivery firms, 32% by banks or financial institutions, and 29% by e-commerce companies. Of the responders who received phishing communications, 3% responded or clicked on a link in the message. 11% of respondents or link-clickers shared personal information susceptible to exploitation by scammers [8].

There are many psychological characteristics that contribute to being a victim of Internet-based fraud [9]. Most of the evaluated research focused on 'phishing' and analysed various elements from personality to heuristics. Most of the information and opinions that exist about the psychological aspects linked to susceptibility to online fraud are mostly anecdotal and might potentially contribute to the formation of erroneous myths, such as the notion that elderly individuals are easy targets. Policies aimed at reducing fraud should acknowledge that compliance is universal and that no one population is inherently more or less susceptible [9]. This is echoed by other authors, who assert that it is crucial to differentiate between the targets of fraudsters, those who fall victim, and the total number of victims within various demographic categories. Fraudsters that focus only on older age groups are more likely to have a higher number of victims from that demographic [1]. A 2009 UK-based study found that in 2009, the average victim of identity theft was more likely to be a man in his late 30s or early 40s than a woman (60:40). Over three-quarters of the victims were between the ages of 25 and 54, with an average victim age of 42 [10].

A study in South Africa concluded that conducting a simulated phishing attack together with integrated training might help enhance users' ability to resist phishing attempts, thereby lowering their vulnerability to future attacks [11]. Interestingly, an analysis of trends in phishing

attacks in 2006 found that phishing incidence decreases significantly on weekends. Additionally, phishers mostly impersonate financial businesses, but they also target other areas such as commerce, community, government, job forums, certificate authorities, and greeting cards [6]. Furthermore, it takes an average of 416 days for fraud victims to recognise they had been a victim [10]. Fraudsters had almost a year to exploit their victims' accounts, accumulate debts, damage their credit scores, and then target new victims. From this same study, the richest residents in the UK are the ones most likely to fall victim to fraud, with an average loss of £1,100 per victim [10].

Within Kazakhstan, few studies have observed the problems of cyber fraud, and more specifically phishing. Some authors have developed suggestions for enhancing victimological criteria to tackle fraud [12]. Consistently alerting the populace about new deception strategies, updating practical recommendations on protecting oneself from fraudsters, and enhancing citizens' legal awareness are suggested to reduce the number of fraud victims in Kazakhstan [12]. Another noteworthy study in this area has utilised several machine learning techniques to forecast instances of fraud, namely credit card and e-commerce fraud. The study concluded that machine learning methods can be utilised to increase the detectability of credit card fraud [13].

Both theoretical and practical components of combating computer technology fraud is examined by some Kazakhstani authors. The research is intended to serve as the basis for revisions to Kazakhstan's laws and the creation of instructional guides for investigating certain criminal offences in law enforcement [14]. To provide efficient strategies to combat fraud, namely housing fraud, using information technology, since theft often originates from cyber assaults on information systems themselves, comprehensive research was conducted by scholars from Kazakhstan [15]. This research used methodologies such as comparative legal analysis and expert review. Proposed amendments to the criminal code of the Republic of Kazakhstan focus on expanding jurisdiction, adding qualifying criteria, and the need of enacting a new Law on real estate business. The authors maintain that an inadequate identification of fraud in the information technology industry in Kazakhstan is due to the operational police units' staff lacking competence in IT technologies. The authors assert that all law enforcement personnel and judges should get basic training on cybercrime and electronic evidence, or as many as practicable. This fundamental information should be included in the initial training of prospective workers and judges, as well as in further training and retraining programmes for existing employees and judges [15].

Based on survey data on young people in Kazakhstan, one study revealed that young people in Kazakhstan are unaware of how to protect themselves from cyber threats, lack knowledge, and misunderstand the importance of cybersecurity [16]. This article also provides recommendations for ensuring cybersecurity, namely the involvement of the state, educational institutions, and the corporate sector in maintaining cybersecurity, along with the significance of international collaboration.

Materials and methods

This study employs a qualitative methodology, centring on the comparative legal analysis of official documents. A search for «phishing» (фишинг) in Russian on the Adilet portal (adilet.zan.kz), Kazakhstan's official repository of legislative and regulatory documents, produced a limited number of results. However, upon closer examination of these documents, it appears that most references do not undertake a substantive discussion of phishing as a distinct form of cybercrime;

rather, they make passing or ancillary mention of the term within broader contexts such as explanations, disclaimers, or notices of risk in general cyber-related regulations and guidelines. None of the identified documents present a dedicated, in-depth legal framework or enforcement mechanism specifically targeting phishing, and the term itself is typically used to illustrate general fraudulent practices involving the unauthorized acquisition of financial or personal data.

This absence of a robust, standalone legal definition or comprehensive policy provisions devoted to phishing suggests that the Kazakhstani legal corpus, as currently indexed on Adilet, has yet to formally codify or elaborate on the precise nature and scope of phishing as a cyber threat. Instead, any legal ramifications for phishing-related activities are subsumed under broader statutes addressing fraud, unauthorised data access, or misuse of information technology. Consequently, the search results highlight a gap in explicit legislative coverage of cyber-enabled social engineering offenses: while authorities recognise and occasionally reference phishing, the lack of tailored statutory language or clear prosecutorial guidelines may hinder consistent enforcement and public awareness efforts. As such, although the documents retrieved allude to phishing in broad, often cautionary terms, they offer limited insight into how Kazakhstani law specifically confronts and prosecutes this rapidly evolving cybercrime.

Following the initial query on Adilet, additional key legal documents were manually searched to shed further light on the scope and treatment of phishing, vishing (voice-based phishing), and online fraud in Kazakhstan. In particular, the Criminal Code of the Republic of Kazakhstan, the national "Cyber Shield" Concept, and the Law of the Republic of Kazakhstan "On Personal Data and Their Protection", among other potentially relevant statutes and policy frameworks, were reviewed. Through the scrutiny of these sources, it was sought to determine whether and to what extent existing legislation explicitly addresses emergent tactics of cybercriminals, provides a coherent prosecutorial basis for such offenses, and includes provisions for victim redress. This broader investigation was also undertaken to yield a more nuanced assessment of any legislative gaps or inconsistencies that may impede the country's efforts to combat cyber-enabled social engineering crimes effectively.

Results and Discussion

The national Cyber Security Concept

The 2017 Government of Kazakhstan Decree No. 407 [17], which approves the national Cybersecurity Concept (commonly referred to as the «Cyber Shield of Kazakhstan», aims to establish a high-level strategic framework for safeguarding the country's digital infrastructure against a broad spectrum of online threats. In principle, the Concept outlines key objectives such as fortifying critical information systems, increasing institutional capacities, and improving public awareness. By emphasising the importance of public-private cooperation and more robust legal provisions, it signals official recognition that cyber threats, from hacking to social engineering, pose significant risks to the nation's socioeconomic stability. However, its treatment of phishing, vishing, and other forms of online fraud remains partial and subsumed under generalised categories of «cyber fraud» and «social engineering», without offering a clear or systematic plan for enforcement, awareness, or remediation. Although the Concept underscores social engineering as an evolving and highly detrimental vector of attack, it does not delineate specific guidelines or penalties for common tactics such as phishing emails, fraudulent phone calls, or SMS-based scams. Instead, it gestures broadly toward the need for collaboration among law

enforcement, telecom operators, and financial institutions, while stopping short of explaining precisely how these stakeholders ought to identify, counteract, and penalise phishing or vishing attempts in everyday practice.

In its vision to create a national «Cyber Shield», the Concept aspires to mobilise a holistic response involving public agencies, private companies, and international partners. Yet the document, being largely conceptual in its orientation, offers little by way of concrete implementation protocols or explicit legal frameworks that would be vital in addressing the increasing prevalence of phone-based fraud, phishing websites, and other internet scams targeting Kazakhstani citizens. The inclusion of measures to enhance digital literacy and promote ongoing training points to an implicit acknowledgment that human error remains a key vulnerability in cyber defence, but even these mentions lack detail regarding scale, target populations, or funding mechanisms. Although the Concept does call for amending existing legal and regulatory structures to address new forms of cybercrime, it does not define essential terms such as phishing or vishing in a manner that would allow for streamlined investigations or consistent enforcement practices across regions. Consequently, while the Concept succeeds in positioning cybersecurity as a national priority, it defers most meaningful action on cyber fraud, particularly in the realm of phishing and vishing, to subsequent regulations or agency-specific decrees, leaving a notable gap between the policy's overarching aspirations and the practical needs of individuals and organisations contending with sophisticated online scams on a daily basis.

Overall, the Concept's vision of bolstering cybersecurity in Kazakhstan is commendable as a guiding framework, yet its language around social engineering threats remains predominantly aspirational and broad. This approach neglects the nuanced complexities of phishing and vishing attacks, which continue to evolve in both technique and scale. By embedding such forms of fraud in a generalised discussion of cyber threats, the document fails to address how existing institutional capacities, and legal mechanisms should be adapted or strengthened to effectively counter these persistent and increasingly sophisticated criminal methods. Moreover, the lack of explicit protocols for public education campaigns, reporting mechanisms, and cross-industry intelligence sharing diminishes the Concept's ability to mitigate real-world threats in an immediate and visible manner. In that sense, while the «Cyber Shield of Kazakhstan» offers a valuable starting point, significant additional legislative and operational steps appear necessary to transform its broad declarations into comprehensive, actionable, and adequately funded measures for defending citizens and organisations against phishing, vishing, and other forms of online fraud.

Law of the Republic of Kazakhstan «On Personal Data and Their Protection»

The 2013 Law of the Republic of Kazakhstan «On Personal Data and Their Protection» (No. 94-V) [18] primarily focuses on regulating the collection, storage, processing, and protection of individuals' personal data. Although it provides definitions and guidelines aimed at safeguarding the confidentiality and integrity of personal information held by various public and private entities, it does not explicitly address specific types of cyber fraud such as vishing or phishing. Instead, it generally stipulates that data controllers and processors must adopt organisational and technical measures to prevent unauthorised access, loss, or misuse of personal data, thereby implying a duty to mitigate security breaches that could occur through fraudulent or criminal acts. This indirect mention of security obligations leaves considerable interpretative room for whether and how the law can be applied to concrete incidents of online fraud, especially those facilitated by social engineering techniques targeting the victim directly, rather than a data controller's databases.

From a critical standpoint, the law's focus on organisational data protection measures, rather than individual scams that exploit users' lack of awareness, underscores a significant gap in addressing the realities of cybercrime in Kazakhstan. While personal data protection is a core concern, the statute's absence of explicit provisions on vishing or phishing suggests that these offenses are subsumed under broader, often imprecise categories of unauthorised data access or fraudulent misuse of personal information. Consequently, enforcement agencies and courts must rely on other criminal or administrative statutes when prosecuting or adjudicating cases of online fraud, potentially complicating the legal process and diluting the specific harm associated with tactics like voice-based deception. In effect, this law provides only a partial framework for securing personal data, offering no dedicated mechanism for redressing the personalised, real-time manipulations, such as vishing, that commonly bypass purely organisational defences.

The Penal Code of the Republic of Kazakhstan

The Penal Code of the Republic of Kazakhstan (No. 226-V, dated 3 July 2014) [19] contains general provisions for criminalising fraud, unauthorised access to information systems, and other offenses that could, in principle, encompass vishing and phishing activities. Most notably, fraud is penalised under broad clauses that prohibit the illegal acquisition of property or property rights through deception or abuse of trust, and certain articles address the misuse of information and communication technologies. Nonetheless, these provisions stop short of explicitly defining or naming phishing, vishing, or analogous social engineering tactics, effectively folding such offenses under traditional fraud classifications. Because the language remains relatively technology-neutral, enforcement authorities are left to interpret whether specific online or phone-based deceptions fit the existing statutory elements, a process that can create legal ambiguities and evidentiary challenges when prosecuting crimes of this nature.

From a critical perspective, the Penal Code's approach highlights a structural gap in adapting legal definitions to the rapidly evolving ecosystem of cybercrime. While incorporating terms such as «electronic information» and «telecommunication networks» signals an acknowledgment of modern-day criminal methods, the absence of dedicated articles or clear sub-provisions specifically addressing phishing or vishing impedes a more nuanced grasp of how these crimes function. In practical terms, victims of sophisticated online fraud, who may be manipulated via phone calls or spoofed emails, are often left with few guidelines for seeking redress under a legal framework that was not designed with these schemes in mind. Consequently, the burden falls on investigators, prosecutors, and courts to interpret technologically diffuse behaviours within older, more generalised fraud statutes, thereby raising the risk of inconsistent enforcement and overlooking the unique harms associated with contemporary forms of cyber-enabled deception.

The Code of the Republic of Kazakhstan on Administrative Offences

The 2014 Code of the Republic of Kazakhstan on Administrative Offences (No. 235-V) [20] provides a framework for penalising a wide variety of non-criminal legal breaches, including some that involve improper use of telecommunications and information systems. While certain clauses could theoretically be invoked in cases of unauthorised data handling or the misuse of telecommunications networks, the text does not explicitly reference phishing, vishing, or other methods of social engineering aimed at extracting confidential information.

Instead, the Code largely covers administrative violations ranging from unlicensed activities to procedural failings by companies and individuals, imposing fines and other non-criminal penalties for infringements. As a result, there is no straightforward mechanism under these provisions for holding perpetrators of cyber-enabled scams administratively liable unless their

actions fit within pre-existing definitions of telecommunication violations or illegal handling of personal data.

Critically, this gap exemplifies a broader systemic challenge in Kazakhstan's legislative environment: social engineering crimes, particularly those executed through phone calls or deceptive emails, are neither distinctly categorised nor clearly delineated under administrative norms. Although the Code could be applied in peripheral areas, such as penalising telecom providers who fail to implement certain cybersecurity protocols, it offers limited avenues for addressing the core misrepresentation and deception at the heart of phishing or vishing schemes. Consequently, the Code's regulatory approach may place undue emphasis on compliance issues rather than on deterring and penalising those who target victims through manipulative online or telephone tactics. Without further legislative refinement, administrative law will continue to offer only fragmentary remedies that fail to capture the unique harm inflicted by these rapidly evolving cyber fraud methods.

Additional statutes and regulatory acts

Beyond the core legal instruments already examined, several additional statutes and regulatory acts in Kazakhstan warrant attention for a more comprehensive analysis of phishing, vishing, and online fraud. In particular, equally pertinent is the Law «On Informatization» [21], which outlines the legal foundations for the development and use of information technologies in Kazakhstan and may shed light on any responsibilities of internet service providers or digital platforms to prevent fraudulent activities. Law «On Electronic Document and Electronic Digital Signature» [22] was also reviewed to understand how electronic transactions and signatures are protected under current regulations, relevant in instances where phishing scams exploit digital credential systems. Additionally, exploring the Law «On Banks and Banking Activities» [23] helped to identify financial-sector obligations to mitigate fraudulent transfers, while official decrees or strategies from the Ministry of Digital Development, Innovations and Aerospace Industry revealed evolving government measures and priorities. Taken together, these documents deepened an understanding of the legal ecosystem governing cyber fraud in Kazakhstan, highlighting both explicit and implied mechanisms that either address or fail to address phishing, vishing, and similar forms of online deception.

Conclusion

It has been demonstrated that although Kazakhstan's legislative frameworks address cyber fraud in general terms, explicit coverage of phishing, vishing, and other social engineering tactics remains inadequate. Existing provisions, which rely on traditional definitions of fraud and unauthorised access, demand interpretive stretching when modern cybercrimes are prosecuted. This reliance on broad categorisation has been noted to create ambiguity, as law enforcement agencies often lack clear guidance on how to classify and investigate deceptive schemes that manipulate human behaviour rather than technical vulnerabilities. The absence of precisely formulated legal definitions also weakens preventive measures, since public awareness campaigns and reporting mechanisms cannot be effectively structured around vague statutory language.

Such gaps are further exacerbated by the rapid emergence of new phishing and vishing techniques, making sporadic legislative updates insufficient to curb evolving criminal methods. It has been observed that while some policy documents, including the "Cyber Shield of

Kazakhstan," acknowledge social engineering threats, they do not prescribe specific remedies or enforcement protocols. Future research is therefore needed to map the full scope of cyber fraud incidents, assess the effectiveness of existing investigative procedures, and explore targeted legislative reforms capable of encompassing the broad array of social engineering tactics. By integrating robust legal definitions with systematic public education initiatives, a more coherent and dynamic approach to safeguarding digital transactions and personal data may be achieved.

The findings of this study imply that researchers and policy analysts must expand traditional understandings of cybercrime to include the unique psychological, technical, and social dynamics of phishing and vishing. Such a shift could encourage interdisciplinary inquiries, blending criminology, law, psychology, and information security, to produce holistic frameworks that address both the technical and human dimensions of modern cyber-fraud.

Conflict of interest

There are no conflicting interests to disclose.

The contribution of the authors

N.S. Temirbolat, S.Sh. Urkumbay, and **R.A. Alshurazova** contributed equally to the preparation and execution of the study. **N.S. Temirbolat** contributed to the research concept, methodology, and preparation of the initial manuscript. **S.Sh. Urkumbay** participated in data collection, literature review, and analysis and interpretation of the findings. **R.A. Alshurazova** contributed to data analysis, formulation of conclusions and recommendations, and final editing of the manuscript.

Funding

This study has not received funding.

References

1. Button M. (2016) Fraud typologies and victims of fraud / Button M., Lewis C., Tapley J. //National Fraud Authority. London, 2016. – Pp. 96.

2. Brenner, S.W. (2004) Cybercrime metrics: old wine, new bottles? // Virginia Journal of Law and Technology. – Vol. 9, No. 13. – Pp. 1-52.

3. Ali M. A. (2019) Consumer-facing technology fraud: Economics, attack methods and potential solutions. / Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., van Moorsel, A. // Future Generation Computer Systems. – Vol. 100. – Pp. 408-427.

4. Zhenisbekova A. (2021). Growing Internet Frauds in Kazakhstan: How to Keep You and Your Money Safe? Central Asian Burau for Analytics Reporting. https://cabar.asia/en/growing-internet-frauds-in-kazakhstan-how-to-keep-you-and-your-money-safe (accessed: 22.12.2024).

5. Aleroud, A. (2017) Phishing environments, techniques, and countermeasures: A survey. /Aleroud, A., Zhou, L. // Computers & Security. – Vol. 68. – Pp. 160-196.

6. Ramzan, Z., Wüest, C. (2007) Phishing Attacks: Analyzing Trends in 2006 // CEAS. Fourth Conference on Email and Anti-Spam (August 2-3, 2007). - Mountain View, California, USA

7. Federal Bureau of Investigation. Washington: Internet Crime Complaint Center. (2023). Internet crime report 2023. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (accessed: 05.11.2024).

8. Office for National Statistics website. Nature of fraud and computer misuse in England and Wales. https://www.ons.gov.uk Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022#:~:text=Estimates%20showed%20there%20were%204.5,%E2%80%9Cconsumer%20and%20retail%20fraud%E2%80%9D (accessed: 05.11.2024).

9. Norris G. (2019) The psychology of internet fraud victimisation: A systematic review / Norris, G., Brookes, A., & Dowell, D. //Journal of Police and Criminal Psychology. – Vol. 34. – Pp. 231-245.

10. Experian (2010). The Insight Report, Victims of Fraud Survey, London. Retrieved from: https://www.experian.co.uk/assets/insight-reports/brochures/The-Insight-Report-Victims-of-fraud-survey-March-2010.pdf (accessed: 21.11.2024).

11. Jansson, K. (2013) Phishing for phishing awareness / Jansson, K., von Solms, R. // Behaviour & Information Technology. – Vol. 32, No. 6. – Pp. 584-593.

12. Ozbekov D.O. (2022) About some issues of victimological prevention of fraud / Ozbekov, D. O., Mashabaev, A. Z., Siubayeva, N. Z. //Bulletin of the Karaganda University Law Series. – Vol. 107, No. 3. – Pp. 54-60.

13. Baitiles R. Y. (2022) DEtecting credit card fraud using machine learning / Baitiles, R. Y., Omarov, B. S. // Международный журнал информационных и коммуникационных технологий. – Vol. 3, No. 4. Pp. 57-69.

14. Temirzhanova L. A. (2019) Countering Fraud Committed Using Information Technology in Kazakhstan / Temirzhanova, L. A., Imangaliev, N. K., Sagymbekov, B. Z., Eshnazarov, A. A., Syzdykov, A. Z. // Journal of Advanced Research in Law and Economics. – Vol. 10, No. 45. – Pp. 2122-2132.

15. Temirzhanova, L.A. (2018) Improving the Mechanism of Countering Certain Types of Fraud in the Republic of Kazakhstan / Temirzhanova, L. A., Imangaliev, N. K., Syzdykov, A. Z., Eshnazarov, A. A., & Sagymbekov, B. Z. // Journal of Advanced Research in Law and Economics. – Vol. 9, No. 35. – Pp 1776-1788.

16. Джекебаева, М. (2023). Cybersecurity: importance for Kazakhstan and international experiences / Джекебаева, М., Изтаева, В., Анасова, К., & Манапбаев, Н. // Известия. Серия: Международные отношения и Регионоведение. – 2023. – Vol. 54(4). – Pp. 1-10.

17. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. «Об утверждении Концепции кибербезопасности» («Киберщит Казахстана»). Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407 (accessed: 05.01.2025)

18. The Law of the Republic of Kazakhstan dated 21 May 2013 No. 94-V. On Personal Data and Their Protection. Available at: https://adilet.zan.kz/eng/docs/Z1300000094 (accessed: 05.01.2025)

19. Penal Code of the Republic of Kazakhstan. 3 July 2014 No. 226-V. Available at: https://adilet.zan.kz/eng/docs/K1400000226 (accessed: 05.01.2025)

20. The Code of the Republic of Kazakhstan dated 5 July 2014 No. 235-V. On Administrative Infractions. Available at: https://adilet.zan.kz/eng/docs/K1400000235 (accessed: 05.01.2025)

21. The Law of the Republic of Kazakhstan dated 24 November 2015 № 418-V. On informatization. Available at: https://adilet.zan.kz/eng/docs/Z1500000418 (accessed: 06.01.2025)

22. The Law of the Republic of Kazakhstan dated 7 January 2003 No.370. On Electronic Document and Electronic Digital Signature. Available at: https://adilet.zan.kz/eng/docs/Z030000370_ (accessed: 06.01.2025)

23. The Law of the Republic of Kazakhstan dated 31 August 1995 № 2444. On Banks and Banking Activities. Available at: https://adilet.zan.kz/eng/docs/Z950002444_#:~:text=Banking%20operations%20carried%20out%20without,Law%2C%20as%20well%20as%20the (accessed: 06.01.2025)

References

1. Button M. (2016) Fraud typologies and victims of fraud / Button M., Lewis C., Tapley J. //National Fraud Authority. London, 2016. – P. 96.

2. Brenner, S. W. Cybercrime metrics: old wine, new bottles? // Virginia Journal of Law and Technology. – 2004. – Vol. 9, No. 13. – P. 1-52.

3. Ali M. A. Consumer-facing technology fraud: Economics, attack methods and potential solutions. / Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., van Moorsel, A. // Future Generation Computer Systems. – 2019. – Vol. 100. – P. 408-427.

4. Zhenisbekova, A. (2021). Growing Internet Frauds in Kazakhstan: How to Keep You and Your Money Safe? Central Asian Bureau for Analytics Reporting. https://cabar.asia/en/growing-internet-frauds-in-kazakhstan-how-to-keep-you-and-your-money-safe (accessed: 22.12.2024).

5. Aleroud A. (2017) Phishing environments, techniques, and countermeasures: A survey. /Aleroud, A., Zhou, L. // Computers & Security. – Vol. 68. – P. 160-196.

6. Ramzan, Z., Wüest, C. (2007) Phishing Attacks: Analyzing Trends in 2006 // CEAS Fourth Conference on Email and Anti-Spam (August 2-3, 2007). - Mountain View, California, USA

7. Federal Bureau of Investigation. Washington: Internet Crime Complaint Center. (2023). Internet crime report 2023. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (accessed: 05.11.2024).

8. Office for National Statistics website. Nature of fraud and computer misuse in England and Wales. https://www.ons.gov.uk Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022#:~:text=Estimates%20showed%20there%20were%204.5,%E2%80%9Cconsumer%20and%20retail%20fraud%E2%80%9D (accessed: 05.11.2024).

9. Norris G. (2019) The psychology of internet fraud victimisation: A systematic review / Norris, G., Brookes, A., & Dowell, D. //Journal of Police and Criminal Psychology. – Vol. 34. – P. 231-245.

10. Experian (2010) The Insight Report, Victims of Fraud Survey, London. Retrieved from: https://www.experian.co.uk/assets/insight-reports/brochures/The-Insight-Report-Victims-of-fraud-survey-March-2010.pdf (accessed: 21.11.2024).

11. Jansson, K. (2013) Phishing for phishing awareness / Jansson, K., von Solms, R. // Behaviour & Information Technology. - Vol. 32, No. 6. – P. 584-593.

12. Ozbekov D. O. (2022) About some issues of victimological prevention of fraud / Ozbekov, D. O., Mashabaev, A.Z., Siubayeva, N.Z. //Bulletin of the Karaganda University Law Series. – Vol. 107, No. 3. – Pp. 54-60.

13. Baitiles R. Y. (2022) Detecting credit card fraud using machine learning / Baitiles, R. Y., Omarov, B. S. // Mezhdunarodnyj zhurnal informacionnyh i kommunikacionnyh tekhnologij. – Vol. 3, - No. 4. - Pp. 57-69.

14. Temirzhanova L. A. (2019) Countering Fraud Committed Using Information Technology in Kazakhstan / Temirzhanova, L. A., Imangaliev, N. K., Sagymbekov, B. Z., Eshnazarov, A. A., Syzdykov, A. Z. // Journal of Advanced Research in Law and Economics. –. – Vol. 10, No. 45. – P. 2122-2132.

15. Temirzhanova, L. A. (2018) Improving the Mechanism of Countering Certain Types of Fraud in the Republic of Kazakhstan / Temirzhanova, L. A., Imangaliev, N. K., Syzdykov, A. Z., Eshnazarov, A. A., & Sagymbekov, B. Z. // Journal of Advanced Research in Law and Economics. –. – Vol. 9, No. 35. – P. 1776-1788.

16. Dzhekebaeva, M. (2023). Cybersecurity: importance for Kazakhstan and international experiences / Dzhekebaeva, M., Iztaeva, V., Anasova, K., & Manapbaev, N. // Izvestiya. Seriya: Mezhdunarodnye otnosheniya i Regionovedenie. – 2023. – Vol. 54(4). – P. 1-10.

17. Postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 iyunya 2017 goda № 407. «Ob utverzhdenii Koncepcii kiberbezopasnosti» («Kibershchit Kazahstana»): https://adilet.zan.kz/rus/docs/P1700000407 (accessed: 05.01.2025)

18. The Law of the Republic of Kazakhstan dated 21 May 2013 No. 94-V. On Personal Data and Their Protection: https://adilet.zan.kz/eng/docs/Z1300000094 (accessed: 05.01.2025)

19. Penal Code of the Republic of Kazakhstan. 3 July 2014 No. 226-V: https://adilet.zan.kz/eng/docs/K1400000226 (accessed: 05.01.2025)

20. The Code of the Republic of Kazakhstan dated 5 July 2014 No. 235-V. On Administrative Infractions. Режим доступа: https://adilet.zan.kz/eng/docs/K1400000235 (accessed: 05.01.2025)

21. The Law of the Republic of Kazakhstan dated 24 November 2015 № 418-V. On informatization: https://adilet.zan.kz/eng/docs/Z1500000418 (accessed: 06.01.2025)

22. The Law of the Republic of Kazakhstan dated 7 January 2003 No.370. On Electronic Document and Electronic Digital Signature: https://adilet.zan.kz/eng/docs/Z030000370_ (accessed: 06.01.2025)

23. The Law of the Republic of Kazakhstan dated 31 August 1995 № 2444. On Banks and Banking Activities:https://adilet.zan.kz/eng/docs/Z950002444_#:~:text=Banking%20operations%20carried%20out%20without,Law%2C%20as%20well%20as%20the (accessed: 06.01.2025)

Information about the authors:

***Temirbolat N.S.* –** candidate of Law Sciences, Senior Lecturer, Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, 71, Al-Farabi Avenue, 050040, Almaty, Kazakhstan

Urkumbay S.Sh. – corresponding author, 2 and-year PhD Student, Faculty of Law, Al-Farabi Kazakh National University, 71, Al-Farabi Avenue, 050040, Almaty, Kazakhstan

***Alshurazova R.A.* –** Master of Laws, Senior Lecturer, M.Auezov South Kazakhstan University, 5, Tauke Khan Avenue, 160012, Shymkent, Kazakhstan

***Темірболат Н.С.* –** заң ғылымдарының кандидаты, аға оқытушы, қылмыстық құқық, қылмыстық процесс және криминалистика кафедрасы, әл-Фараби атындағы Қазақ ұлттық университеті, әл-Фараби даңғылы, 71, 050040, Алматы, Қазақстан

***Үркүмбай С.Ш.* –** хат-хабар үшін автор, 2-курс докторанты, заң факультеті, әл-Фараби атындағы Қазақ ұлттық университеті, әл-Фараби даңғылы, 71, 050040, Алматы, Қазақстан

***Альшуразова Р.А.* –** заң ғылымдарының магистрі, аға оқытушысы, Әуезов атындағы Оңтүстік Қазақстан университеті, Тәуке хан даңғылы, 5, 160012, Шымкент, Қазақстан

Темирболат Н.С. – кандидат юридических наук, старший преподаватель, кафедра уголовного права, уголовного процесса и криминалистики, Казахский национальный университет имени аль-Фараби, пр. аль-Фараби, 71, 050040,Алматы, Казахстан

Үркүмбай С.Ш. – автор для корреспонденции, докторант 2-го курса, юридический факультет, Казахский национальный университет имени аль-Фараби, пр. аль-Фараби, 71, 050040, Алматы, Казахстан

Альшуразова Р.А. – магистр права, старший преподаватель, Южно-Казахстанский университет имени М. Ауэзова, проспект Тауке хана, 5, 160012, Шымкент, Казахстан

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (https://creativecommons.org/licenses/by-nc/4.0/).