



DIGITAL SECURITY AND THREATS IN KAZAKHSTAN

Digital fraud has been a persistent issue for decades, with its origins tracing back to the early 1970s when email phishing first emerged, even though the term itself was not coined, and the practice did not gain widespread prevalence until the mid-1990s. Since then, the online world has seen scammers try their hand at everything from fake email addresses to exploiting information obtained from major data breaches [Strandell, 2024]. But email isn't the only digital channel that's been hacked. The earliest mobile phone scams emerged in the turbulent 1980s, and their prevalence skyrocketed in the 1990s. For example, phone owners receive text messages asking them to "quickly send" funds to a family member's account. Password theft, website hacks, and spyware among other things have spread around the world at an alarming rate during this time.

One of the biggest challenges we face today is the ease with which online fraud can occur. Hackers are evolving their skills to keep up with advances in technology. A recent Microsoft survey found that internet users worldwide are most concerned about fakes, scams, and abuse. 71% of respondents from 17 countries surveyed by Microsoft in July and August 2023 were "very or somewhat concerned" about AI-powered fraud. It is most likely to involve impersonating someone in the spotlight, a government official, or a close acquaintance of the respondent. Deepfakes and sexual or online abuse come in second at 69%. AI hallucinations, defined as chatbots like ChatGPT that provide nonsensical responses rank fourth. Data privacy concerns rank fifth at 62 percent [Strandell, 2024]. In the UK, research shows that more than a third (36%) of people have fallen victim to scams playing on fears of infection during quarantine [Safonov, 2022]. In the US, consumers lost \$10 billion to fraud in 2023 – a new record, according to data released by the Federal Trade Commission, and \$1 billion more than in 2022. Imposter scams, where criminals pose as government officials or legitimate businesses, top the list of fraud categories [Delling, 2024].

This problem is extremely relevant today for Kazakhstan as well. According to the police, in 2023, citizens of Kazakhstan suffered damages in the amount of more than 17.5 billion tenge due to the actions of digital fraudsters [Smagulov, 2023]. In 2024, 11,765 cases of Internet fraud were registered, which is 152 more cases than in the same period last year [Kazakhstan today, 2024].

There are several types of digital crime:

Social engineering uses deception and emotional manipulation to influence another person's behavior. In the digital world, cybercriminals use social engineering tactics to trick people into revealing sensitive information or taking actions that could cause them or their employers financial harm. They can even influence elections or manipulate financial markets.

Phishing is a social engineering tactic that relies on fraudulent emails to lure recipients into sending money or disclosing sensitive information. Many emails ask recipients to click on a link or download an attachment, but either action can lead to unintended consequences, such as being redirected to a malicious website, running a computer virus, or downloading dangerous software.

With spear phishing, scammers do their research before initiating contact, so they may address the victim by name or pose as a representative of a company or person the victim knows. Vishing is a form of phishing that uses phone calls or voice messages, while smishing is done via SMS [Delling, 2024].

Even those trained to be cautious can fall victim to deception, as illustrated by a recent incident in Hong Kong, where a multinational financial services company lost \$25.6 million. An employee transferred corporate funds to a criminal account following a fake video conference featuring individuals who appeared and sounded like colleagues—including the company's CFO—but were actually computer-generated. The ability to use AI to create convincing images, videos, or voices of others introduces new opportunities for digital crime [Chen and Magramj, 2024].

What can be done to combat digital criminals? Some experts believe that analytical thinking provides resilience to fraudulent websites [Shang et al., 2023], as well as systematic actions to improve cyber resilience.

In March 2023, the Kazakh government approved the Concept of Digital Transformation, Development of the Information and Communication Technologies and Cybersecurity Industry for 2023-2029, which plans to further develop the National Coordination Center for Cybersecurity, previously created within the framework of the Cyber Shield of Kazakhstan program. It is also planned to create a cyber training ground for training information security specialists [Avezova, 2024].

According to the international rating of 194 countries' readiness for cyberattacks in 2024, Kazakhstan demonstrated significant progress, rising to the second level out of five, which confirms its successful development in the field of cybersecurity [The Tech, 2024]. A sociological study on information security and personal data protection highlights that 80.4% of Kazakhstan's population is aware of existing threats to cybersecurity and personal data. The study also found that 74.64% of respondents can recognize phishing attempts, and 90.52% are knowledgeable about protecting personal information on social media. These results demonstrate positive progress in raising public awareness in this field.

However, the challenges in this area call for continuous improvement of measures and mechanisms to ensure the sustainable protection of citizens' interests in the digital age. Overall, the findings underscore the growing significance of information security in the daily lives of Kazakhstan's citizens. In this regard, considering the conducted sociological survey, the research group developed relevant recommendations and proposals for further ensuring the security of citizens and protecting their data in the digital space [gov.kz, 2023]. On December 11, 2023, a new protection system was introduced, which provides for a legislative ban on the collection and processing of copies of identity documents containing personal data; by Article 56 of the Law of the Republic of Kazakhstan «On Informatization», persons possessing this information are obliged to take measures to protect it by this Law [egov.kz, 2023].

In addition to following the legal framework and government recommendations, individuals must remain vigilant and proactive about data security. Key steps include:

Keeping computers and mobile devices updated is one of the most effective measures for protecting digital devices, using strong, unique passwords for each account, updating them regularly, and opting for the longest possible passwords. Enabling multi-factor authentication (MFA) on all accounts for an extra layer of security. Exercising caution when clicking on links, opening attachments, or sharing sensitive information. Before entering personal details, such as credit card information, ensure the website uses HTTPS (the "S" stands for "secure"). Backing up data on both computers and mobile devices. Shopping only on trusted websites and checking customer reviews beforehand. Discussion of online safety with children and family members. Staying in control of personal information and financial records. Regularly review privacy settings on online accounts to manage who can access your data and report fraud immediately.

By adopting these practices, citizens can take an active role in safeguarding their digital security. The growing level of digital crimes in Kazakhstan and around the world requires a comprehensive approach. It is important to combine government measures, educational initiatives, and the personal responsibility of citizens. This is the only way to ensure sustainability and protection from digital threats in the era of high technology.

References:

- Avezova, Yana (2024). Current cyber threats in the CIS countries 2023-2024. Retrieved from <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id6>. Accessed on 17.12.2024.
- Chen, Heather and Kathleen, Magramo (2024). Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'. Retrieved from <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html#:~:text=A%20finance%20worker%20at%20a,according%20to%20Hong%20Kong%20police>. Accessed on 22.12.2024.
- Delling, Dianna (2024). Fraud prevention. Your guide to identifying social engineering scams and cyber threats. Retrieved from <https://newsroom.mastercard.com/news/perspectives/2024/your-guide-to-identifying-social-engineering-scams-and-cyber-threats/>. Accessed on 11.12.2024.
- Egov.kz (2023). Cybersecurity issues. Retrieved from https://egov.kz/cms/sites/default/files/rekomendacii_2023.pdf. Accessed on 11.12.2024.
- Kazakhstan today (2024). The number of cases of Internet fraud has increased in Kazakhstan. Retrieved from https://www.kt.kz/rus/crime/v_kazahstane_vozroslo_kolichestvo_faktov_1377968514. Accessed on 12.12.2024.
- Safonov, Vladimir and Andreev, Dmitri (2022). «Pandemic Fraud»: New Ways of Theft. Bulletin of the Volga University named after V.N. Tatishchev, vol.1, № 2 (101), 177-184. Retrieved from <https://cyberleninka.ru/article/n/moshennichestvo-ot-pandemii-novye-sposoby-hischeniy> Accessed on 12.12.2024.
- Shang, Yuxi, Wang, Kaije, Tian, Yuye, Zhou, Yingyu, Ma, Beibei and Liu, Sanyang (2023). Theoretical basis and occurrence of internet fraud victimization: Based on two systems in decision-making and reasoning. Retrieved from <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1087463/full> Accessed on 11.12.2024.
- Smagulov, Aset (2024). The number of cases of online fraud in Kazakhstan has increased tenfold over the past seven years. Retrieved from <https://ulysmmedia.kz/news/24758-v-desiat-raz-vozslo-kolichestvo-internet-moshennichestva-v-kazahstane-za-poslednie-sem-let/>. Accessed on 11.12.2024.
- Strandell, Jonas (2024). The evolution of online scams. Retrieved from <https://besedo.com/blog/the-evolution-of-online-scams-moderation-methods/> Accessed on 11.12.2024.
- The Tech (2024). Kazakhstan strengthens its position in global cybersecurity ranking 2024. Retrieved from <https://the-tech.kz/kazakhstan-ukrepil-poziczii-v-globalnom-rejtinge-kiberbezopasnosti-2024/#:~:text=%>. Accessed on 22.12.2024.