**Кому:** Правительству Республики Казахстан.

**Ф.И.О и должность автора**: Ашимов Ерхан Ержанулы – ведущий специалист отдела финансового обеспечения.

**Дата:** 13.03.2025

**Аналитическая записка**

**Тема:** Интернет – мошенничество: угрозы, схемы и способы защиты.

**Ключевые слова**: кибеугрозы, мошенничество, социальная инженерия.

## Введение

В современном мире интернет-мошенничество стало одной из самых актуальных угроз для пользователей сети. С развитием цифровых технологий мошенники используют всё более изощренные схемы, направленные на кражу личных данных, финансовых средств и даже цифровой идентичности.

В данном аналитической записке будут рассматриваться:

- Основные виды интернет-мошенничества;
- Статистика по интернет-мошенничеству;
- Рекомендации по защите и снижению уровня интернет-афер в Казахстане.

Цель данной работы — анализ интернет-мошенничества в Казахстане, выявление основных угроз и мошеннических схем, а также разработка рекомендаций по усилению защиты граждан и повышению эффективности мер противодействия киберпреступности.

Методология: анализ статистических данных о киберпреступлениях МВД РК, статистические исследования.

## Основная часть

Современные интернет-мошенники используют различные схемы, направленные на обман пользователей и кражу их личных данных, финансовых средств и цифровой идентичности. С каждым годом преступники становятся все более изобретательными, применяя новые методы социальной инженерии, технологии подделки и цифровые инструменты. Рассмотрим наиболее распространенные виды киберафер.

В законодательстве Республики Казахстан не предусмотрено определение терминам – Кибератака и интернет мошенничество, по этому будут использованы термины зарубежных стран.

**Кибератаки** — это попытки получить несанкционированный доступ к компьютерным системам и украсть, изменить или уничтожить данные.

**Интернет-мошенничество** — вид мошенничества с использованием Интернета. Оно может включать в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства.

1. **Фишинг** – один из самых распространенных видов мошенничества, при котором злоумышленники отправляют поддельные письма или сообщения от имени известных компаний, банков или государственных учреждений, маскировка под популярные сайты. Их цель – заставить пользователя перейти по фальшивой ссылке и ввести конфиденциальные данные (логины, пароли, номера карт).

**Пример 1:**

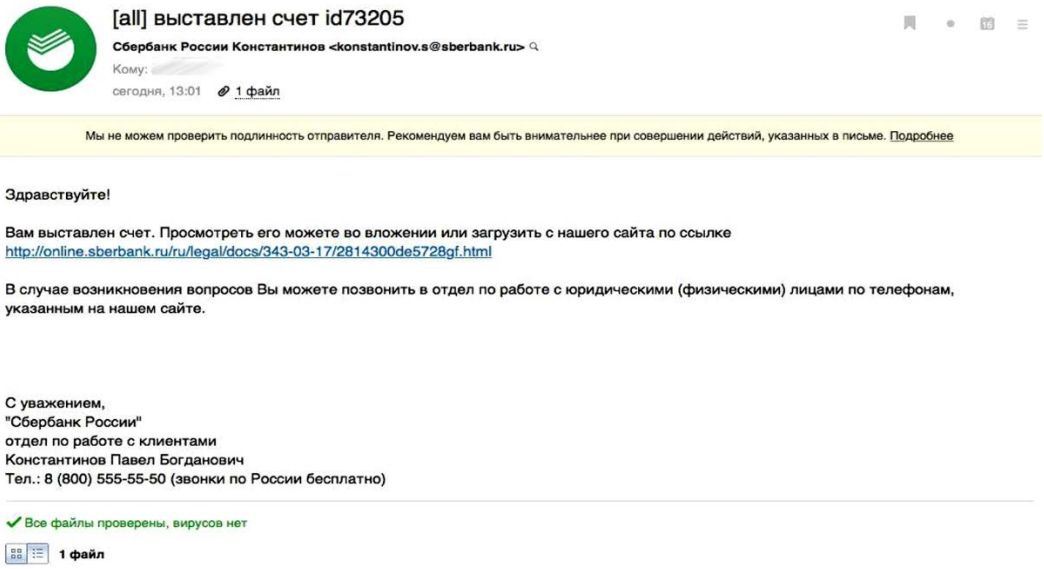


*Рисунок – 1 пример фишинга № 1.*

- *Жертва получает письмо якобы от банка с просьбой подтвердить данные карты, после чего злоумышленники получают доступ к ее счету.*

**Пример 2:**

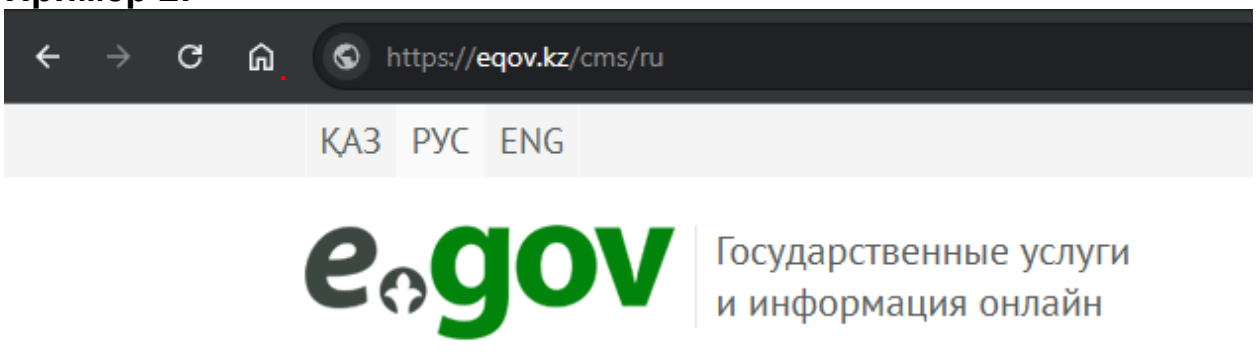


*Рисунок – 2 пример фишинга №2.*

- *Мошенники могут полностью скопировать сайт, но изменив одну букву в ссылке, чтобы невнимательные пользователи не заметили разницы.*

2. **Вишинг (голосовой фишинг)** – мошенники звонят жертве, представляясь сотрудниками банка, полиции или технической поддержки, и под разными предлогами пытаются выманить важные данные или заставить совершить перевод средств. Звонки под видом сотрудников КНБ, Нацбанка и полиции. Такие звонки чаще нацелены на людей зрелого возраста, так как мошенникам легче убедить эту категорию граждан

**Пример** : "Звонок от следователя" (схема на страхе и угрозах). Одной нашей пожилой клиентке позвонили якобы из КНБ. Мошенники представились следователями и в течение трех дней запугивали ее, утверждая, что на нее и ее родственников заведут уголовное дело, если она не поможет "поймать настоящих мошенников". Для этого ей нужно было снять все свои сбережения с депозита, около 10 млн тенге, и перевести на счета, указанные "следователями".[1]

3. **Ложные инвестиционные проекты** – мошенники обещают высокий доход от вложений в криптовалюту, акции или стартапы, но на деле это финансовая пирамида.

**Пример**: "Быстрый заработок на инвестициях" (схема на жажде легкой наживы). Молодому человеку в соцсетях попалась реклама псевдоинвестиционной компании с обещанием 300% годовых. Перейдя по ссылке, он оставил свои контактные данные. Вскоре ему перезвонил "менеджер" компании, который убедительно рассказал о невероятных перспективах и быстром обогащении. Ему даже был предоставлен "личный кабинет" с графиками, демонстрирующими рост его "инвестиций". Поверив в сказку, клиент вложил крупную сумму, оформленную в кредит, чтобы увеличить свой "доход". Разумеется, никаких реальных инвестиций не было, а "личный кабинет" оказался созданной под него фикцией. Когда клиент попытался вывести деньги, связь с "менеджером" прервалась.

4. **Обман на маркетплейсах и в интернет-магазинах** – фальшивые продавцы размещают объявления о продаже товаров, требуя предоплату, но после получения денег исчезают.

**Какие психологические методы используют мошенники, чтобы убедить людей поделиться информацией и перевести деньги?**

Мошенникам важно зацепить клиента, завладеть его вниманием. Они используют несколько основных психологических приемов:

**Первый** – это введение человека в состояние страха, паники и даже угрозы.

**Второй метод** – это мотивация быстрого заработка. Мошенники предлагают легкие деньги, обещая высокий доход от инвестиций, финансовых пирамид или участия в каких-либо акциях.

---

1. [1] Противодействие интернет мошенничеству. https://www.zakon.kz/finansy/6467964-moy-otvet--slovo-net-kak-evraziyskiy-bank-pomogaet-davat-otpor-moshennikam.html

**И третий фактор**, который, к сожалению, играет на руку мошенникам, – это недостаточная финансовая грамотность населения и их неосмотрительность, особенно среди пожилых людей.

Статистические данные по случаем мошенничества в Казахстане:

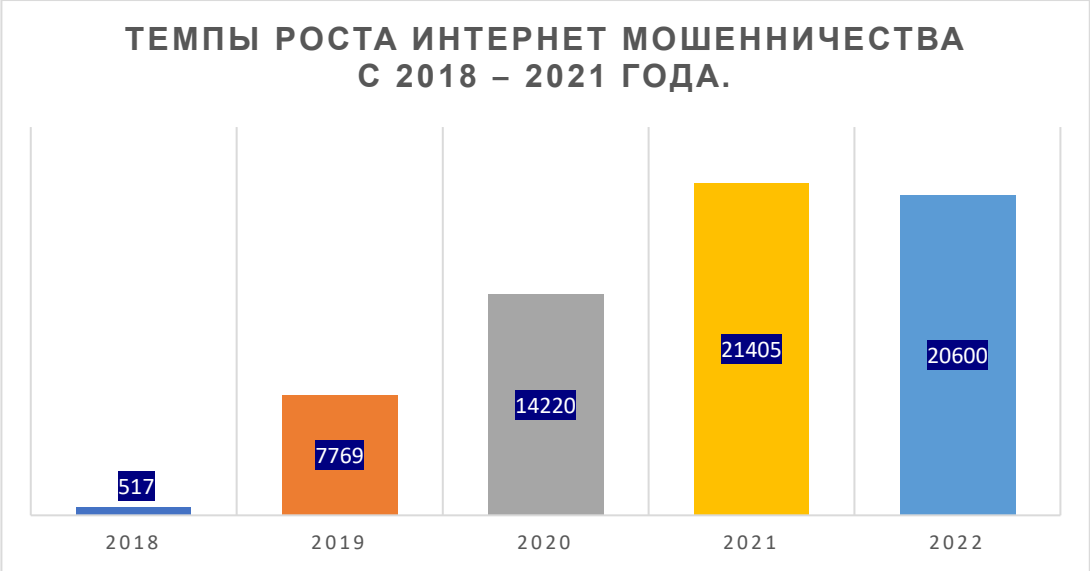


*График – 1 Темпы роста мошенничества.*[2]

Наблюдая рост регистрации интернет мошенничеств, можно сделать вывод, с одной стороны, о недостаточности и малоэффективности проводимых мер по предупреждению и профилактике данных деяний; с другой стороны, о доверчивости и правовой неграмотности граждан, бесконтрольном распространении мошеннических мобильных приложений, об открытой рекламе финансовых интернет-пирамид, малоэффективности существующих мер киберзащиты платёжных интернет-платформ, нехватке специалистов по кибербезопасности и др.

В результате мошеннических действий в **2023 году** пострадало **34 623** лица из них **15616** или же **45%** фактов **интернет-мошенничества.**

[2] ОСОБЕННОСТИ ДИНАМИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН И ЕЕ ВЛИЯНИЕ НА ВОПРОСЫ ЕЁ ПРЕДУПРЕЖДЕНИЯ А.Д. Мухамеджанова Карагандинская академия Министерства внутренних дел Республики Казахстан имени Б. Бейсенова (Караганда, Казахстан)

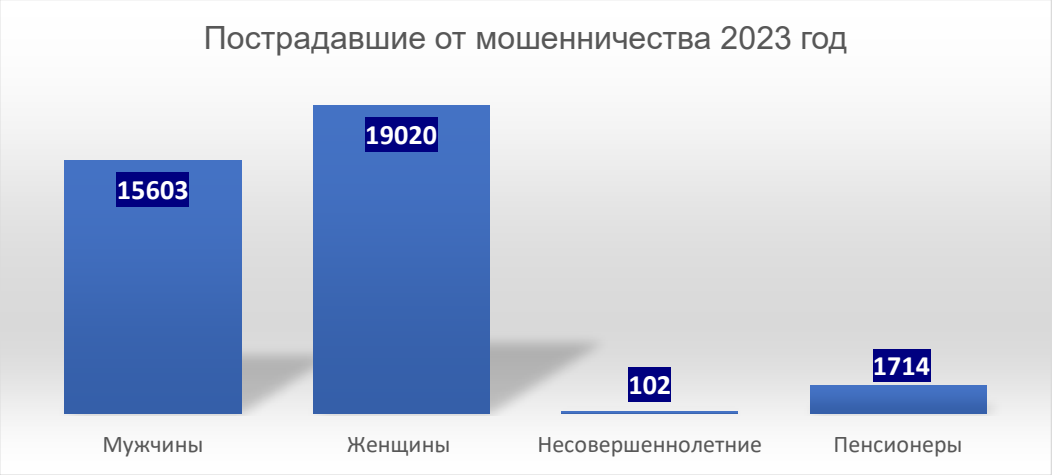


*График -2 Пострадавшие от мошенничества за 2023 год.*

В первой половине **2024** года в Казахстане зарегистрировано **9936 случаев интернет-мошенничества**, что на **4,1%** больше, чем за тот же период **2023** года.

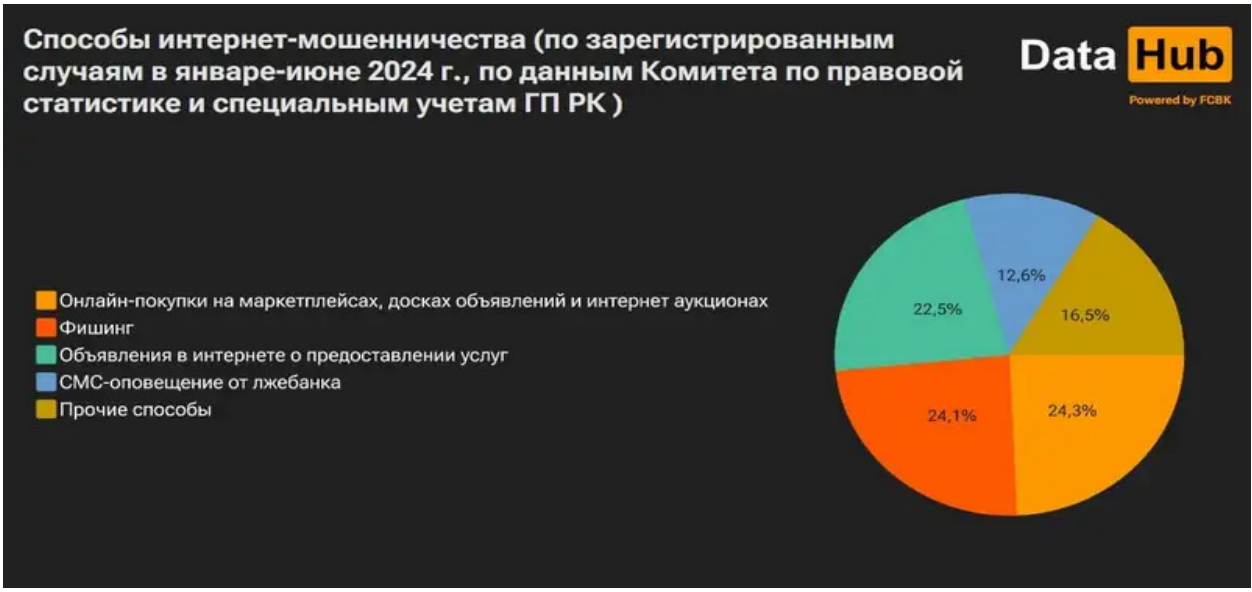


*Рисунок – 3 способы интернет мошенничества.*[3]

В целом, в 2024 году киберпреступность в Казахстане достигла новых высот, с многочисленными утечками данных и кибератаками на государственные учреждения и частный сектор. Эти данные подчеркивают необходимость усиления мер по защите граждан от интернет-мошенничества и повышения осведомленности населения о киберугрозах.

Согласно последнему исследованию **Visa Stay Secure 2023**, проведенному **Wakefield Research**, **63% казахстанцев** не уверены, что способны распознать онлайн-мошенничество. **А 7 из 10 казахстанцев**

[3] Интернет-мошенничество: как и где чаще всего обманывают граждан.

обеспокоены тем, что их друзья или близкие могут отреагировать на мошенническое сообщение.

Вот основные выводы исследования Visa Stay Secure 2023:

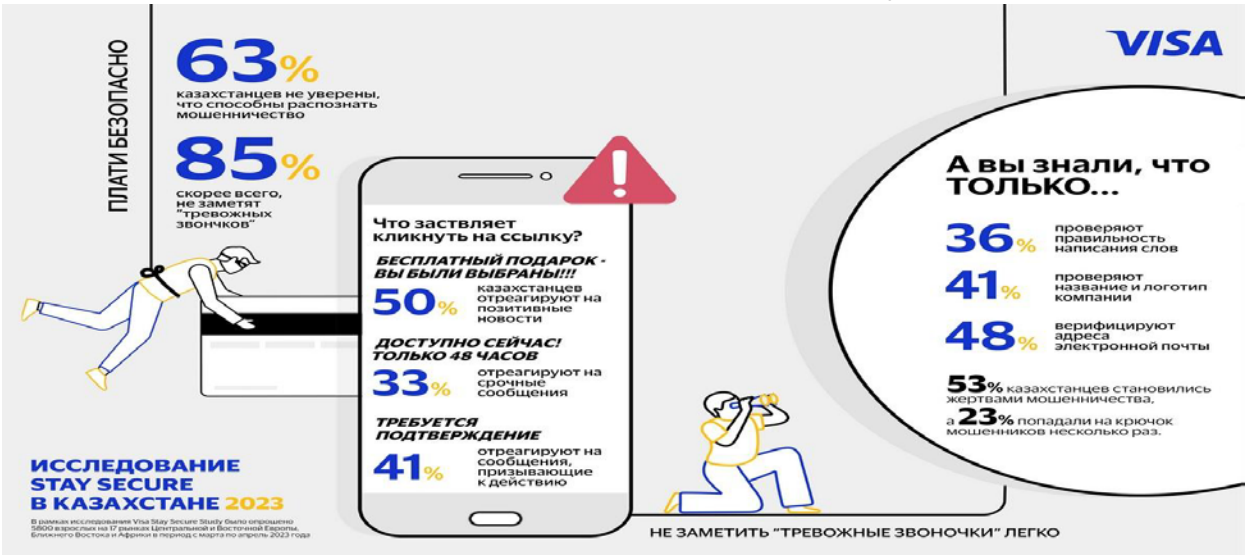


*Рисунок -4 результат Visa stay secure 2023*[4]

**Вывод:**

**Какие меры Казахстану можно внедрить для борьбы с интернет-мошенничеством?**

Казахстан сталкивается с ростом интернет-мошенничества, и для его эффективного снижения можно внедрить **лучшие международные практики**, адаптировав их к местным реалиям.

1. Ужесточение законодательства и регулирование интернет-платформ

**В краткосрочной перспективе:**

- Ввести **обязательную верификацию пользователей** на маркетплейсах и в соцсетях (как в Великобритании).
- *Снижение случаев мошенничества на маркетплейсах на **20%.***
- Обязать **банки и операционные компании** блокировать счета, связанные с мошенническими схемами (как в Китае).
- ***Cybersecurity Law of China (2017)** – регулирует работу интернет-компаний и кибербезопасность. Благодаря этим мерам уровень киберпреступности в Китае снизился на **30%** в 2023 году.*
- **Ограничение покупки SIM-карт без идентификации** (чтобы мошенники не могли массово использовать "одноразовые" номера).
- **Внедрение Caller ID Protection** – автоматическое определение звонков от официальных номеров банков (как в США и ЕС).
- *В **2023** году заблокировано более **2 млрд** нежелательных звонков. В сумме **8,5 млн** часов спама и мошеннических звонков.*

[4] Основные выводы исследования Visa Stay Secure 2023.

- **SMS-уведомления от банков** – предупреждения клиентам о новых схемах мошенничества

**В долгосрочной перспективе:**

2. Повышение цифровой грамотности населения.

- Создать **национальную образовательную кампанию** о киберугрозах.
- Внедрить **уроки цифровой безопасности** в школьную программу.

**Заключение**

Для эффективной борьбы с интернет-мошенничеством в Казахстане необходимо усилить законодательство, внедрив обязательную верификацию пользователей и ужесточив наказания, использовать современные технологии, создать национальный реестр мошеннических номеров и сайтов, а также развивать просветительские кампании для повышения цифровой грамотности населения. Только комплексный подход с участием государства, банков, операторов связи и общества поможет значительно снизить уровень киберпреступности.

**Ожидаемый результат:**

**1.** Снижение уровня интернет-мошенничества.

**2.** Повышение уровня цифровой грамотности населения.

**3.** Проведение мероприятии по предотвращению интернет-мошенничества.

**Использованные источники**

1. ОСОБЕННОСТИ ДИНАМИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН И ЕЕ ВЛИЯНИЕ НА ВОПРОСЫ ЕЁ ПРЕДУПРЕЖДЕНИЯ А.Д. Мухамеджанова Карагандинская академия Министерства внутренних дел Республики Казахстан имени Б. Бейсенова (Караганда, Казахстан) - https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya/viewer

2. Основные выводы исследования Visa Stay Secure 2023 - https://digitalbusiness.kz/2023-09-14/63-kazahstanczev-ne-uvereny-chto-sposobny-raspoznat-onlajn-moshennichestvo/?utm_source=chatgpt.com

3. https://www.zakon.kz/finansy/6467964-moy-otvet--slovo-net-kak-evraziyskiy-bank-pomogaet-davat-otpor-moshennikam.html

4. Противодействие киберпреступности https://www.gov.kz/memleket/entities/qriim/activities/25086?lang=ru

5. Интернет-мошенничество: как и где чаще всего обманывают граждан - https://www.zakon.kz/finansy/6441298-internetmoshennichestvo-kak-i-gde-chashche-vsego-obmanyvayut-grazhdan.html