Кому: Министерству цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
ФИО и должность автора: Али Дильназ, эксперт Департамента социальной сферы Агентства по стратегическому планированию и реформам Республики Казахстан
Дата: 18.02.2025

АНАЛИТИЧЕСКАЯ ЗАПИСКА

Тема: Современные угрозы цифровой безопасности: борьба с фишингом и телефонным мошенничеством

Ключевые слова: Цифровизация, киберпреступность, фишинг, телефонное мошенничество, кибербезопасность.

Введение

«Широкое проникновение цифровых технологий в повседневную жизнь людей сопровождается ростом количества разного рода мошенничеств. Мы это уже видим. Поэтому в современных реалиях знание основ экономики и финансов, обладание элементарными цифровыми навыками становится особенно важным», - отметил глава государства Касым-Жомарт Токаев [1].

Стремительное развитие цифровизации в Казахстане привело к росту киберпреступности, в частности, в сфере фишинга и телефонного мошенничества. Подобные мошеннические схемы наносят значительный ущерб обычным гражданам и финансовым учреждениям, подрывают доверие к цифровым услугам и создают угрозы для национальной кибербезопасности.

В этой записке разбираются методы, которыми пользуются мошенники, их влияние на общество, а также предлагаются меры противодействия, ориентированные на Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан *(далее – МЦРИАП РК)*.

Основная часть

Фишинг

Одним из наиболее распространенных видов киберпреступности является фишинг, при котором злоумышленники рассылают заведомо ложные сообщения, внешне имитирующие официальную коммуникацию от доверенных организаций. Чаще всего такие сообщения поступают по электронной почте или в виде текстовых уведомлений. Основной целью мошенников является незаконное получение конфиденциальных данных, включая учетные записи пользователей и финансовую информацию, хищение денежных средств или заражение устройств жертвы вредоносным программным обеспечением.

Согласно информации Министерства внутренних дел Республики Казахстан, в период с января по сентябрь 2024 года на территории Казахстана было зарегистрировано свыше 15,9 тыс. случаев интернет-мошенничества, что составляет приблизительно 47% от общего числа мошеннических преступлений, зафиксированных за данный период (33 832). Общий материальный ущерб, причиненный данными преступлениями, оценивается в размере около 26 млрд тенге [2].

По данным Комитета по правовой статистике и специальным учетам Генеральной Прокуратуры РК, за первое полугодие 2024 года в Казахстане было выявлено 9 936 случаев интернет-мошенничества, что на 4% больше, чем за соответствующий период 2023 года. Вторым по распространенности видом интернет-мошенничества является «фишинг», с зафиксированными 2 614 случаями.

В разрезе городов наибольшее количество случаев интернет-мошенничества зафиксировано в Астане — 2 204 случая, в то время как Алматы занимает второе место с 1 048 случаями [3].

В период с января по октябрь 2024 года решения «Лаборатории Касперского» заблокировали более 5,8 млн попыток пользователей из Казахстана посетить фишинговые страницы, из которых более 861 тыс. были нацелены на мошеннические ресурсы [4].

Одна из распространенных схем мошенничества в Telegram заключается в том, что пользователь получает сообщение от контакта из своего списка с просьбой принять участие в голосовании за лучший детский рисунок в онлайн-конкурсе. В сообщении содержится ссылка на веб-страницу, на которой для участия в голосовании требуется ввести номер телефона и полученный проверочный код. После выполнения этих действий пользователь теряет доступ к своей учетной записи [5].

Телефонное мошенничество

Телефонные мошенничества возникают, когда злоумышленники представляются сотрудниками банков, правоохранительных органов или медицинских учреждений, сообщая о неотложных проблемах, требующих немедленного перевода денежных средств или предоставления личной информации. В качестве инструмента для повышения достоверности своих рассказов они нередко используют данные, полученные из социальных сетей.

В 2024 году каждый второй пользователь в Казахстане стал жертвой телефонного мошенничества. Согласно данным приложения Kaspersky Who Calls, в период с января по ноябрь 2024 года 72,4% пользователей в Казахстане получали спам-звонки. При этом более половины этих пользователей (52,1%) столкнулись с мошенниками.

В отчетах отмечается, что в этом году получили распространение мошеннические схемы, при которых злоумышленники запрашивают SMS-код под различными предлогами. Например, они представляются сотрудниками Казпочты, утверждая, что информируют о доставке

заказного письма, или звонят от имени Алматы Су, якобы для проверки счетчиков [6].

Например, в Актобе мошенники обманули женщину, выманив у нее 53 млн тенге. Позвонивший через WhatsApp мужчина, представившийся президентом программы «Болашак», сообщил о проверке на мошенничество и предложил связаться с «сотрудником КНБ». Вскоре она продала две квартиры и автомобиль, переведя деньги на счет злоумышленников [7].

Международный опыт

Многие страны внедряют комплексные меры для борьбы с кибермошенничеством.

В Великобритании создан Национальный центр кибербезопасности (NSCS), который сотрудничает с частным сектором для блокировки фишинговых сайтов.

Агентство по кибербезопасности (CSA) в Сингапуре разработало программы повышения осведомленности о киберугрозах и внедрило системы раннего оповещения о фишинговых атаках.

В России в 2025 году предлагаются поправки в законодательство, направленные на усиление борьбы с телефонным и онлайн-мошенничеством, включая пересмотр ряда законов для повышения эффективности борьбы с киберпреступностью [8].

Выводы

Увеличение числа фишинговых атак и телефонного мошенничества в Казахстане требует комплексного подхода, включающего передовые технологические решения. Такой подход не только снизит риски цифрового мошенничества, но и укрепит доверие граждан к безопасности и надежности цифровых услуг. Укрепление технологической защиты и правовой базы является ключевым для создания безопасной и доверенной онлайн-среды.

Рекомендации

Для эффективной борьбы с фишинговыми атаками и телефонным мошенничеством в Казахстане МЦРИАП РК рекомендуется до 01.01.2027 г. реализовать следующие меры:

1. Создание национальной системы мониторинга и блокировки фишинговых сайтов

МЦРИАП РК рекомендуется разработать автоматизированную систему мониторинга и выявления фишинговых сайтов, интегрированную с базами данных правоохранительных органов, банковского сектора и телекоммуникационных компаний. Это позволит выявлять и блокировать подозрительные ресурсы в реальном времени. Эти меры доказали свою эффективность в других странах, например, в Великобритании программа Active Cyber Defense снизила фишинговые атаки на 46% за год.

2. Создание централизованной базы данных мошеннических номеров и ссылок

МЦРИАП РК предлагается создать базу данных с информацией о мошеннических номерах и подозрительных веб-ресурсах, обновляемую в реальном времени. Подобная система успешно функционирует в США, где Федеральная торговая комиссия ведет реестр телефонных мошенников, что существенно снизило количество случаев телефонного мошенничества. Казахстан может внедрить аналогичную систему с возможностью автоматического уведомления граждан о подозрительных звонках через СМС или мобильные приложения.

Список использованных источников

1. О финансовой грамотности и цифровой гигиене высказался Президент // 24.kz. — 02.09.2024. — https://24.kz/ru/news/social/668477-o-finansovoj-gramotnosti-i-tsifrovoj-gigiene-vyskazalsya-prezident
2. Фишинг, дипфейки, QR-код: как интернет-мошенники обманывают казахстанцев // Kapital.kz. — 29.10.2024. — https://kapital.kz/gosudarstvo/131012/fishing-dipfeyki-qr-kod-kak-internet-moshenniki-obmanyvayut-kazakhstantsev.html
3. В Казахстане выявили почти 10 тыс. случаев интернет-мошенничества // 24.kz. — 28.08.2024. — https://24.kz/ru/news/incidents/item/667709-pochti-10-tys-sluchaev-internet-moshennichestva-vyyavili-v-kazakhstane
4. Заблокировали более 5,8 миллионов фишинговых атак в Казахстане // Businessmir.kz. — 04.12.2024. — https://businessmir.kz/2024/12/04/zablokirovali-bolee-5-8-millionov-fishingovyh-atak-v-kazahstane/
5. Казахстанцев предупреждают о фишинговых атаках в Telegram и WhatsApp // Zakon.kz. — 06.05.2024. — https://www.zakon.kz/obshestvo/6433407-kazakhstantsev-preduprezhdayut-o-fishingovykh-atakakh-v-Telegram-i-WhatsApp.html
6. В 2024 году каждый второй пользователь в Казахстане столкнулся с телефонным мошенничеством // Profit.kz. — 04.12.2025. — https://profit.kz/news/68517/V-2024-godu-kazhdij-vtoroj-polzovatel-v-Kazahstane-stolknulsya-s-telefonnim-moshennichestvom/
7. Женщина продала всё имущество и отдала 53 млн тенге главе программы «Болашақ» и сотруднику КНБ // Zakon.kz. – 11.02.2025. – https://www.zakon.kz/obshestvo/6466659-zhenshchina-prodala-vse-imushchestvo-i-otdala-53-mln-tenge-glave-programmy-bolashak-i-sotrudniku-knb.html
8. Правительство изменит десятки законов для борьбы с кибермошенниками: Какие нововведения предложили // RBC. – 10.02.2025. – https://www.rbc.ru/technology_and_media/10/02/2025/67a752bb9a7947c806896597