Кому: Министерством цифрового развития Республики Казахстан

ФИО и должность автора: Балтабек Дамир Мейремханулы главный специалист отдела проведение государственных закупок ГУ «Управление государственных закупок области Абай»

Дата: 11.ноября.2024 года.

Аналитическая записка

Тема: «Интернет-мошенничество: распространённые схемы и способы защиты»

Ключевые слова: Мошенничество, фишинг, Киберпол. информационная безопасность

«Интернет мошенничество» самый распространенный вид мошенничества связан с интернет-торговлей, где преступники выманивают деньги через фиктивные объявления.

Современное общество характеризуется развитием информационных технологий и глобализацией информационных процессов. Одним из самых ярких примеров такого процесса – это появление сети Интернет, а также стремительное и постоянное развитие его информационных технологий во всех сферах общественной жизни.

В настоящее время нельзя представить себе жизнь человека без Интернета, он буквально стал неразрывной частью общества.

Первоначальной целью разработки сети Интернет являлось создание надежной системы обмена информацией между компьютерами, а также (что явилось одной из главных целей) для отработки методов поддержания связи в случае ядерного нападения.

При этом по прошествии уже нескольких десятилетий с момента его создания, и не смотря, что проблема ядерной войны уже не является такой актуальной, хотя с повестки дня не снята, информационные технологии из военной сферы были переведены в гражданскую область жизнедеятельности, где получили новое дыхание, приобрели новейшие возможности и стали активно расти с каждым годом в Интернет пространстве.

Среди них можно выделить следующие:

− получение, хранение, обработка, распространение и использование информации и знаний благодаря возрастающим техническим возможностям коммуникации;

− осуществление коммуникации почти мгновенно, что принципиально отличает его от других средств коммуникации; −

функционирование виртуального пространства, повторяющего реальные сферы жизнедеятельности человека;

− проникновение компьютерных технологий в науку, культуру, медицину, образование, экономику, политику, технологии, производство;

− осуществление коммуникации с другим человеком (часто совершенно незнакомым), при этом отсутствует зависимость от местонахождения обоих, а коммуникация может поддерживаться непрерывно.

Растет не только количество интернет пользователей, но и время, которое они проводят, пользуясь устройствами и сервисами, работа которых зависит от подключения к Интернету и в 2020 году эта цифра составляла в среднем 6 часов в день.

Однако вместе с возможностями сети Интернет для развития и расширения коммуникации между людьми и, также возможности поиска, хранения и обработки большого количества информации, Интернет стал и полем для деятельности мошенников, т.е. обмана людей и выманивания у них на «добровольных основах» денежных средств.

Мошенничество - разновидность хищения чужого имущества или приобретения прав на чужое имущество путем обмана или злоупотребления доверием, за которые предусмотрена уголовная ответственность по статье 190 Уголовного кодекса Республики Казахстан.[2]

Анализ статистики показывает, по данным Первого кредитного бюро, в I полугодии 2024 года в Казахстане зарегистрировано 9 936 случаев интернет-мошенничества, что на 4,1% больше, чем в I полугодии 2023 года.. Этот рост, хоть и незначительный, демонстрирует, что преступники продолжают адаптироваться и искать новые пути для обмана граждан. Особенное внимание стоит уделить возрастной группе от 40 до 49 лет, так как она оказалась самой уязвимой".

Вместе с этим за последние годы в стране участились фишинговые атаки. Мошенники через вредоносную ссылку получают доступ к аккаунту жертвы в мессенджере WhatsApp и рассылают всем контактам взломанного аккаунта сообщение с просьбой прислать деньги. Также участились случаи, когда мошенники через мессенджеры направляют госсслужащим сообщение от имени лиц, занимающих руководящие должности. Злоумышленники под разными предлогами просят перевести деньги. только за январь и февраль этого года интернет-мошенники обманули казахстанцев более чем на 4 млрд тенге. При этом большинство мошеннических звонков поступает с Украины.[1]

Важным признаком, отличающим мошенничество от других преступлений, направленных против собственности, является то, оно

осуществляется посредством обмана потерпевшего или введения его в заблуждение.

Одной из отличительных характеристик, нового мошенничества является следующее, в интернет-мошенничестве субъект не входит в прямой контакт (непосредственный, личный, совместные встречи) с жертвой, что значительно снижает шансы на разоблачение и такой способ с каждым годом набирает популярность, проникая во все сферы общественной жизни. Именно отсутствие прямого контакта и применение информационных технологий упрощает получение персональных данных потенциальных жертв.

Важно отметить, что в основном мошенники полагаются не столько на высокие технологии и уникальные возможности, а на классические психологические методы воздействия на человека, позволяющие ввести жертву в заблуждение. Мошенники чаще всего пользуются доверчивостью своих жертв, когда она сама рассказывает личную и сугубо личную информацию о себе, пренебрегает или не знает основные правила интернет-безопасности (информационной безопасности), используют элемент неожиданности и запугивания потенциальной жертвы, чтобы получить информацию, которую впоследствии используют для совершения кражи или иной противоправной деятельности.

Наряду с этим, мошенники целенаправленно входят в доверие к жертве, а потом им злоупотребляют, т.е. осуществляют обман.

Обман может выражаться в ложном заявлении о том, что оно сознательно не соответствует действительности, или в преднамеренном замалчивании разных фактов, сообщение которых было необходимо. В любой форме обмана и злоупотребления доверием его суть заключается в том, что преступник посредством гарантий или упущений формирует у потенциальной или реальной жертвы наличие недостаточно верного или абсолютно неправильного представления о каком-либо объекте. Подобная ситуация приводит жертву к убеждению в необходимости передачи активов, или так называемого имущественного права. То есть реализуется ключевой принцип мошенничества, при котором преступление совершается на основе введения в заблуждение или обмане.

В настоящее время банковская сфера является одной из самых популярных среди интернет мошенничества. Один из самых популярных и распространенных методов ограбления клиентов в Интернете – это фишинг.

Слово представляет собой сочетание двух английских слов: пароль и рыбалка. В просторечии это словосочетание переводится как «перехват паролей». Этот метод чаще всего используется для обмана жертв, использующих интернет-банкинг, когда мошенники выдают себя за банк и отправляют поддельное сообщение на сотни случайно выбранных адресов электронной почты с просьбой срочно войти в

систему онлайнбанкинга определенного банка. Сообщение содержит ссылку на поддельный веб-сайт. После входа в фальшивую учетную запись покупателя просят ввести одноразовые коды или иную информацию, помогающую мошеннику получить доступ к банковскому вкладу жертвы.

Во всех регионах созданы и действуют специализированные группы по расследованию интернет-мошенничеств. В-частности, в городе Астана Республики Казахстан запущен пилотный проект «Киберпол».

Основной акцент сделан на усиление взаимодействия с другими госорганами, финансовыми учреждениями и частным сектором.

Также нами реализуется комплекс мер, направленных на выявление и раскрытие таких преступлений, а также задержание организаторов и соучастников.

Так, в прошедшем году по результатам проведенных оперативных мероприятий в ряде городов страны пресечена преступная деятельность 6 групп, занимавшихся обналом похищенных у граждан денег.

Среди них есть как казахстанцы, так и граждане бывшего союза. Последние занимались поиском и оформлением банковских карт, а также переводами денег организаторам мошеннических схем.

Кроме этого у них постоянно совершенствуются и изменяются методы совершения преступлений, модернизируются «инструменты» (создаются новые программы), появляются новые схемы обмана и как результат от таких действий страдают люди и компании, которым приносится значительный ущерб.

Эту тенденцию хорошо показывают различные статистические отчеты, отмечая, что правоохранительные органы еще недостаточно эффективно противодействуют интернет мошенничеству.[3]

В этой связи необходимо сказать, что службы безопасности коммерческих организаций и государственных органов постоянно выявляют эти схемы, но интернет мошенники придумывают новые. Простые и примитивные виды интернет - мошенничества остались далеко в прошлом с момента появления Интернет-пространства. Новое поколение мошеннических систем разработали и разрабатывают не «школьные» хакеры, а профессиональные преступники, поэтому абсолютно все недостатки устаревших систем постоянно учитываются и устраняются при разработке.

Таким образом, раскрыть мошеннические схемы, доказать их существование и уничтожить все системы злоумышленников «под корень» в современных реалиях является практически невозможным.

В заключение необходимо отметить, что схемы интернет-мошенничества становятся с каждым годом все более и более изощренными. Раньше использовались классические методы для привлечения трафика на мошеннические сайты или электронный спам,

всплывающая и баннерная реклама, поисковая оптимизация. Сегодня социальные сети и социальная инженерия не только расширили, но и упростили, расширили масштабы для деятельности мошенников, так как теперь они являются стандартным и традиционным методам личного и конфиденциального общения.

Таким образом можно сделать вывод, что, мошенники в настоящее время - это не отдельные хакеры-любители (такие тоже существуют), а крупные организованные криминальные группировки со значительными ресурсами (финансовыми, информационными и техническими) начали конкретно и достаточно активно атаковать людей на изъятие мошенническими способами денежных средств В результате количество случаев онлайн мошенничества растет с каждым годом, причем намного быстрее, чем количество простых случаев обычного фишинга.

При этом растут масштабы мошенничества и количество обманутых людей, даже из числа тех, кто считает себя подкованным на уловки преступников. Все это говорит о формировании негативной тенденции к дальнейшему развитию интернет-мошенничества.

Однако важно сделать вывод о том, что интернет-мошенничества не было бы, если бы не существовало алчности и жадности простых людей. Мошенники только отвечают на поведение людей, на их потребность и желание рисковать, ради получения выгоды и при этом для достижения своих целей и задач, при необходимости, совершенствуют использование психологических уловок в отношении потенциальных жертв.

В завершении хочу сказать, что с интернет мошенничеством можно бороться, в первую очередь, путем повышения бдительности самих людей, а также путем противодействия жадности и неоправданными рискам, которые свойственны простым людям.

В этой связи надо больше, активней говорить о таких явлениях и может быть тогда из-под преступников будут выбита противоправная платформа, а люди задумаются и себя информационно обезопасят (информационная безопасность - это как личная гигиена). Так же не желательно отвечать или произносить слово «Да» при телефонном разговоре. Так как при записи телефонного разговора они могут ставить ваш ответ как согласие на какие либо мошеннические действие. А так же рекомендуется разговаривать на казахском языке так как злоумышленники в основном люди из соседних стран.

Список использованных источников/литературы

1. Kazahkstan today 24/7 www.kt.kz/rus/crime/v_kazahstane_vozroslo_kolichestvo_faktov_1377968514.html

2. УГОЛОВНЫЙ КОДЕКС РЕСПУБЛИКИ КАЗАХСТАН https://online.zakon.kz/Document/?doc_id=31575252

3. Принимаемые меры по противодействию интернет-мошенничеству

https://www.gov.kz/memleket/entities/qriim/press/article/details/110479?lang=ru.

4. Chat gpt