## Хищения в сфере информационно-телекоммуникационных систем

Согласно данным Роскомнадзора в 2023 году число интернет-пользователей в России составило 129,8 млн. человек, что составляет 90% населения современной России. Безусловно, внедрение информационных и телекоммуникационных технологий (далее – ИТТ) в повседневную жизнь и профессиональные сферы необходимо для оптимизации жизненных и рабочих процессов.

В 2023 на территории Городищенского района зарегистрировано 218 преступлений, совершенных с использованием ИТТ, что на на 47,3% больше, чем в аналогичном периоде прошлого года (148). Раскрываемость таких преступлений снизилась на 6% и составила 26,6% против 32.6%.

Доля преступлений, совершенных с использованием ИТТ, от общего количества зарегистрированных на территории района (787) составила 27,7% или каждое 3-е преступление.

В структуре преступности, совершаемой с использованием ИТТ, преобладают все виды дистанционного мошенничества (93 или 42,6%) и кражи (15 или 7%).

С неуклонным ростом числа активных пользователей закономерным является рост количества разнообразных преступных схем в сфере ИТТ, в том числе с использованием сети «Интернет», банковских карт, мобильных телефонов.

В связи с цифровизацией общества, затрагивающей и социально уязвимые категории граждан, в том числе пожилых людей, инвалидов, несовершеннолетних, испытывающих сложности при освоении и использовании современной техники и информационных технологий, обладающих повышенной доверчивостью и внушаемостью.

Так, в 2023 году 29 преступных деяний (13,3% от общего количества IT-преступлений) совершены в отношении социально-незащищенных категорий граждан, из них 2 преступления в отношении несовершеннолетних, 25 – пенсионеров по старости, 2 – инвалидов.

Одним из самых распространенных видов мошенничества в сфере ИТТ является использование психологических уязвимостей человека, в том числе создание иллюзии правомерности происходящего. Так, злоумышленники придают своим действиям правомерный вид, действуя от лица знакомых, служб безопасности организаций, правоохранительных органов.

К примеру, 17.11.2023, неустановленное лицо, используя абонентские номера, под предлогом защиты от несанкционированного оформления кредита, убедило К. установить приложение банка и осуществить внесение наличных на «безопасные счета», после чего К. в этот же день, осуществил 4 транзакции на общую сумму 600 000 рублей. После перечисления денежных средств, неустановленное лицо распорядилось похищенным по своему усмотрению. По рассмотренному факту следственным отделом ОМВД России по Городищенскому району возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ.

Популярным способом хищения денежных средств в сфере ИТТ является завладение конфиденциальной информацией, предоставляющей доступ к персональным данным владельца, в ситуации передачи самим владельцем таких данных, находясь под влиянием злоумышленника.

Так, зачастую преступники используют арендованные (как правило виртуальные) мобильные номера, которые не оформляются на конкретное физическое лицо, в связи с чем достаточно сложно установить не только конкретное устройство, а и определенный регион из которого осуществлялся вызов.

Посредством арендованных номеров, преступники могут осуществлять телефонные звонки на абонентские номера граждан, представляясь сотрудниками ФГИС «Единый портал государственных и муниципальных услуг», коммерческих банков, после чего предлагают продиктовать смс-код (являющийся простой электронной подписью, подтверждением

списания денежных средств/проведение финансовой операции), направленный на абонентский номер с целью хищения денежных средств.

Также распространены случаи, когда преступники представляются родственниками либо знакомыми потерпевших, просят о перечислении денежных средств, в связи со сложившейся неблагоприятной ситуацией. Например, для решения вопроса с уголовным преследованием вследствие нарушения ПДД родственником или знакомым.

Так, например, в период времени с 01.09.2023 по 14.09.2023, неустановленное лицо, используя абонентский номер, осуществил телефонный вызов посредством мессенджера «WhatsApp», после чего ввело М., являющуюся пенсионером по возрасту, в заблуждение и убедило последнюю перечислить денежные средства в размере 540 000 рублей, путем выполнения транзакций на реквизиты банковского счета. После получения денежных средств неустановленное лицо распорядилось ими по своему усмотрению. По указанному факту следственным отделом ОМВД России по Городищенскому району возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ.

Кроме того, хищения в сфере ИТТ совершаются посредством размещения на сайтах в сети «Интернет» заведомо ложных сведений об оказываемых услугах и купле-продажи товаров. Злоумышленники требуют внести предоплату, залог, задаток, после чего получив денежные средства удаляют объявление или иным образом не исполняют обязательств, указанных в объявлении.

Как способ совершения преступления используется также «фишинг». То есть, злоумышленник направляет потерпевшему электронное письмо, СМС, имитирующее официальное обращение со стороны банка и требующее проверки информации, либо совершения тех или иных действий. Сообщение же содержит ссылку на **поддельный** интернет-сайт, имитирующий настоящий (отличить который порой очень непросто), и содержащий форму, требующую ввести необходимую для злоумышленника информацию – данные банковской карты, ПИН-код, паспортные данные.

**Как не стать потерпевшим от действий злоумышленников в сфере ИТТ?**

Безопасность в анализируемой сфере в первую очередь зависит от осведомленности граждан о базовых мерах предосторожности в сфере ИТТ.

- Не переходите по подозрительным ссылкам, предлагающим какие-либо выгоды или вознаграждения.
- Контролируйте операции по вашей банковской карте, так как в случае неправомерного доступа и попытки хищения денежных средств, необходимо обратиться в службу поддержки Вашего банка для заморозки и операций по карте.
- Используйте усложненные пароли, которые будут содержать буквенный и цифровой набор (не используйте даты рождений, повторяющиеся числа).

➢ Помните, что в случае поступления предложений предоставить данные банковской карты, установить какое-либо приложение либо указать иную информацию, к ним стоит относиться критически, информацию перепроверять путем самостоятельных звонков на горячую линию, службы поддержки.

При поступлении звонков либо получения сообщений от «родственников» прежде, чем переводить денежные средства необходимо самостоятельно созвониться с ними, выяснить их местонахождение и иные обстоятельства. При утрате банковской карты необходимо незамедлительно обращаться по горячей линии банка и требовать заблокировать утраченную карту.

В настоящее время во всех социальных учреждениях, территориальном отделе полиции и иных государственных и муниципальных органах и учреждениях размещены листовки, стенды с информацией о том, как не стать жертвами мошенников.

О предполагаемых фактах хищений незамедлительно сообщать в органы внутренних дел.

**Об уголовной ответственности за хищения персональных данных, денежных средств в сфере и с использованием информационно-телекоммуникационных технологий (далее – ИТТ) и меры предосторожности.**

Стремительный рост числа преступлений в сети Интернет свидетельствует о том, что преступники теперь используют цифровую/виртуальную среду также активно, как и реальный мир, что создает для них новую специализацию в преступной сфере: в 2023 году в Российской Федерации было зарегистрировано более 2 миллионов преступлений, из которых более 500 000 (>25%) были преступлениями с использованием ИТТ.

В секторе ИТТ происходят различные преступления, в основном это интернет и мобильное мошенничество с целью хищения денег с банковских счетов граждан ст. 159 УК РФ. Среди других преступлений - кража с помощью платежных карт (пластиковых карт) - п. «г» 3 ст. 158 УК РФ; производство, использование и распространение вредоносных программ - ст. 273 УК РФ; распространение незаконной информации через интернет - ч. 2 ст. 128.1 УК РФ.

**Важным элементом защищенности Ваших персональных данных и денежных средств являются - знания.**

Для этого рассмотрим некоторые из наиболее распространенных техник, используемых злоумышленниками в сфере ИТТ. К ним относятся:

1. Фишинг - вид интернет-мошенничества, который используют для получения доступа к личной информации пользователя: логинам, паролям, номерам телефонов, данным банковских карт и так далее посредством массовых рассылок электронных писем на электронную почту, текстовых сообщений.

2. Вишинг (голосовой фишинг) - это специальное манипулирование телефонными сетями с целью получения личной и финансовой информации жертв. После создания копии системы банка жертву просят (предпочтительно через поддельное электронное письмо) позвонить по номеру банка для подтверждения деталей.

Система банка копирует и отклоняет данные, введенные жертвой.

3. SMS-мошенничество - мошенники рассылают SMS-сообщения о транзакциях жертвы (блокировка банковских счетов и кредитных карт) и просят потерпевшего сообщить данные счета и пароли в полученном SMS-сообщении, что приводит к хищению средств;

4. Мошенничество с предоплатой - покупка и продажа товаров на разнообразных сайтах (Юла, Avito.ru и др.),

5. Поиск работы (JOB.ru, HH.ru или интернет ресурсы RABOTA.ru, HeadHunter.ru и др.);

6. Взлом аккаунтов в социальных сетях и отправка сообщений друзьям и знакомым с требованием денег - мошенники пользуются беспечностью людей и используют специальное программное обеспечение для входа в аккаунты в социальных сетях и отправки сообщений всем знакомым от имени

взломанного пользователя с описанием сложной жизненной ситуации и просят финансовой помощи или одолжить денег;

7. Мошенники, выдающие себя за сотрудников полиции или следователей, сообщают родственникам жертв, что те подозреваются в совершении несчастного случая или преступления, и предлагают им иммунитет от судебного преследования, если они переведут определенную сумму денег на указанный счет;

8. Участие в онлайн-опросах, сообщение о выигрышах в лотерею и компенсация за ранее оказанные услуги - мошенники предлагают крупные суммы денег пользователям Интернета, которые участвовали в онлайн-опросах или сообщили о выигрыше в лотерею. Иногда требуется «депозит» для получения соответствующих документов или уплаты пошлины.

## Как нужно действовать, чтобы не дать злоумышленнику похитить Ваши персональные данные, денежные средства?

В случае если к вам обратились по сотовой связи или же в онлайн, и под разными поводами пробуют признать данные о вашей банковской карте, пароли или же иную индивидуальную информацию, будьте аккуратны: это видимые симптомы действий злоумышленников.

Если у Вас появились подозрения, советуем закончить общение и как можно быстрее связаться с банком по телефонному номеру, обозначенному на оборотной стороне вашей банковской карты. Не следуйте рекомендациям третьих лиц.

Сохраняете вашу карту в недоступном от посторонних людей месте. В случае если совершено хищение с Вашей банковской карты, немедленно пишите заявление в ближайший отдел полиции.

**Уважаемые граждане, ни в коем случае не наносите информацию на банковскую карту о код-пароле (пин-код) для доступа к банковской карте посредством терминала, не храните такую информацию в непосредственной близости с банковской картой в виде записей на листе и тому подобное.** Такие действия создают беспрепятственную возможность для злоумышленников по обналичиванию денежных средств с банковского счета.

При заявлении в полицию необходимо приложить копию выписки счета, полученную предварительно в банке, где станет заметно перемещение денежных средств по счету. Кроме того возможно обеспечить детализацию телефонных звонков и смс, это в случае, если хищение денежных средств произошло методом телефонной связи.