## ВНИМАНИЮ ГРАЖДАН!

В 2021 году правоохранительными органами Зауралья зарегистрировано более двух тысяч хищений денежных средств с банковских счетов граждан, а причиненный ущерб превысил 184 миллиона рублей. Каждый месяц жертвами мошенников становились порядка 170 жителей региона, которые ежедневно в среднем переводили мошенникам около полумиллиона рублей.

На территории г. Шадринска и Шадринского района в прошлом году зафиксировано 248 краж, мошенничеств и вымогательств, совершенных с использованием IT-технологий, при этом сумма ущерба варьировалась от нескольких сотен рублей до миллиона и больше, а в общей сложности составила 26,5 миллиона рублей.

В текущем году совершено уже более 40 таких преступлений, общая сумма причиненного шадринцам ущерба превысила 5 миллионов рублей.

Жертвой аферистов может стать любой гражданин. Как показывает практика, это не только пенсионеры, но также лица молодого и среднего возраста, в том числе работники различных организаций, учреждений и ведомств, студенты и даже безработные. В ряде случаев потерпевшими становились даже те, кто самостоятельно проводил среди коллективов профилактическую работу и разъяснял коллегам, как не поддаться на уловки мошенников.

Практически в каждом случае пострадавшие заявляли, что из средств массовой информации, от правоохранительных органов, работодателей и прочих источников им уже были известны используемые злоумышленниками приемы, но даже не могли предположить, что такое может произойти именно с ними. Именно поэтому вопрос предотвращения преступления и сохранения своих сбережений в настоящее время касается **АБСОЛЮТНО ВСЕХ ГРАЖДАН!!!**

Действительно, способы незаконного завладения денежными средствами граждан многообразны и со временем становятся еще изобретательнее.

Самыми распространенными являются телефонные звонки, во время которых злоумышленник называет Вас по имени и отчеству и представляется сотрудником отдела безопасности банка, корректно выясняет, проводились ли Вами операции по карте, не оставляли ли вы заявку на оформление кредита и сообщает о том, что кто-то пытается оформить на Ваше имя долговое обязательство либо выпустить карту. В последнее время распространены случаи, когда похитители представляются сотрудниками полиции, Следственного комитета и иных правоохранительных органов и также сообщают о том, что якобы кто-то совершает хищение Ваших денежных средств, предлагают помочь пресечь преступление, «поймать вора» и сохранить Ваши накопления.

Все больше набирает обороты использование в преступных целях возможностей IP-телефонии, позволяющей скрывать как фактическое местонахождение преступников, так и реальные номера используемых ими телефонов.

Однако единственная цель таких звонков - ввести жертву в заблуждение и вызвать у нее чувство беспокойства, паническое или шоковое состояние, не дать трезво оценить обстоятельства.

После этого мошенник, а чаще - группа мошенников, убеждают совершить действия по переводу денег на так называемые «безопасные», «резервные» и тому подобные счета, которые на самом деле подконтрольны злоумышленникам. В ряде случаев преступники даже убеждают граждан оформить кредит на свое имя, чтобы предотвратить «попытку» его получения другими лицами, после чего потерпевшие опрометчиво и бездумно переводят заемные средства на такие же «безопасные» или «резервные» счета.

Зачастую гражданину достаточно лишь назвать реквизиты своей банковской карты (номер, дата действия, CVC-код на обороте карты) и сообщить коды (пароли) из приходящих СМС-со- общений, благодаря которым мошенники дистанционно совершают хищение денежных средств. Однако, как показывает практика, чаще всего именно жертвы самостоятельно переводят денежные средства с одного счета на другой через мобильное приложение либо с использованием банкоматов.

Так, в январе 2022 года 61-летнему жителю г. Шадринска поступил звонок с подставного номера дежурной части органа внутренних дел и неустановленное лицо, представившись сотрудником полиции г. Кургана, сообщило о попытке оформления кредита, после чего убедило потерпевшего обратиться в банк и взять кредит на сумму 380 000 рублей. В дальнейшем к разговору подключилась женщина, представилась сотрудницей банка и обманным путем получила коды из СМС-сообщений, позволившие похитить у жертвы 300 000 рублей. Более того,

преступники убедили мужчину подать заявку на заем крупной суммы в другом банке, однако в предоставлении кредита ему там было отказано из-за нехватки документов.

В феврале 2022 года неустановленные лица, также представившись сотрудниками банковской организации и Следственного комитета, под предлогом предотвращения попытки хищения денег убедили 36-летнюю жительницу г. Шадринска перевести почти 600 тысяч рублей на подконтрольные им счета. При этом мошенники обладали не только анкетными сведениями потерпевшей, но и данными об имеющихся у нее счетах и точных суммах денежных средств, что придавало их действиям эффект правдоподобности.

Для предотвращения подобных ситуаций важно помнить одно простое правило - **НИ В КОЕМ СЛУЧАЕ НЕ ПРОДОЛЖАТЬ РАЗГОВОР ПО ТЕЛЕФОНУ.** Ни при каких обстоятельствах настоящие сотрудники банковских организаций не будут звонить по телефону и выяснять у Вас данные, которыми они не располагают. Банк несет ответственность за сохранность Ваших денежных средств и для их сбережения он никогда не будет обращаться за помощью к своим клиентам.

Если же денежные средства переведены самим собственником (даже под влиянием обмана) либо иным лицом, но после получения от собственника паролей и иных необходимых сведений, то вся ответственность за судьбу сбережений возлагается уже на клиента.

Например, в феврале 2022 года мошенник, представившись сотрудником банка, предложил 48-летнему жителю г. Шадринска оформить кредитный лимит с выгодным предложением под 6% годовых, назвал первые 6 цифр кредитной карты и попросил назвать оставшиеся цифры, а также 3-значный код на обороте карты. После этого попросил у потерпевшего продиктовать код из СМС-сообщения и, получив необходимые сведения, похитил у мужчины более 18 тысяч рублей.

В последнее время участились случаи, когда преступники пользуются желанием людей получить высокий доход без применения каких-либо существенных усилий для этого, заработки на фондовых биржах, инвестиции в крупные известные компании. Криминальные посягательства в таких случаях совершаются лицами, выдающими себя за представителей крупных инвестиционных организаций, аналитиков банков, трейдеров, специализирующихся в этой сфере «Интернет-площадок».

Преступления могут также совершаться путем заключения соглашений о купле-продаже товаров на различных интернет-сайтах. Зачастую общение в таких случаях происходит с вымышленным продавцом, а денежные средства переводятся потерпевшим на счета третьих лиц. Встречаются даже случаи, когда потерпевший, сам являясь продавцом, поддается уговорам потенциального покупателя и переводит ему деньги.

Так, в январе текущего года с использованием сайта «Юла» неустановленный в ходе переписки с 30-летним жителем г. Шадринска, разместившим объявление о продаже сотового телефона, под предлогом покупки товара скинул последнему ссылку для оформления доставки, после чего потерпевший перешел по ссылке, заполнил анкетные сведения, номер телефона, данные банковской карты и ее баланс. Воспользовавшись полученными сведениями, мошенник похитил у мужчины 50 750 рублей, переведя их с банковской карты на неизвестный счет.

В некоторых случаях злоумышленниками используются сайты-двойники, пользование которыми приводит к разглашению потерпевшим, полагающим, что он находится на привычном для него ресурсе, конфиденциальной информации, позволяющей списать денежные средства без ведома потерпевшего.

Набирает обороты применение ссылок и QR-кодов, которые подменяют собой реально существующие ссылки для оплаты различных товаров и услуг (к примеру, коммунальных), в связи с чем безналичные денежные средства переводятся не законному получателю, а поступают на подконтрольные преступникам счета.

Зачастую мошенники, выдавая себя за знакомых или близких родственников, используют страницы взломанных аккаунтов в социальных сетях или создают двойники страниц реально существующих людей.

Как показывает практика в подавляющем большинстве случаев преступления в отношении жителей Курганской области совершаются лицами из других регионов России. Как правило, такие преступления остаются нераскрытыми, поскольку злоумышленники используют сим-карты и банковские счета, оформленные на других граждан, часто меняют их, переводят деньги за границу и обналичивают иными ухищренными способами.

Истории мошенников различны и нескончаемы, но нужно понимать, что банками обеспечена безопасность денежных средств, которые находятся на банковских счетах, но лишь до того момента, пока владелец счета сам не сообщит преступникам реквизиты банковских карт или не перейдет по ссылкам.

Если в ходе разговора у Вас возникают сомнения по поводу сообщаемых сведений, не торопитесь действовать по указанию «сотрудников банков», «полицейских», «следователей», которые якобы хотят Вас обезопасить от хищения денег, **НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР** и перезвоните по телефону «горячей» линии, указанному на обороте карты, выясните, действительно ли совершаются попытки хищения денег. Вам всегда разъяснят, что в данном случае необходимо предпринять.

Если преступникам все же удалось обманным путем завладеть необходимыми реквизитами банковских карт и счетов либо убедить Вас самостоятельно перевести денежные средства на другие счета, необходимо **НЕЗАМЕДЛИТЕЛЬНО НАПРАВИТЬ ЗАЯВКУ В БАНК ОБ ОТМЕНЕ ПРОВЕДЕННЫХ ОПЕРАЦИЙ И БЛОКИРОВАНИИ БАНКОВСКИХ КАРТ,** после чего сообщить о случившемся в межмуниципальный отдел МВД России «Шадринский» по адресу: г. Шадринск, ул. Михайловская, 110 (тел. 8 (35253) 9-65-10, 9-65-11) либо в иной территориальный правоохранительный орган по месту жительства, а также по телефону 02.

Для результативного раскрытия преступного деяния в своем заявлении гражданам следует отразить информацию об обстоятельствах произошедших событий, месте, времени совершения преступления, размере причиненного ущерба, контактах злоумышленников. Также необходимо сохранить переписку и историю телефонных звонков (например, сделать скриншот экрана), иные следы преступления (например, запись телефонного разговора), запросить в банке выписку о движении денежных средств по счетам, а у оператора сотовой связи - детализацию телефонных переговоров и сообщений.

Знание гражданами основных положений закона и мер предосторожности способствует борьбе с преступностью, укреплению законности и правопорядка.