Татьянкина С.Ф.
надо довести до коллектива

М В Д Р о с с и и

Г Л А В Н О Е У П Р А В Л Е Н И Е
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО АЛТАЙСКОМУ КРАЮ
(ГУ МВД России по Алтайскому краю)

пр. Ленина, 74, Барнаул, 656015

14.02.2023 № 4/1382

на № _____ от _____

Директору КГБПОУ «Алтайский архитектурно-строительный колледж»

В.А. Баленко

пр. Ленина, 68, г. Барнаул, 656015

Уважаемый Виталий Антонович!

Сегодня практически каждый гражданин нашей страны (независимо от пола, возраста, уровня образования и социального положения) ежедневно использует множество разнообразных высокотехнологичных устройств – банковские карты, смартфоны и компьютеры. Для того, чтобы сделать нашу повседневную жизнь удобнее и проще, участниками рынка товаров и услуг постоянно внедряются новые устройства, программы и сервисы, призванные избавить каждого из нас от лишних передвижений и хлопот. С внедрением в повседневную жизнь высоких технологий появляются и новые виды преступлений - мошенничества, позволяющие преступникам с использованием описанных выше «благ» обмануть граждан и похитить принадлежащие им деньги.

По итогам 2022 года в крае зарегистрировано около **6200** сообщений о преступлениях, связанных с тайным хищением денежных средств с банковских счетов граждан и с хищением денег у граждан путем обмана. Количество преступлений указанной категории снижается незначительно.

Анализ преступлений, совершенных с использованием информационно-телекоммуникационных технологий показал, что преступления указанной категории совершаются в большинстве случаев в отношении физических лиц в возрасте от 30 до 50 лет, потерпевшими в большинстве случаев признаются женщины. Около 20% дистанционных преступлений совершаются в отношении граждан в возрасте от 50 до 70 лет, являющихся наемными рабочими и пенсионерами по старости.

В качестве причин и условий, способствующих совершению таких преступлений продолжают оставаться излишняя открытость и доверчивость потерпевших в диалоге с мошенниками; беспечное отношение к конфиденциальной информации, разглашение которой приводит к хищению денег с банковского счета; предоставление банками возможности оформить кредит на большую сумму без личного визита в банк, а также возможности получить мгновенный доступ к распоряжению кредитными средствами.

Наличие в арсенале преступников современных средств коммуникации, позволяющих совершать «дистанционные» преступления в отношении жителей Российской Федерации с территории иностранных государств, совершенствование

преступных схем и многоступенчатость используемых при их совершении механизмов сокрытия похищенных денег, осложняют процесс раскрытия таких преступлений и минимизируют потенциальную возможность возмещения материального ущерба, причиненного в результате их совершения.

Сотрудниками МВД России проводится колоссальная работа по профилактике мошенничеств, которая осуществляется по нескольким направлениям. Участковые уполномоченные полиции обходят граждан и доводят до них информацию о видах мошенничества и способах их предотвращения; профилактические памятки размещаются в подъездах домов и раздаются гражданам на улицах, в подразделениях органов внутренних дел и иных организациях; через средства массовой информации граждане предупреждаются о совершении мошеннических действий, им даются рекомендации, как не стать жертвой аферистов; следователи и сотрудники полиции проводят разъяснительные беседы с участниками уголовного судопроизводства.

Мошенники хорошо знают психологию людей, манипулируют их чувствами, используя такие мотивы, как тревога за близких и знакомых и желание оказать любую помощь; беспокойство за имеющиеся на банковских счетах сбережения; чувство корысти, а также такие человеческие качества как доверчивость, невнимательность и беспечность.

Несмотря на усилия правоохранительных органов, прилагаемые для борьбы с данным видом преступлений, каждый гражданин может сам лично обезопасить себя от противоправных действий, для чего достаточно соблюдать ряд простых правил.

Вот некоторые из них:

- телефонные мошенники рассчитывают на доверчивых и мнительных людей, которые соглашаются с тем, что им говорят и выполняют чужие указания. Если в ходе телефонных переговоров или электронной переписки с неизвестными лицами у Вас возникли сомнения в достоверности предоставленных Вам сведений – спокойно и уверенно задавайте собеседнику уточняющие вопросы – они отпугнут мошенников и они сами прекратят начатый разговор либо обман станет для Вас очевидным. В период совершения преступлений мошенники всяческими способами пытаются удержать потенциальную жертву в режиме телефонного разговора, не давая возможности прервать разговор, опомнится, в полной мере осознать происходящее и посоветоваться. **Ни при каких обстоятельствах не впадайте в панику!** Прекратите разговор, обратитесь к Вашим родственникам, знакомым либо в полицию и сообщите о происшедшем;

- никогда не сообщайте посторонним свои персональные данные. Помните: сотрудник банка **никогда** не предложит Вам перевести денежные средства на какие-либо «безопасные» счета и не попросит предоставить ему информацию, необходимую для доступа к Вашему банковскому счету (номер карты, пин-код, поступившие в sms-сообщениях пароли и т.д.);

- если Вам звонят якобы из банка и просят совершить подобные действия, нужно прекратить диалог. Если у вас возникли вопросы, то можно позвонить в банк по номеру телефона, который указан на оборотной стороне вашей банковской карты, но не перезванивать на тот номер, с которого звонили;

- если Вам звонят и сообщают о том, что мошенники якобы пытаются оформить на Ваше имя кредит либо получить доступ к Вашим банковским счетам – **сразу же прекратите разговор**! Если у Вас остались сомнения – позвоните в банк сами, при наличии поводов беспокоиться – заблокируйте Ваш банковский счет путем личного обращения в банк либо по телефону официальной «горячей» линии;

- если Вам кто-то звонит и просит принять участие в спецоперации, якобы проводимой под контролем сотрудников МВД, ФСБ и других правоохранительных органов – немедленно прекратите разговор (**даже в том случае, если Вам звонят с городских телефонных номеров, официально закрепленных за соответствующими ведомствами**), и сообщите о происшедшем в полицию;

- если к Вам через социальные сети обратился кто-то от имени Ваших знакомых и родственников с просьбой одолжить деньги – прекратите переписку, свяжитесь с Вашими знакомыми по телефону и выясните с какой целью им необходимы деньги;

- не вкладывайте деньги в сомнительные инвестиционное проекты, на Интернет-сайтах которых размещена информация о возможности получения в кратчайшие сроки прибыли, значительно превышающей суммы инвестиций, **даже в том случае, если тот или иной инвестиционный проект Вам порекомендовали Ваши знакомые и родственники**;

- пользуйтесь только проверенными сайтами, порталами и Интернет - магазинами. Простым способом защитить и не потерять свои деньги является оплата товара исключительно после доставки. **Не приобретайте товары, предложения о продаже которых размещаются в группах в социальных сетях и на Интернет-сайтах (например «Одноклассники», «ВКонтакте» и т.д.)**;

- при продаже (покупке) предметов обихода через соответствующие Интернет-сайты не производите по указанию продавцов (покупателей) никаких действий с открытыми на Ваше имя банковскими картами (счетами), в том числе, с использованием банкоматов и смартфонов. При необходимости получить оплату просто сообщите покупателю номер открытой на Ваше имя банковской карты, либо произведите перечисление денег на указанный последним банковский счет с использованием доступных сервисов. Однако, перед приобретением того или иного товара попросите продавца предоставить Вам подтверждение наличия указанного товара в его распоряжении;

- в случае, если Вам с незнакомого номера позвонил кто-то от имени Вашего родственника (знакомого) и, сообщив о наличии у него каких-либо проблем, *попросил прислать на определенный счет либо передать кому-то деньги*, **не поддавайтесь панике**, а просто прекратите разговор и перезвоните Вашему *родственнику (знакомому) по известному Вам до этого момента номеру телефона*, либо позвоните третьим лицам (общим родственникам и знакомым) и проясните ситуацию;

- в случае, если Вам позвонил представитель какой-либо компании (организации) и сообщил о том, что Вам полагаются какие-либо выплаты (за ранее приобретенные медицинские препараты и приборы, в качестве лотерейного

выигрыша, возмещение оплаты за ЖКХ и т.д.) – сразу же прекратите разговор и сообщите о происшедшем в полицию;

- в случае, если Вы решили воспользоваться для организации поездки мобильным приложением «BlaBlaCar», предназначенным для онлайн-поиска автомобильных попутчиков, производите оплату за поездку только в приложении, **никогда не переходите по ссылке, предоставленной Вам водителем в целях проведения платежа**. Такие ссылки являются фишинговыми, переход по ним и введение реквизитов Ваших банковских карт в предложенной форме приведет к списанию всех находящихся на Вашем банковском счете денежных средств. Это касается и оплаты товаров на сайтах «Авито» и «Юла» - злоумышленники могут предоставить Вам фишинговую ссылку, якобы для оплаты покупки с использованием сервиса «безопасная сделка», в действительности таким образом мошенники стремятся получить реквизиты Вашей банковской карты для последующего использования их в целях хищения денежных средств с Ваших банковских счетов;

- **не пользуйтесь услугами гадалок**, размещающих информацию о своих экстрасенсорных и сверхъестественных лечебных способностях в сети «Интернет». Используемые «гадалками» методы социальной инженерии, основанные, в том числе, на устрашении и обещании выполнить невозможное, неизбежно приведут к тому, что Вы, опасаясь мнимых, но кажущихся реальными угроз, передадите злоумышленникам все имеющиеся у Вас сбережения;

- храните открытые на Ваше имя банковские карты, оснащенные функцией бесконтактной оплаты, в надежном и недоступном для третьих лиц месте;

- при совершении покупок в Интернет-магазинах уделяйте особое внимание размещенным в сети Интернет отзывам о работе выбранного магазина; дате создания магазина; проверьте наличие указанного на сайте юридического адреса;

- не стоит доверять сайтам, имеющим в названии знакомые слова, но расположенные в доменных зонах **com.**, **org.**, **biz.**, **net.**, **info.**, **tv.**, **mobi.** и других, не связанных с российским Интернет-пространством

- если в ходе телефонных переговоров Вы, будучи обманутым, все-таки сообщили мошеннику информацию, достаточную для доступа к вашим банковским счетам, сразу же после окончания разговора позвоните в банк и заблокируйте Ваши банковские карты (счета).

Предлагаем Вам довести изложенные выше правила поведения до сведения подчиненных сотрудников и направить в наш адрес информацию о порядке проведенного профилактического мероприятия и числе его участников.

Начальник
главного следственного управления
генерал-майор юстиции О.В. Кузнецова

М.В. Дитятева
(3852) 391-258