Информационное письмо для направления в трудовые коллективы в целях профилактики преступлений, совершенных с использованием информационно-телекоммуникационных технологий

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.

За первое полугодие 2024 года в крае зарегистрировано около **3500** преступлений, связанных с хищением денег у граждан путем обмана. Жителям Алтайского края причинен ущерб на сумму свыше 670 млн. рублей.

В качестве причин и условий, способствующих совершению таких преступлений продолжают оставаться излишняя открытость и доверчивость граждан в диалоге с мошенниками; беспечное отношение к конфиденциальной информации, разглашение которой приводит к хищению денег с банковского счета; желание получить выгоду при приобретении и продаже товаров повседневного спроса, легкий заработок, обращение в целях решения жизненных проблем к гадалкам и магам.

Мошенники хорошо знают психологию людей, манипулируют их чувствами, используя такие мотивы, как тревога за близких, желание оказать им 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.

ОБЯЗАТЕЛЬНО ВНИМАТЕЛЬНО ПРОЧТИТЕ КАЖДОЕ ИЗ НИХ, ЭТО ПОМОЖЕТ ВАМ ОБЕЗОПАСИТЬ СЕБЯ И СВОИХ БЛИЗКИХ от МОШЕННИКОВ!

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 деньги 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**), сообщите о происшедшем в полицию;

- не реагируйте на звонки, поступающие якобы от сотрудников ФСБ, полиции и прокуратуры, которые в ходе телефонных переговоров сообщают Вам об использовании Ваших банковских счетов для финансирования вооруженных сил Украины, а также на другую информацию, касающуюся проведения СВО, урожая привлечением Вас к уголовной ответственности. **НЕ БОЙТЕСЬ! Не впадайте в панику! Сразу же прекратите разговор и позвоните в полицию**;

- не реагируйте на звонки и сообщения, поступающие якобы от знакомых Ваших родственников, проходящих службу в зоне проведения СВО, с просьбой об оказании материальной помощи. **Дождитесь сеанса связи с родственником, убедитесь в том, что поступившая просьба исходила именно от него;**

- если на Ваш мобильный телефон в социальных сетях (WhatsApp, ВКонтакте, Телеграм и т.д.) поступило сообщение от Ваших знакомых и родственников с просьбой одолжить деньги и с указанием реквизитов

банковской карты для их перечисления - **Прекратите переписку! Деньги не перечисляйте, свяжитесь с Вашими знакомыми по телефону и убедитесь в том, что сообщение поступило именно от них;**

- **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** либо его название созвучно или соответствует названию какой-либо крупной и успешной компании;

- если в поисках подработки Вы увидели объявление в сети Интернет либо в социальных сетях с предложением за вознаграждение оценивать товары, реализуемые через известные маркетплейсы – «Wildberries», «ОЗОН» и т.д. – **НЕ РЕАГИРУЙТЕ** на него, в ходе общения мошенники предложат Вам сначала оценивать товары, затем заказывать их с возвращением потраченных средств, а в тот момент, когда Вы начнете доверять им, попросят Вас сделать заказ товара уже на большую сумму, которая Вам **ВОЗВРАЩЕНА НЕ БУДЕТ**!

- осуществляйте поиск работы в сети Интернет только на специализированных сайтах;

- 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;

- **НЕ ПОЗВОЛЯЙТЕ** Вашим несовершеннолетним детям брать Ваш смартфон с подключенным банковским приложением в Ваше отсутствие, контролируйте действия, которые Ваш ребенок производит с Вашим мобильным телефоном. Мошенники **ИСПОЛЬЗУЮТ ДЕТЕЙ** как инструмент доступа к Вашему банковскому счету, путем обмана убеждая их в ходе телефонных переговоров сообщить номера телефонов родителей, поступившие на абонентские номера последних пароли и коды, в том числе необходимые для получения доступа к их банковским счетам;

- в случае, если Вы решили сменить абонентский номер телефона – **НЕЗАМЕДЛИТЕЛЬНО** после приобретения новой sim-карты обратитесь в банк и отключите прежний номер от банковских счетов, либо сделайте это с использованием мобильного приложения банка. В противном случае новый владелец Вашего абонентского номера сможет получить доступ к Вашим банковским счетам и похитить принадлежащие Вам деньги;

- 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.