**Информация**

**о профилактических мерах, по имущественным преступлениям, совершённых с использованием информационно-телекоммуникационных технологий**

На территории г.Перми самым распространенным видом преступления в сфере ИТ-преступлений является хищение денежных средств под предлогом проблемы с банковскими картами. Целью преступников в первую очередь является получение информации от потенциальных потерпевших, а именно о наличии имеющихся у них банковских карт и их реквизитов.

Зачастую преступники узнают данные банковской карты от самих потерпевших. Псевдосотрудник банка осуществляет звонок потерпевшему и вводит его в заблуждение о совершении несанкционированных банковских операциях по его банковской карте и просит назвать реквизиты карты либо коды из смс-сообщений. После чего и происходит хищение денежных средств.

Например, мошенники могут использовать такой предлог, как акция от банка. В данном случае при общении с потерпевшим преступник сообщает, что потерпевший выиграл бонусы от банка, и просит продиктовать реквизиты карты с целью начисления данных бонусов. После получения реквизитов карты либо доступа в личный кабинет мобильного банка потерпевшего происходит хищение денежных средств.

При поступлении звонков от псевдосотрудников банков ни в коем случае нельзя сообщать реквизиты банковских карт, пароли, приходящие в смс-сообщениях на сотовый телефон. Необходимо обратиться в ближайшее отделение банка с письменным заявлением о проведении проверки по несанкционированному доступу к банковским счетам потерпевшего.

Сотрудники банков осуществляют звонки своим клиентам в основном:

- когда для них есть персональное предложение в виде кредита со сниженной процентной ставкой, либо кредитной картой или открытие вклада;

- либо при наличии у них кредитной задолженности.

Второй самый распространенный способ – это так называемый «родственник в беде», когда на домашний стационарный телефон потенциального потерпевшего поступает звонок от «родственника», попавшего в трудную ситуацию. В ходе разговора злоумышленник представляется родственником и сообщает, что попал в беду, например, совершил ДТП, подрался, задержали сотрудники полиции, в связи с чем ему нужны денежные средства, чтобы решить данный вопрос. В основном такие преступления совершаются в группе, чаще всего преступниками, ранее уже преступившими закон, но не вставшими на путь исправления. После того, как у преступников получилось обмануть потенциальную жертву, и войти в доверие, к потерпевшему приезжает подельник – так называемый «курьер», – который забирает приготовленные денежные средства и скрывается. Бывали случаи, когда одних и тех же потерпевших обманывали несколько раз за несколько лет. Зачастую жертвами данного вида преступления становятся пожилые люди.

Самым простым способом обезопасить себя и своих близких – это отключить стационарный домашний телефон, возможно, это не совсем удобно для пожилых людей, но данный метод очень эффективен. Также, чтобы не попасться на уловки мошенников, если данный звонок уже поступил, необходимо незамедлительно связаться с близкими родственниками по имеющимся контактам, игнорируя требования злоумышленников.

Еще один способ совершения преступления в сфере ИТ-технологий – это просьба о финансовой помощи со взломанных станиц в социальных сетях. Преступники получают доступ к персональным страницам в социальных сетях различных людей и начинают вести диалоги с добавленными друзьями на этой станице. В ходе общения злоумышленники, пользуясь доверием потенциальных потерпевших, высказывают просьбы об одолжении денежных средств, после чего предоставляют реквизиты подконтрольных им банковских счетов. В основном жертвами становится более молодое население нашего города. В настоящее время видна динамика снижения данного вида преступления в связи с тем, что население становится более бдительным. При поступлении сообщений в социальных сетях от знакомых, друзей или родственников с просьбой финансового характера необходимо также связаться с данным человеком по имеющимся контактам, например, по мобильной связи, и убедиться в достоверности данной просьбы, игнорируя требования преступников.

Также в настоящее время широко распространены сайты бесплатных объявлений, такие как «Авито», «Дром.ру», «Юла», «Из рук в руки», «Авто.ру». Данными сайтами пользуются не только простые обыватели, но и мошенники.

Различают два основных способа совершения мошенничеств с использованием торговых площадок в сети Интернет.

**1. «Обманул покупатель».**

При использовании данного способа совершения преступлений преступники, просматривая объявления на сайте, выбирают те объявления, которые размещают слабо осведомленные социальные слои населения о данном виде мошенничества (женщины, находящиеся в отпусках по уходу за ребенком, жители сельских местностей, несовершеннолетние). Злоумышленники созваниваются с продавцами и убеждают их предоставить данные банковской карты, с целью перевода предоплаты за продаваемый товар, после того, как они получат нужную информацию, похищают денежные средства.

**2. «Обманул продавец».**

При совершении данного вида мошенничества злоумышленники сами размещают объявления о продаже различных товаров, чаще всего это автомобили, запчасти для автомобилей, бытовая техника. С целью привлечения потенциальных потерпевших преступники указывают цену товара значительно ниже среднерыночной. После того, как с ним связывается потерпевший, мошенник убеждает лицо о необходимости внесения предоплаты за товар на подконтрольные ему банковские счета, после получения денежных средств товар не отправляет, дальнейшее общение с потерпевшим прекращает.

В данных способах совершения преступлений большую роль играет убеждение преступниками потенциальных потерпевших в необходимости приобретения или продажи определенного товара. При установлении доверительного контакта мошенники могут использовать различные способы хищения денежных средств потерпевших.

**6 простых правил, которые помогут вам распознать мошенников:**

1. Обращайте внимание на цену товара, не стоит доверять слишком выгодным предложениям, мошенники часто используют этот прием.

2. Осторожнее с предоплатами при покупке, не стоит ее осуществлять.

3. Тщательно проверяйте товар, не отдавайте деньги, пока не проверите товар, если вещь дорогая, то лучше всего выбрать спокойное место для встречи.

4. Задумайтесь, если покупатель на все согласен, будьте бдительны, если покупатель почти не интересуется качеством товара, соглашаясь на все, и предлагает вам предоплату, скорее всего это обман.

5. Не сообщайте полные данные вашей банковской карты.

6. Не переходите по ссылкам в сообщениях от незнакомцев и не открывайте файлы, если не знаете, кто их отправил, особенно на смартфонах.

**Если вы все же стали жертвами мошенников:**

- незамедлительно обратитесь в банк с заявлением о проведении проверки по несанкционированному доступу к банковским счетам и получите выписку о движении денежных средств по банковским счетам;

- обратитесь к оператору сотовой связи либо самостоятельно через личный кабинет получите детализацию телефонных звонков по абонентскому номеру потерпевшего;

- с полученными вышеуказанными документами обратитесь в территориальный орган внутренних дел по месту жительства.

**Управление МВД России по г.Перми**