**Мошенничество в сети «Интернет»**

Количество указанных противоправных деяний продолжает увеличиваться. Высокая степень общественной опасности таких преступлений подтверждается их спецификой - совершить их могут лишь лица, обладающие специальными знаниями и использующие технические средства именно в криминальных целях, что приводит к нарушению не только права собственности граждан, но и банковской тайны. Зачастую пострадавшими являются доверчивые граждане социально уязвимых слоев населения: пенсионеры, несовершеннолетние, граждане, оставшиеся без работы и испытывающие финансовые трудности.

Гражданам необходимо быть бдительными, не поддаваться на звонки и навязывание каких-либо бонусов, товаров, выплат путем использования их банковских карт и телефонов.

В настоящее время наиболее распространены 9 форм хищений денежных средств, совершаемых с использованием IT-технологий:

***1. Хищения, совершенные с использованием сайтов объявлений.***

При данном способе хищения злоумышленник размещает на сайтах объявлений («Авито», «Юла» и др.) информацию о продаже какого-либо товара либо оказании услуги, обязательным условием которых является частичная или полная предоплата, после получения которой денежные средства похищаются, размещенное объявление блокируется.

***2. Хищения, связанные со взломом страниц социальных сетей.***

В указанном случае хищение денежных средств пользователей осуществляется в социальных сетях «ВКонтакте», «Одноклассники», «Инстаграм» путем либо приобретения злоумышленником логинов от взломанных страниц, либо их самостоятельного взлома с последующим размещением на них сообщений подписчикам об оказании финансовой помощи под различными предлогами, в первую очередь, в связи с произошедшим несчастьем, сбором денежных средств «на мечту» и т.д.

***3. Хищения, связанные с платными телефонными номерами.***

В данном случае абоненту поступает SMS-сообщение с просьбой перезвонить на указанный номер с мобильного телефона в связи с произошедшим несчастьем, изменением тарифа связи, проблемами со связью, списанием денег с банковской карты. При осуществлении звонка на телефонный номер, с которого поступило такое сообщение, абонент удерживается на линии и в течение срока ожидания с его мобильного счета списываются денежные средства.

***4. Хищения, совершенные с использованием Интернет-магазинов.***

Злоумышленник регистрирует несколько виртуальных номеров (преимущественно 8-800-.., 8-495-...) и указывает их на созданном Интернет-сайте по продаже товаров в качестве контактных. В последующем принимает заказы от покупателей, похищая оплаченные за товар денежные средства.

***5. Хищения, совершенные с использованием «Фишинга».***

Является одним из самых распространенных видов интернет-мошенничества путем совершения определенных действий, направленных на получение доступа к денежным средствам на счетах банковских карт при помощи почтовых и SMS-рассылок, рекламных объявлений и т.д., содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов банковских организаций, Интернет-площадок и магазинов, на которых предлагается ввести данные карты для возможности ее дальнейшего использования.

***6. Хищения, совершенные под предлогом разблокировки банковской карты или предотвращения списания денежных средств.***

Злоумышленник с абонентских либо виртуальных (8-800-... , 8-495-...) номеров осуществляет звонок на телефон потерпевшего, представляется сотрудником службы безопасности банка или сотрудника правоохранительного органа и сообщает о попытке несанкционированного списания денежных средств с банковской карты, получении кредита, подозрительных операциях, для предотвращения которых просит предоставить контрольные данные банковской карты либо подойти к банкомату для совершения необходимых операций. Иногда для убеждения потенциальной жертвы в почтовый ящик по месту жительства доставляются поддельные уведомления от имени правоохранительных органов о ведущемся расследовании факта хищения c банковской карты и т.д.

***7. Хищения с участием «фальшивых» сотрудников правоохранительных органов.***

В данном случае на телефон абонента поступает звонок лица, представляющегося одним из руководителей правоохранительных органов и прокуратуры с просьбой пополнить его абонентский счет или оказать услугу финансового характера с уверением о последующем возмещении денежных средств. Как правило, данный способ мошенничества ориентирован на лиц, занимающихся предпринимательской либо иной публичной деятельностью, которые, руководствуясь принципом уважения и доверия к правоохранительным органам, переводят требуемые суммы денежных средств через терминал банка либо через иные финансовые услуги.

***8. Хищения, совершенные под предлогом помощи родственнику, попавшему в беду.***

При указанном способе хищения на стационарный или абонентский номер потерпевшего звонит злоумышленник, который обращаясь под видом родственника сообщает, что попал в беду (совершил ДТП и сбил человека, с кем-то подрался и т.д.), после чего передает трубку другому лицу, представляющемуся сотрудником полиции, который за отдельную плату предлагает решить вопрос об отказе в возбуждении уголовного дела.

***9. Ошибочный перевод средств.***

В этом случае абоненту поступает два SMS-сообщения, одно из которых о зачислении на его счет с помощью услуги «Мобильный перевод» денежных средств, второе – от неизвестного лица об ошибочном совершении операции с просьбой возврата денежных средств. В действительности деньги на счет потерпевшего не поступают, мошеннику переводятся собственные финансы.

***Не осталась вне поля зрения мошенников ситуация с пандемией, обусловленной возникновением новой коронавирусной инфекции.***

Так, правоохранительными органами фиксируются факты хищений денежных средств путем направления злоумышленниками
СМС-уведомлений о начислении компенсации за нерабочий период во время эпидемии, для получения которой предлагается перезвонить в банк; осуществления звонков «сотрудниками лаборатории» о срочной необходимости сдачи платного анализа в связи с имевшимися контактами с заболевшими, для отбора которых выездной бригадой в целях соблюдения режима самоизоляции требуется предоплата.

В обоих случаях у потерпевших выясняются сведения о счете банковской карты с последующим списанием с него денежных средств.

При совершении такого рода преступлений необходимо незамедлительно обращаться в органы полиции.

**Разъясняет прокурор Болховского района К.И.Петраков**