Мошенники год за годом придумывают новые способы завладения денежными средствами граждан. Преступления данной категории очень сложны в раскрытии, требуют проведения огромного комплекса технических и оперативных мероприятий. Зачастую они совершаются лицами, находящимися в других регионах. Полиции удается раскрывать подобные преступления. Но мы считаем, что лучше быть предупрежденным заранее и самостоятельно оградить себя от мошенников, прежде чем «попасться на их удочку».

Несмотря на предпринимаемые сотрудниками полиции профилактические меры на территории Октябрьского района продолжается увеличение количества совершенных мошенничеств. На сегодняшний день наиболее распространенным стало дистанционное мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий, т.е. средств сотовой связи и сети «Интернет». В 2020 году На 29% возросло число преступлений, совершенных с использованием информационно-телекоммуникационных технологий (с 81 в 2019 до 105 в 2020 году), раскрыто и направлены в суд уголовные дела по – 23 преступлениям (что +3,8 раза больше чем в 2019 году; в 2019 г.- было раскрыто только 6 преступлений). В числе преступлений, совершенных с использованием ИТТ, большую часть (53,3%) составляют дистанционные мошенничества (+55,6%; с 36 до 56). В 2020 году жители Октябрьского района в результате мошеннических действий лишились несколько миллионов рублей. С начала текущего года на территории района зарегистрировано более 30 фактов мошенничества совершенных с использованием информационно-телекоммуникационных технологий.

Злоумышленники постоянно совершенствуются и изобретают все новые схемы завладения денежными средствами доверчивых граждан. Можно выделить несколько наиболее распространенных преступных схем бесконтактного мошенничества, используемых аферистами зарегистрированными на территории Октябрьского района.

«Мошенничество с предоплатой»

В последнее время участились случаи совершения мошенничеств с использованием популярных сайтов и социальных сетей. Ситуации могут развиваться по нескольким направлениям:

— Мошенники размещают на сайте объявления о продаже по низким ценам каких-либо вещей, техники, транспортных средств, недвижимости и т.п., затем просят покупателя внести предоплату, а после перевода денежных средств номер лже-продавца перестает отвечать.

- Противоположная ситуация, когда гражданину, разместившему на популярных сайтах объявление о продаже своего имущества, поступает звонок от, якобы, потенциального покупателя. Мошенник предлагает перевести предоплату за товар и для этого запрашивает реквизиты банковских карт продавца, получая тем самым доступ к денежным средствам, находящимся на его счетах.

«Взлом аккаунта в социальных сетях»

Мошенники, пользуясь беспечностью граждан, путем использования специального программного обеспечения, получают доступ к страницам пользователей социальных сетей. После чего злоумышленники от имени пользователя запускают рассылку сообщений всем контактам «взломанной страницы» с просьбой оказать материальную помощь в сложной жизненной ситуации или дать в долг.

«Ваша карта заблокирована»

Еще один способ мошенничества, неоднократно освещаемый в СМИ, однако, не теряющий своей актуальности. Гражданину звонит незнакомец, представляясь сотрудником банка, и сообщает о блокировке банковской карты, либо на телефон приходит соответствующее СМС-сообщение. Чтобы решить эту проблему, злоумышленник, под предлогом уточнения информации, выясняет данные карты или вынуждает гражданина самостоятельно воспользоваться банкоматом, набрать определенную

комбинацию цифр и, тем самым, совершить операцию по переводу своих денежных средств на сторонний счет.

«Ваш родственник стал виновником смертельного ДТП»

По прежнему аферисты используют старую стандартную мошенническая схема, когда злоумышленник звонит на стационарный или мобильный телефон, представляется сотрудником полиции и сообщает гражданину о том, что его сын (дочь) задержан (а) за совершение тяжкого преступления, либо кто-то из родственников стал виновником ДТП, в результате которого под колесами его автомобиля погиб человек. Для того, чтобы родственнику избежать уголовной ответственности, мошенник предлагает заплатить определенную сумму денег. Деньги, как правило, просят передать курьеру или перевести через платежный терминал на указанный расчетный счет или телефонный номер.

Новые виды телефонного мошенничества

Внушительное число граждан уже осведомлены о типичных случаях мошенничества, которое совершается с использованием мобильной связи. Тем не менее, злоумышленники совершенствуют способы мошенничества, о которых потенциальные жертвы не осведомлены.

Так, распространение получила мошенническая схема с незаконным использованием подменных абонентских номеров (используются номера банков и подразделений МВД России). Звонок осуществляется якобы сотрудником банка, который информирует о попытке оформления неизвестным третьим лицом кредита в онлайн-банке. Далее злоумышленник убеждает гражданина в необходимости самостоятельно оформить онлайн-кредит на ту же сумму, обналичить поступившие на банковскую карту деньги и перечислить их на так называемый резервный счет для мгновенного погашения кредита. Для подтверждения информации звонок поступает якобы от "сотрудника полиции", который подтверждает слова мошенника, представившегося сотрудником банка. Один факт данной схемы уже был зафиксирован в этом году в Октябрьском районе.

Также соответствующая схема может быть реализована с помощью автоматизированных систем. В настоящее время около 30% мошеннических

звонков проходит с применением роботов: около 10% — с использованием робота в начале диалога и еще около 20% — с переключением на робота, чтобы сообщить ему конфиденциальные сведения, которые доступны только клиенту (например, код подтверждения совершения банковской транзакции из СМС). По мнению экспертов, преимущество роботов заключается в том, что они вызывают доверие жертвы и, как следствие, повышают результативность мошеннических действий. При необходимости получения конфиденциальной информации робот помогает ввести клиента в заблуждение, убедив, что клиент сообщает код не сотруднику банка, а защищенной системе. В дополнение к этому злоумышленники используют психологический прием и перед переключением на робота напоминают жертве, что нельзя называть секретные коды сотрудникам банка, подразумевая, что сотруднику сообщать конфиденциальную информацию нельзя, а роботу — можно.

Уважаемые граждане!

Соблюдение элементарных правил поможет вам не стать жертвой мошенников и сохранить личное имущество. Потерпевшими от преступных действий злоумышленников становятся не только излишне доверчивые пенсионеры, но и молодые люди. Поэтому стоит как можно чаще напоминать своим родственникам и знакомым о том, как действуют мошенники и объяснять, что ни при каких обстоятельствах не следует перечислять деньги незнакомым людям или сообщать свои персональные данные, логины, пароли и коды банковских карт.

- При получении сообщения о заблокированной банковской карте следует перезвонить на номер круглосуточной справочной службы, указанный на карте, а не на номер, присланный в сообщении.

— Не торопитесь предпринимать какие-либо действия, если на ваш телефон поступили сообщение или звонок с просьбой о незамедлительной помощи родственнику, якобы попавшему в неприятную ситуацию или о блокировании вашей банковской карты.

- Отнеситесь более ответственно к созданию паролей и логинов к своим личным страницам, старайтесь чаще их менять и не использовать один пароль для всех возможных случаев. Не сообщайте никому PIN-код и CVV2-код карты (**цифры с обратной стороны карты**), а также срок её действия и персональные данные владельца. Ни один банк не будет по телефону запрашивать у вас эти реквизиты. Для зачисления средств на ваш счёт достаточно лишь 16-значного номера, указанного на лицевой стороне карты.

Не сообщайте неизвестным лицам пин-код для входа в ваш онлайн-банк — для перевода денежных средств это не требуется.

Не используйте карты со своим основным финансовым капиталом для оплаты товаров и услуг в сети Интернет.

Не рекомендуется входить в интернет-банк с чужих компьютеров или из незащищенных публичных сетей Wi-Fi.

На личном компьютере, смартфоне, планшете установите антивирусное программное обеспечение и своевременно его обновляйте.

Не скачивайте файлы из непроверенных источников (файлообменные сервисы, социальные сети). Не переходите по ссылкам на информационные ресурсы, полученным от сомнительных источников. Не открывайте файлы из подозрительной электронной почты.

— При покупке товаров в сети «Интернет» нужно помнить, что современные технологии позволяют за считанные минуты создавать в Интернет-пространстве сайты, страницы, аккаунты в социальных сетях. Мошенники активно используют данную возможность, привлекая потенциальную жертву, прежде всего, низкими ценами, быстрой доставкой и качеством предоставляемых товаров или услуг, при этом злоумышленники требуют предоплату.

Не доверяйте виртуальному собеседнику, если его аккаунт недавно создан. Не перечисляйте деньги, не убедившись в благонадежности продавца и не увидев товар в реальности.

— Не производите расчеты через непроверенные сайты.

Постарайтесь оплатить товар «из рук – в руки» при его получении в ходе личной встречи.

Если вы все же решились купить товар по предоплате, поищите информацию о продавце в Интернете. Любая деталь поможет, в случае обмана, найти злоумышленника и привлечь его к ответственности.

В случае совершения мошенничества в отношении вас или ваших близких, незамедлительно обращайтесь в органы внутренних дел, так как вовремя поступивший сигнал поможет полицейским быстрее раскрыть преступление и предотвратить совершение новых.