Основные виды и способы совершения мошенничеств и краж денежных средств

1. Мошенничества, совершенные с использованием средств сотовой связи и Интернет-ресурсов

- заражение вирусами сотовых телефонов, работающих на операционных системах «Андроид» с подключенной услугой «мобильный банк»

Данному виду преступлений в основном подвергнуты клиенты ОАО «Сбербанк России», так как банком при открытии счета гражданам услуга «мобильный банк» подключается автоматически, а для ее отключения необходимо написать заявление, о чем не всегда предупреждают клиентов.

В настоящее время можно выделить три основных способа, при помощи которых совершаются хищения денежных средств, но сразу следует пояснить, что данный перечень не исчерпывающий, так как возможны абсолютно иные способы хищений денежных средств, а также измененные или скомбинированные из различных способов.

Способ «Двойной «Мобильный банк».

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «мобильному банку». По различным причинам, многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи, с чем оператор сотовой связи через 6 месяцев перевыпускает СИМ-карту с данным абонентским номером и выставляет ее на продажу. Также возможна утеря СИМ-карты и неотключение ее «мобильного банка».

Новый абонент приобретая данную СИМ-карту начинает получать СМС о движении денежных средств по счёту потерпевшего, кроме того он получает возможность управлять денежными средствами лицевого счета, к которому она подключена.

Меры противодействия: в случае утраты сим-карты, либо ее неиспользовании более полугода отключить услугу «мобильный банк»

Способ «Вредоносные программы».

*Способы заражения вредоносным программным обеспечением (ВПО) телефонных аппаратов на операционной системе «**Android**».*

1. Потерпевший получает СМС-сообщение от контент-провайдера, в котором находится ссылка на информационный ресурс, перейдя по которой, абонент закачивает на телефон вредоносное программное обеспечение (далее ВПО).

2. Потерпевший получает СМС-сообщение от своего «знакомого», телефон которого уже заражен ВПО, при этом ВПО само направляет данное сообщение на номера, которые имеются в адресной книге потерпевшего. В данном сообщении также находится ссылка на

информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

3. Потерпевший, находясь в сети «Интернет», с помощью телефона, получает по электронной почте, либо через социальные сети, ICQ сообщение, в котором находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

4. Потерпевший, находясь в сети «Интернет», с помощью телефона, скачивает, например, программные продукты, музыку, фотографии, в которых находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

Поле заражения телефона «вирус» проверяет наличие подключенной услуги «Мобильный банк». Если услуга подключена, то вирус с помощью нее осуществляет перевод денежных средств с банковской карты протерпевшего на различные абонентские телефонные номера, электронные платежные системы (Киви-кошелек и др.), либо на лицевой счет абонентского телефонного номера потерпевшего и далее на электронные платежные системы, либо банковские карты преступника. При этом вирус блокирует (не выводит на дисплей телефона, а также удаляет их из телефона потерпевшего) информационные СМС-сообщения о произведенных транзакциях, которые поступают от Банка.

Меры противодействия: гражданам, имеющим телефоны, работающие на операционной системе «Андроид», в случае получения СМС, ММС и др. сообщений (в т.ч. от своих «знакомых»), содержащих ссылки на незнакомые ресурсы ни в коем случае не переходить по ним, не скачивать программные продукты с сомнительных сайтов.

- взлом странички в социальной сети «ВКонтакте»

Преступниками осуществляется взлом странички в социальной сети пользователя, после чего посредством электронной переписки предлагает его друзьям под различными предлогами перевести денежные средства якобы для пользователя, при этом друзья переводят деньги без опаски, считая, что помогает своему товарищу.

Также преступник получает доступ к личным фото-, видео-материалам потерпевшего, зачастую интимного характера, и в дальнейшей требует перевода определенной суммы денежных средств за нераспространение указанной информации среди друзей и родственников потерпевшего в сети Интернет.

Меры противодействия: обезопасить себя от взлома возможно периодически меняя пароль от вашей учетной записи в социальной сети, при подключении к ресурсу социальной сети рекомендуется вводить пароль вручную, отключив функцию его автоматического ввода.

- покупка-продажа товаров через Интернет-сайты

При осуществлении мошенничества в сети Интернет преступления в основном совершаются под предлогами реализации потерпевшим различных товаров, при которых преступники делают якобы выгодные предложения, обещают бесплатную доставку, сниженные цены и т. п.

Потерпевшими становятся в основном лица, которые ранее приобретали какие-либо товары и услуги через Интернет и доверяют этому способу реализации, сайтам с объявлениями и т. п.

<u>1 способ:</u> Преступник размещает на сайте электронных объявлений (Из «Рук в Руки» «Авито» или иных) объявление о продаже каких-либо товаров на территории Республики Марий Эл, для связи указывает телефон либо электронную почту.

Потерпевший обнаруживает объявление, и решает приобрести заявленные в нем товары.

Потерпевший созванивается с преступником по указанному в объявлении абонентскому номеру сотовой связи, преступник сообщает ему, что товар имеется в наличии и он готов его продать. Показать товар преступник под разными предлогами отказывается, сообщает что находится в другом городе (субъекте РФ), и предлагает переслать фото товара на электронную почту.

Преступник сообщает потерпевшему адрес электронной почты для связи либо узнает у потерпевшего адрес его электронной почты.

Преступник и потерпевший некоторое время ведут электронную переписку, при этом преступник как правило демонстрирует потерпевшему фотографии товара, заверяет в надежности и качестве. Оговаривается цена товара, способ оплаты и сроки поставки.

Потерпевший перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек, мелкие суммы на счет абонентского номера.

Еще один вариант данного способа, когда преступник сам звонит по объявлениям о продаже товара, сообщает, что товар его очень заинтересовал, он готов его купить, желает внести предоплату, чтобы товар не был продан другому покупателю, для чего в ходе общения с продавцом узнает номер и CUV-код его банковской карты, после чего с карты продавца успешно списываются денежные средства, а связь с покупателем пропадает.

<u>2 способ:</u> Преступник создает в сети Интернет сайт в виде магазина (либо зеркальный сайт-двойник известного магазина) для продажи различных товаров, указывает значительный ассортимент, невысокие цены и т.п. для привлечения клиентов.

Потерпевший обнаруживает сайт и решает заказать какой-либо товар, регистрируется на сайте, указывает свои данные, оформляет доставку.

Потерпевший получает от магазина электронные письма с подтверждением заказа, ему высылается счет на оплату либо указываются реквизиты банка, электронной платежной системы для платежа.

В некоторых случаях потерпевший звонит на указанные на сайте либо в электронных письмах номера, где преступник либо его сообщники заверяют потерпевшего в том что заказ принят, оговаривают сроки

поставки и т.п., создавая у потерпевшего впечатление о реальности и честности магазина.

Потерпевший оплачивает выставленный ему счет, перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек.

Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

3 способ: преступник создает в социальной сети (Одноклассники, ВКонтакте) тематические группы либо объявления о продаже различных товаров, указывает значительный ассортимент, невысокие цены и т.п. для привлечения клиентов. Социальные сети допускают публикацию изображений и видеоматериалов, отражающих свойства товаров.

Потерпевший обнаруживает объявления и решает приобрести товар, для чего вступает с преступником в электронную переписку посредством системы обмена сообщениями в социальной сети.

Потерпевший ведет с преступником электронную переписку, по достижению договоренности о покупке ему высылается счет на оплату либо указываются реквизиты банка, электронной платежной системы для платежа.

В некоторых случаях потерпевший звонит на указанные в объявлении телефоны, где преступник либо его сообщники заверяют потерпевшего в том что заказ принят, оговаривают сроки поставки и т.п., создавая у потерпевшего впечатление о реальности и честности продавца.

Потерпевший оплачивает выставленный ему счет, перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек.

Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

Преступник либо его сообщники обналичивают собранные денежные средства, после чего прекращается всякое взаимодействие с потерпевшим.

Некоторое время после перечисления потерпевшим денежных средств, с целью сокрытия следов своей деятельности преступники отвечают потерпевшему на его звонки, электронные письма, под рядом предлогом откладывая поставку товара.

Меры противодействия: помните, что предоплату за товар вы вносите на свой страх и риск, 100%-ой гарантии получения товара не существует. При заказе товаров внимательно проверяете название сайта в адресной строке браузера, чтобы не попасть на сайт-двойник. Пользуйтесь услугами Интернет-магазинов, работающих длительное время и заслуживших положительную репутацию покупателей, читайте отзывы покупателей о работе данных Интернет-магазинов.

Ни при каких обстоятельствах, как бы вас не уговаривал продавец (покупатель), не сообщайте номер вашей банковской карты вместе с CUV-кодом (указан на оборотной стороне банковской карты)

- сообщение о блокировке банковской карты, либо списании с нее денежных средств

Преступник осуществляет звонок на телефон (отправляет СМС-сообщение) потерпевшему и сообщает о том, что его банковская карта заблокирована (или о иной проблеме со счетом, пластиковой картой). Для того чтобы решить проблему необходимо в короткий срок оказаться рядом с банкоматом и осуществить ряд операций, которые будет диктовать преступник.

Потерпевший, дойдя до банкомата, созванивается с преступником и выполняет все его действия.

Преступник сообщает потерпевшему набор цифр для устранения проблем с картой (счетом).

При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

Подельник преступника, осуществивший снятие денежных средств с расчетного счета, использует банкомат (терминал или Интернет) осуществляет перевод денежных средств преступнику.

Меры противодействия: помните главное: банки никогда не звонят своим клиентам с просьбой представиться, назвать номер карты и CUV-код. Все возникшие неисправности банк устраняет самостоятельно, не привлекая клиентов. Не вступайте в беседы с незнакомцами, которые представляются работниками службы безопасности банка, не выполняйте их поручения, полученные по телефону. В случае возникновения вопросов необходимо обратиться в ближайшее отделение банка, либо позвонить по телефону «горячей линии», который указан на оборотной стороне каждой банковской карты.

- сообщение о том, что родственник попал в беду

Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) проблема (попал в ДТП, совершил преступление, иное) и предлагает разрешить проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается и самостоятельно выполняет платежные операции (схема аналогична случаю с сообщениями о блокировке банковских карт).

Меры противодействия: Не вступайте в беседы с незнакомцами, которые звонят (отправляют сообщения) с неизвестных вам номеров, представляются вашими знакомыми, родственниками, сотрудниками правоохранительных органов, и просят перечислить денежные средства. Ни что не мешает вам прервать разговор и перезвонить своим знакомым, родственникам, уточнив, действительно ли с ним случились неприятности.

- сообщение о выигрыше

Преступник осуществляет отправку потерпевшему СМС-сообщения о выигрыше какого-либо приза, при этом указывая номер контактного телефона по которому необходимо позвонить.

Потерпевший звонит по указанному телефону и ему поясняют, что для получения выигрыша необходимо оплатить стоимость доставки, причем запрашиваемые суммы не столь велики, так что подозрения у граждан не вызывают. Естественно, после оплаты доставки потерпевший никакого приза не получает.

Меры противодействия: запомните главное правило – «халявы» не бывает! Не задумываясь удаляйте из телефона полученные сообщения о выигрыше BMW, Mercedes, Apple IPhone и т.д.! Не будьте жадными!

2. Социальные мошенничества

- мошенничества под видом работников социальной сферы

На мошенничествах данного вида в основном специализируются лица цыганской национальности женского пола. Жертвами преступлений в основном являются одинокие престарелые граждане, зачастую слабовидящие, в жилища к которым преступники попадают под видом работников социальной сферы, поясняя пенсионерам, что им положена компенсация по оплате коммунальных услуг. Потерпевшим передается купюра, зачастую номиналом 5000 рублей, и предлагается вернуть определенную сумму для сдачи. После ухода «соцработников» потерпевший обнаруживает, что купюра является билетом «Банка приколов».

Меры противодействия: не впускайте в жилище посторонних, требуйте представить документы, подтверждающие принадлежность к той или иной организации. Не поленитесь позвонить в данную организацию и уточнить, работает, ли там сотрудник и действительно ли вам положены какие-либо выплаты.

- мошенничества под видом денежной реформы

Способ аналогичен предыдущему, преступники сообщают пожилым гражданам о проведении денежной реформы и необходимости обмена старых денег на новые, потерпевшие осуществляют обмен своих сбережений на билеты «Банка приколов».

Меры противодействия: Реформа денежных знаков давно проведена. Не впускайте в жилище посторонних, сообщите об их визите родственникам, соседям или в полицию.

- мошенничество под видом гадания и снятия порчи

Классический способ, на котором специализируются лица цыганской национальности женского пола. Преступления данного вида совершаются как на улицах, так и в жилищах граждан, в которые преступники проникают под различными предлогами. Основной задачей мошенников является завязать разговор с жертвой и в дальнейшем убедить ее, что на нее, либо на ее имущество (золото, деньги) наложена порча или сглаз. Если потерпевший сразу не пресекает данные попытки, то вскоре самостоятельно передает преступникам золотые изделия или деньги. Как

правило, лишь спустя время гражданин понимает, что его обманули, но причину добровольной передачи имущества пояснить не может.

Меры противодействия: главное правило – не вступать с данными лицами в разговор, не выполнять их просьбы, не отвечать на их вопросы. Если жуликам удалось завести с вами доверительную беседу, то денег и ценностей вы лишитесь!

3. Подлом пачки денег

Как правило, данные преступления совершаются в торговых точках преступниками, имеющими определенные навыки обращения с денежными купюрами. В текущем году зарегистрировано 2 преступления данной категории на территории г.Йошкар-Олы.

Преступник обращался к кассирам с просьбой обменять старые тысячерублевые купюры на новые и в процессе разговора и отбора нужных купюр «ломал» пачку и осуществлял хищение денежных средств. При этом кассиры добровольно раскладывали перед преступником имеющуюся денежную наличность, чтобы он сам смог выбрать необходимые банкноты.

Меры противодействия: касается трудящихся, работающих с денежной наличностью в сфере торговли или оказания услуг (кассиров АЗС, продавцов магазинов и т.д.). При обращении незнакомцев с просьбой разменять, обменять денежные знаки, старайтесь отвечать отказом. Ни в коем случае не передавайте неизвестным денежные средства, находящиеся в кассовых аппаратах для того, чтобы они могли самостоятельно выбрать интересующие купюры. Тщательно пересчитывайте полученные деньги непосредственно после момента передачи, насторожитесь, если вас просят возвратить деньги обратно: как правило «подлом» пачки купюр происходит во время данных манипуляций. Не забывайте проверять крупные банкноты на подлинность.