ОСТОРОЖНО МОШЕННИКИ!

В настоящее время наблюдается рост мошенничеств, совершаемых с использованием современных средств связи и глобальной сети «Интернет». Примерами мошеннических действий могут являться ситуации:

Блокировка банковской карты.

Смс-сообщения о блокировке банковской карты приходят с различных номеров, включая 8 800, 8 495 и номера схожие с 900. После чего человек перезванивает на указанный в сообщении номер, где на звонок может ответить либо девушка, либо мужчина, которые, представляются сотрудниками банка. Далее мошенники поясняют, что с банковской карты были не санкционированно списаны деньги, либо она заблокирована, и для того чтобы разблокировать карту и предотвратить списание денежных средств необходимо подойти к ближайшему банкомату. Когда человек подходит к банкомату он под руководством мошенника вставляет банковскую карту в банкомат и набирая определенные комбинации в банкомате, под диктовку мошенника, переводит со своей банковской карты денежные средства на различные счета мошенника.

Родственник попал в беду.

Звонок совершается на стационарный номер телефона, используемый престарелым гражданином. При этом злоумышленник искажает голос, делает невнятную речь поясняя что якобы разбит нос или губа, после чего говорит что задержан и находится в полиции за драку либо ДТП, и передает трубку «сотруднику полиции», чаще всего мошенник представляется «следователем», после этого требует от граждан определенную сумму денег для того чтобы на родственника не возбуждали уголовное дело,

либо для выплаты денег потерпевшему. При этом мошенник не дает гражданам возможности позвонить родственнику, так как просит, чтобы человек всегда был на связи и не отключался. В конце концов, обманутый гражданин передает деньги либо курьеру, которого заранее направил мошенник, либо перечисляет сам на различные счета мошенника

Вирусы.

Как правило, граждане, пострадавшие от действий такого вида мошенничества являются держателями банковских карт «Сбербанк», с подключенной услугой «Мобильный банк». То есть, человек пользуясь телефоном, осуществляет выход в Интернет, где в основном через приложение «Плей-маркет, магазин Apple и Microsoft» скачивает различные программы, либо игры, на которых уже имеется вирус. Когда Вы решили продать какую-либо вещь на сайтах бесплатных объявлений. Не редко после публикации объявлений Вам могут поступать на абонентский номер, указанный как контактный, СМС сообщения следующего вида: Сергей, давай меняться? О! Сергей, не ожидал от тебя такого, это действительно ты на фото??? А далее ссылка вида: http:yxYOPI-_Cdyhd. Перейдя по указанной ссылке, скорее всего, получите информацию о невозможности перехода. Данный вирус, попадая в телефон, полностью «сканирует» телефон и получает доступ через услугу мобильный банк к банковской карте и в последствии мошенник удаленным доступом может распоряжаться денежными средствами человека с его карты, без ведома владельца банковской карты. Как правило, денежные средства перечисляются на различные банковские счета или же на абонентский номер самого потерпевшего, а уже с него на банковские карты.

Покупки в интернете.

В настоящее время существует много сайтов, на которые осуществляется продажа товара. Как правило, данные сайты требуют 100% предоплату за заказанный товар, после чего сайт блокируется, номера телефонов отключаются. Так же это касается социальных сетей «В контакте» и «Одноклассники», где мошенник создает страницу и под видом представителя какой-либо компании осуществляет продажу того либо иного товара. Соответственно так же при оплате требует 100% предоплату (продажа одежды, техники, автозапчастей и.т.д.).

Сложность в раскрытии данной категории преступления состоит в том, что все сайты, с которых происходит продажа товарно-материальных ценностей, регистрируются в различных регионах на подставных лиц. Что значительно осложняет поиск злоумышленников.

Продажа товара в интернете.

Когда человек выкладывает на продажу имущество, оставляя свой контактный телефон для связи. На телефон человека звонит мошенник, поясняет, что он хочет приобрести товар, при этом говорит, что находиться в другом городе. После просит продиктовать номер банковской карты, как с лицевой стороны, так и с обратной, чтобы якобы перечислить оплату за товар. Человек ничего не подозревая, говорит номера своей карты, и впоследствии, с его карты списываются денежные средства на различные счета мошенника.

Взлом страничек в социальных сетях «ВКонтакте».

Мошенник, выдавая себя за (хозяина аккаунта) владельца странички, ведет переписку с родственниками и

знакомыми, и под различными предлогами просит перевести денежные средства на абонентский номер либо на банковскую карту, кроме того пытается завладеть данными банковской карты, после чего с банковской карты происходит списания денежных средств в различных суммах.

Пользователям социальных сетей надо помнить о том, что необходимо перепроверять любую поступившую информацию, для чего можно просто связаться с другом и уточнить, действительно ли ему нужна помощь. В случае взлома аккаунта, необходимо обратиться к администратору социальной сети, а с целью недопущения взлома вашей страницы в социальных сетях меняйте чаще пароли, не заходите на подозрительные сайты, запрашивающие ваши логины пароли, регулярно проверяйте компьютеры на наличие вирусных программ, которые могут передавать мошенникам пароли от аккаунта.

Электронные биржи.

В сети интернет люди часто сталкиваются с рекламой быстрого заработка денежных средств на различных фондовых биржах. То есть граждан завлекают возможностью получения большой прибыли от вложения их денег в различные товарно-сырьевые, фондовые или валютные биржи. Некоторое время дают возможность якобы заработать, а в дальнейшем при вложении большой суммы Вы теряете все или по факту денежные средства невозможно вывести. Кроме того, имеются случаи, когда Ваш личный менеджер попросит Вас установить некую программу, которая позволит ему удаленно управлять Вашим компьютером.

Онлайн кредиты.

Всем нужны деньги, а некоторым срочно и много, но не все имеют положительную кредитную историю, поэтому размещают объявления в сети интернет сами или находят объявления о предоставлении различных займов. Вы сами или мошенник звонит и поясняет, что он является руководителем среднего звена в одном из банков и готов за некоторое вознаграждение или первоначальную страховку пропустить Вашу заявку на кредит. После согласия гражданина мошенник просит подойти в банк и перед подачей документов произвести оплату на подконтрольные ему счета

Возврат вещей.

Многие граждане при утрате вещей размещают объявления на различных сайтах в сети Интернет, социальных сетях. Мошенники этим пользуются и перезванивают на указанный в объявлении номера, представляются сотрудниками ломбарда и просят перевести на указанный им абонентский номер денежные средства, объясняя тем, что сам встретиться не может ввиду опасения за свое здоровье. Ошибка граждан в том, что они сами размещают полное описание вещи и мошенники просто называют описание

Когда человек желает приобрести товар, увиденный на сайте бесплатных объявлений, как правило, человека заманивает цена на товар, так как она на порядок ниже рыночной. Человек звонит мошеннику и говорит, что хочет приобрести товар, на что мошенник чаще всего отвечает о том, что он находиться в другом городе, и ему срочно нужны деньги на операцию родственнику, либо иная причина, в связи, с чем он так дешево продает товар. После мошенник требует предоплату в различных суммах, чтобы

не продать товар другому лицу. Впоследствии человек перечисляет предоплату на счет мошенника. После чего абонентский номер мошенника отключается, либо мошенник начинает звонить и требовать полную стоимость товара, иначе он продаст его другому человеку.

ВАЖНО!

- Никогда не перечислять предоплату пока не увидите товар лично, не поддаваться «дешевой» цене за товар.
- Если Вы не имеете ни какого представления о работе финансового рынка, то даже не стоит пробовать, тем более, что некоторые торговые платформы созданы только для того, чтобы вы вложили денежные средства.
- Не паниковать, уточнить у мошенника полные анкетные данные своего родственника, что соответственно мошенник знать не может, незамедлительно позвонить своему родственнику и убедиться что с ним все в порядке.
- Не осуществлять покупку на не проверенных сайтах, перед покупкой обратить внимание на отзывы, посмотреть дату создания сайта, проверить ресурс через сайт «Whois», где будет отображена дата создания сайта, т.е если сайт существует меньше года, это должно вызвать подозрение, ну и соответственно не отправлять предоплату, ни в каких суммах по не проверенным сайтам. Ну и опять же не соблазняться заниженной ценой товара
- при получении смс-сообщения, не паниковать, не бежать к банкомату, следует позвонить в горячую линию своего банка (номер обычно указан на обратной стороне карты), не диктовать ни каких номеров с карты, как на передней стороне, так и на обратной. Сотруднику банка не нужна данная информация для идентификации Вашей личности. Если отсутствует возможность позвонить, пройти в ближайшее отделение своего банка и уточнить там информацию.