**ГРАЖДАНЕ, БУДЬТЕ БДИТЕЛЬНЫ!**

**УБЕРЕГИТЕ СЕБЯ, СВОИХ РОДНЫХ И ЗНАКОМЫХ ОТ ПОСЯГАТЕЛЬСТВ МОШЕННИКОВ!**

Проведенный сотрудниками полиции анализ, свидетельствует о том, что в последнее время на территории ЗАТО Сибирский, а в целом и на территории Российской Федерации существенно осложнилась оперативная обстановка связанная с мошенничествами и совершением хищения денежных средств, с банковских карт и счетов граждан, данные преступления совершаются с использованием средств сотовой связи и Интернет-ресурсов.

В настоящее время используются следующие схемы совершения мошенничеств:

***1. «Ваша банковская карта заблокирована»,*** для совершения хищения по данной схеме, исполнитель рассылает СМС-сообщения на абонентские номера граждан, от имени службы безопасности банка и указывает контактный абонентский номер для обратной связи. В процессе звонка с потерпевшим происходит беседа с мнимым сотрудником службы безопасности банка, который в свою очередь поясняет, что произошел сбой системы и ряд банковских карт заблокировано, и для устранения неполадок предлагает потерпевшему при помощи банкомата произвести следующую операцию: «вставить банковскую карту – ввести пин-код – зайти в меню «оплата услуг» – выбрать «платежи» – далее «Билайн» – ввести абонентский номер – выбрать позицию «без оплаты» - забрать карту», которая в последствии приводит к автоматическому подключению услуги операторов сотовой связи «Мобильный кошелек», затем разговор заканчивается. После чего мошенник осуществляет перевод денежных средств имеющихся на карте на абонентский номер, который самим же потерпевшим и был введен ранее. Также мошенники при использовании данной схемы просят потерпевших назвать реквизиты своей банковской карты, с которой в последующем происходит перечисление денежных средств на абонентские номера по услуге «Мобильный кошелек».

***2. «Вам в сотовый телефон системы «Андроид» автоматически поступает вирус»,*** хищения денежных средств данного вида совершаются в отношении граждан, которые пользуются услугами мобильный банк и интернет ресурсами со своего сотового телефона, т.е. у вас имеется банковская карта, на которой подключена услуга мобильный банк. Данная услуга подключается на абонентский номер вашего сотового телефона и вам после проведения, каких-либо банковских операций по карте поступают смс оповещения. В дальнейшем вы пользуетесь на своём сотовом телефоне Интернет-ресурсами, в один из дней вам понадобились обновления приложений системы «Андроид», которые вы закачиваете с интернета, совместно с приобретенными вами приложениями на ваш сотовый телефон автоматически поступает вирусная программа, вы на первый взгляд не определите о том, что она имеется у вас в наличии. Но в дальнейшем данная вирусная программа делает своё дело, она собирает всю информацию о вашей банковской карте, которая привязана на ваш абонентский номер сотового телефона и в дальнейшем вся собранная информация смс-сообщением отправляется с вашего сотового телефона на телефон мошенника. После чего мошеннику становится известны все ваши коды по банковской карте, что ему позволяет без всяких трудностей в системе интернет при помощи мобильного банка и вашего личного кабинета совершить операции по вашей банковской карте, т.е совершить хищение денежных средств со всех банковских счетов, которые у вас имеются. При совершении преступником хищения денежных средств, с вашей банковской карты, вам на сотовый телефон смс-оповещение о проведении операций по карте не поступают, как правило вам становиться это известно только после того, как вы обратитесь к сотрудникам банка. Помимо указанного способа попадания вирусного программного обеспечения, имеются и иные способы – например, посредством направления на Ваш сотовый телефон ммс-сообщения, содержащего ссылку, под видом картинки, при переходе по которой посредством Интернет-браузера происходит скачивание вируса. В последнее время распространена рассылка ммс-сообщением под предлогом обмена или просмотра товара по размещенному объявлению на Интернет-ресурсах размещения объявлений о продаже различных товаров – «Авито», «Юла» и т.п.

***3. «Задаток за покупку покупаемой вещи по Вашему объявлению»,*** В последнее время является одним из самых распространенных способов хищения денежных средств. Хищение денежных средств происходит следующим образом – Вы размещаете объявление на сайтах продаж товаров вторичного использования («Авито», «Юла», и т.п.). Через некоторое время – как правило в течении нескольких дней, Вам поступает звонок, в ходе разговора злоумышленник сообщает, что ему очень понравился продаваемый Вами товар, он хотел бы приобрести его, однако в настоящее время за пределами Алтайского края, ввиду чего просит «придержать» данный товар, предлагая Вам перевести задаток на Вашу банковскую карту. После получения номера банковской карты сообщает Вам, что, по неизвестным причинам, у него не получается произвести операцию перевода, просит сообщить дополнительные реквизиты карты – дату действия карты, наименование собственника карты (указанное на лицевой стороне карты», CVV-код карты (указан на обратной стороне карты, как правило состоит из 3 цифр), а также просит сообщить коды, которые пришли Вам в смс-сообщении в ходе разговора. После сообщения Вами указанных сведений, злоумышленник получает доступ к сервису «Сбербанк Онлайн» по Вашей карте (даже в случае, если Вы никогда указанным сервисом никогда не пользовались), подключает услугу «Мобильный Банк» к своему сотовому номеру (с целью отключить Вас от информирования о проводимых по Вашим карта и счетам операциям), после чего осуществляет перевод всех имеющихся денежных средств на ваших счетах и картах, на имеющиеся в его распоряжении банковские карты как правило других банков.

**Как не стать жертвой подобных преступлений и защитить своих близких от данного посягательства?** Прежде всего, не следует быть слишком доверчивым. Если вам позвонили от лица какого-либо серьезного ведомства или любой другой организации и потребовали деньги, не бойтесь перезвонить по официальным телефонам учреждения и выяснить, соответствует ли полученная вами информация действительности. Также, узнав о новом способе, применяемом мошенниками в мобильной сфере, обязательно расскажите о нем всем своим знакомым. Часто преступники пользуются не информированностью населения.

Время не стоит на месте, и мошенничество подстерегает нас везде: на просторах Интернета, в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Случаи Интернет-мошенничества имеют место быть в нашей жизни, ведь большинство граждан для своего удобства пользуются предложениями в сфере товаров и услуг в сети Интернет. Однако не всегда случаи Интернет-мошенничества люди могут распознать «с ходу». К сожалению, не редко жители нашего края, а также жители ЗАТО Сибирский попадаются на уловки мошенников и в итоге такие истории заканчиваются плачевно.

Не торопитесь, перед тем как совершить какие-либо необратимые действия, подумайте, только сам пользователь сети может сделать свою жизнь в виртуальном пространстве безопасной. «Предупрежден-значит вооружен» - гласит поговорка. Это справедливо по отношению к защите от мошенничества.

Также МО МВД России по ЗАТО п. Сибирский просит всех, кому известно о случаях мошенничеств, а также при попытках совершения в отношении Вас или Ваших близких преступлений указанной сферы, обращаться в МО МВД России по ЗАТО п. Сибирский, расположенный по адресу: ЗАТО Сибирский,
ул. Победы 1, или по телефону: 8(38532)50-334.

Оперуполномоченный НУР МО МВД

России по ЗАТО п. Сибирский

капитан полиции Е.Ю. Крючков