**РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ СРЕДСТВ СВЯЗИ**

В связи с увеличением роста преступлений, совершённых посредством мобильных средств связи,  даем рекомендации по защите от преступных посягательств.

  Зачастую преступники используют одни и те же способы мошенничества:

1) Рассылаются смс – сообщения с текстом: «обслуживание вашей банковской карты заблокировано» и указываются номера телефонов, по которым можно узнать информацию по данному факту. После того как граждане перезванивают на указанные номера, преступники представляются сотрудниками банков, в ходе разговора узнают, является ли гражданин владельцем банковской карты, если да, то сообщают, что с банковской картой возникли проблемы, и в целях исключения блокировки, необходимо немедленно через банковский терминал протестировать и произвести активацию банковской карты. Гражданин, введенный в заблуждение, через банковский терминал, по указанию преступников, осуществляет перевод денежных средств со своего счета на счет указный преступниками, так же производит оплату различных услуг, включая оплату услуги связи.

2) сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Типы сообщений: «здесь наши с тобой фото http:\\\\…», , «ваш акакунт, страница «вКонтакте» взломаны, пройдите регистрацию http:\\\\…», «вы выиграли автомобиль, подробности http:\\\\…” «я по вашему объявлению, согласны ли на обмен на это http:\\\\foto3.inc…»

При получении данного сообщения откажитесь от прохождения по указанным ссылкам и активации полученных ссылок. По возможности проверьте есть ли в сети Интернет в поисковых системах сведения о данных ссылках и возможных мошенничествах. Сообщите пользователям сети Интернет, что данная ссылка мошенническая. Удалите указанное сообщение если убеждены, что оно не нанесло вред Вашему устройству.

Вредоносные программы создаются и усовершенствуются мошенниками регулярно и при работе с телефоном Вы можете столкнуться с видом вредоносных программ, которые не требуют Вашей активности и самостоятельно могут быть загружены на Ваше мобильное устройство через уязвимости операционной системы.

Особенностью современного мошенничества является его групповой характер совершения. В связи с этим определенную сложность представляет раскрытие данного вида преступления: возникают трудности в установлении обстоятельств совершения преступлений, потому как зачастую преступники находятся в других городах, или субьектах или даже странах; преступниками при совершении преступлений используются абонентские номера сотовых телефонов, которые зарегистрированы на подставных лиц.

Чтобы не стать жертвой телефонных мошенников, нужно придерживаться простых правил:

1) Получив сообщение о блокировании банковской карты не звоните на номера указанные с смс-сообщении, а свяжитесь с банком по телефону «горячей линии» как правило, он указан на оборотной стороне банковской карты. При разговоре с «операторами» не называйте пароль карты, ее реквизиты, свои персональные данные: вся необходимая информация у банковских работников имеется и она сообщается при открытии счета.

2) В случае заражения мобильного устройства рекомендуем определить угрозы и последствия получения доступа хакера к Вашему мобильному устройству.

Признаками заражения мобильного устройства могут быть блокирование операционной системы, блокирование входящих СМС сообщений, отправка искусственно сгенерированных мобильным устройством сообщений. Зараженный мобильный телефон следует немедленно выключить. Сим-карту перевыпустить у оператора, а телефон сохранить для последующего изучения полицией, если было совершено мошенничество, либо передать в сервисный центр, если деньги похищены не были.

Если к данному мобильному устройству привязана банковская карта, банковские услуги такие как «Мобильный банк», «Онлайн Банк», «Интернет-банк», то необходимо срочно связаться с банком, заблокировать карту и приостановить обслуживание по счетам. Если с помощью телефона это не удается сделать, то необходимо обратиться в ближайшее отделение банка. Если мобильное устройство используется для доступа к страницам в социальных сетях, то необходимо с другого устройства либо компьютера выйти в социальную сеть и сменить привязанный номер телефона.

Зараженное мобильное устройство так же является источником распространения вредоносной информации по контактам, содержащимся в телефоне. Для предотвращения рассылки необходимо уведомить максимальное количество знакомых о Вашей проблеме и о возможно приходящих от Вашего имени вредоносных сообщениях.

В случае если с Вашего телефона, банковской карты похитили денежные средства необходимо в день совершения хищения обратиться в банк с требованием вернуть денежные средства, заблокировать ваш счет, запретить перевод денежных средств с вашего счета на другие счета, приостановить обслуживание счетов, на которые были перечислены ваши денежные средства. После получения ответа от банка, с выпиской по счету обратиться в полицию.

– Для работы с банковскими картами, системами «Мобильный банк», «Банк-онлайн», «Интернет-банк» и др. использовать отдельное мобильное устройство, не предназначенное для разговоров и развлечения в сети Интернет;

– Не указывать номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах соц. сетей;

– Приобрести и установить на мобильное устройство лицензионное антивирусное программное обеспечение из официальных источников;

– Указать в договоре с банком, либо в иной форме согласовать с банком что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, ограничить круг операций, установить лимит, который можно переводить с помощью мобильного устройства.

– Запретить перевод всего объема денежных средств с карты, счета.

Будьте осмотрительны, не позвольте мошенникам наживаться за ваш счет!