**Памятка**

**по профилактике мошенничеств**

***Как распознать мошенника, какие способы хищения денежных средств наиболее популярны, и главное* - *правила безопасного пользования банковскими картами.***

1. Одно из самых распространенных бесконтактных хищений происходит под предлогом попытки несанкционированного списания денег с вашей банковской карты. На ваш телефон поступает звонок от человека, который представляется сотрудником банка и сообщает, что кто-то пытается оплатить товары или услуги с вашей карты, и чтобы сохранить сбережения, необходимо незамедлительно назвать ее реквизиты — это номер, СVV-код, расположенный на обратной стороне, и срок действия, или перечислить деньги на указанный псевдобанкиром «безопасный» счет.

Никогда не называйте реквизиты своей карты! Запомните, работники банков не станут их запрашивать, они и так владеют информацией по вашей карте. Если вам позвонили с информацией о попытке хищения денег, положите трубку и перезвоните на телефон горячей линии банка, указанной на обратной стороне карты!

2. Огромное количество мошенничеств совершается с использованием сайтов бесплатных объявлений при покупке-продаже товаров.

Схема следующая: мошенник размещает в Интернете объявление о продаже товара, который вам нужен. После телефонного разговора или переписки в Интернете, «продавец» просит перечислить деньги, после чего желаемый товар либо вообще не приходит, либо присылают гораздо более дешевую вещь. В этой ситуации не нужно переводить деньги заранее. С 90%- й вероятностью это мошенники! Вы можете попросить продавца отправить товар по почте с использованием услуги — описью вложения. К посылке будет приложено юридически значимое описание содержимого. Работники почты будут обязаны дважды проверить посылку - перед отправлением и после ее получения, что будет являться гарантией того, что вам отправят тот товар, который обещали.

Разберем еще одну ситуацию. Когда вы сами продаете товар. К вам может позвонить покупатель и попросить назвать реквизит банковской карты для перечисления залога или полной стоимости товара, назвать только номер своей карты, это безопасно Но ни в коем случае не называйте секретный код, расположенный на ее обратной стороне и пароли, приходящие в смс-сообщениях!

3. Нередко мошенники получают доступ к взломанным аккаунтам в соцсетях и под видом ваших знакомых просят одолжить деньги. Прежде чем перечислять на указанный счет денежные средства, перезвоните, этому человеку. Наверняка у него все хорошо, не считая того, что его аккаунт взломали.

4. Мошенничество под предлогом получения кредита. Вы оставили заявку на сайте или нашли объявление в Интернете о выдаче кредита. Представитель финансовой организации, прежде чем выдать кредит просит оплатить комиссию, страховку, проценты по кредиту – ничего не перечисляйте! Это мошенник!

5. Вам позвонили и сообщили, что положена компенсация за ранее приобретенные лекарственные средства. Преступник под видом следователя или работника прокуратуры сообщает, что поймана банда продававшая некачественные медицинские препараты, и вам положена денежная компенсация. Но для этого необходимо оплатить комиссию, транспортные услуги, за открытие счета и так далее. Мошенники будут придумывать все новые предлоги, пока у вас не кончаться деньги или вы не сообразите, что вас обманывают.

6. К вам пришло сообщение в виде ссылки от неизвестного отправителя, пройдя по которой, вам обещают приз, интересное фото или что угодно. Скорее всего, перейдя по ссылке, вы скачаете вирус и с вашей карты будут похищены деньги. Никогда не открывайте ссылки от незнакомцев, да и от знакомых аккаунтов - с осторожностью. И не забудьте установить на свой смартфон антивирусную программу.

7. Вы решили совершить покупку через Интернет, например, купить билет на самолет или в кино, и для этого нужно ввести реквизиты банковской карты. В начале убедитесь, что вы зашли на настоящий сайт, а не подделку. Так называемый фишинговый сайт, создаваемый кибер-преступниками, как правило, имеет ключ в названии «http» вместо безопасного «https». Еще один способ распознать фальшивку - скопировать адрес сайта в адресной строке и запросить по нему информацию в поисковой системе о дате создания. Как правило, сайты, работающие несколько дней, не настоящие.

И даже если вы все проверили и оставили данные вашей карты на одном из сайтов, остается риск хищения ваших денег. Преступники могут получить доступ к вашему счету, взломав базу данных того или иного сайта. Для избежания потери крупной суммы денег необходимо завести дополнительную дебетовую банковскую карту с отдельным счетом, и пополнять ее на ту сумму, которая вам необходима. И ни в коем случае нельзя совершать покупки в Интернете с использованием кредитной или зарплатной карты, где у вас могут быть крупные суммы денег!

Банковская карта является ключом к вашему счету. Поэтому никому ее не передавайте, не сообщайте ее реквизиты, кроме самого номера карты. В случае поступления информации о сомнительных операциях, обращайтесь непосредственно в банк или по телефону горячей линии, указанному на обратной стороне карты. Мошенники могут использовать различные уловки - представляться сотрудниками правоохранительных органов, вашими близкими, придумывать что угодно! Их главная цель — получить от вас деньги или реквизиты банковской карты! Помните об этом!

Пресс-служба МВД по Чувашской Республике