

За 10 месяцев 2020 года в Чебоксарах зарегистрировано 2029 бесконтактных хищений – мошенничеств, краж с банковских карт и интернет-вымогательств. Ущерб, причиненный жителям города, составил 135 миллионов 921 000 рублей.

Чаще всего преступники звонят на сотовый телефон, как правило, с номеров с кодом 495 (город Москва) и **представляются сотрудниками службы безопасности банка**. Мошенники сообщают, что кто-то пытается похитить деньги с вашей банковской карты или оформил кредит на ваше имя, и для решения проблемы просят назвать реквизиты карты, срок ее действия, секретный код, пароли, поступающие в смс, и другие данные. Могут также попросить перевести деньги на «безопасный счет».

В этой ситуации лучше всего сразу положить трубку, а если сомневаетесь, перезвоните в банк по телефону, указанному на обратной стороне карты. И никогда не называйте ее реквизиты! Работники банков не станут их запрашивать, они и так владеют этой информацией.

Огромное количество мошенничеств совершается с использованием сайтов бесплатных объявлений **при покупке-продаже товаров**. Преступники размещают объявления о продаже, просят перевести предоплату или полную стоимость за товар, но желаемое вы так и не получите. И наоборот, если вы сами разместили объявление о продаже чего-либо, вам могут позвонить и попросить назвать реквизиты карты для перевода денег за товар, а затем похищают все содержимое вашего счета.

Как себя обезопасить? В первой ситуации не следует переводить деньги, если вы не уверены, что вас не обманут. Да, существуют известные продавцы с надежной репутацией, но к ним никак не относятся люди, разместившие частные объявления в Интернете. Как вариант, 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.

И если вы сами продаете товар и хотите получить за него деньги, достаточно будет назвать номер телефона, привязанный к вашей карте. И все! Никаких кодов, паролей и реквизитов карты!

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.

В последнее время участились случаи хищения денег **под предлогом перевозки людей**. Желаящие уехать в другой город находят водителя через приложения в Интернете, затем, обговорив детали поездки, заранее переводят деньги. Чтобы не попасться на такую уловку, безопаснее будет оплачивать услугу, убедившись лично, что вас действительно довезут и не обманут.

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 кончатся деньги или вы не сообразите, что вас обманывают.

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.

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.

В случае **потери банковской карты**, необходимо как можно скорее ее заблокировать, обратившись непосредственно в банк, через приложение банка или по телефону горячей линии финансового учреждения.

Еще раз запомните! Банковская карта является ключом к вашему счету. Поэтому никому ее не передавайте и не сообщайте ее реквизиты. Мошенники могут использовать различные уловки – представляться сотрудниками банков, правоохранительных органов, вашими близкими, придумывать что угодно! Их главная цель – получить от вас деньги или реквизиты банковской карты!