**Памятка**
**об основных способах совершения сотовых мошенничеств с банковскими картами и мерах их предупреждения**

Одна из схем сотового мошенничества выглядит следующим образом. Злоумышленники звонят и представляются специалистами социальных служб или сотрудниками банков. Они обещают различные льготы, социальные выплаты и компенсации. Предлагают оформить кредит с минимальной ставкой или снизить проценты по действующему кредиту. Своими обещаниями они вызывают доверие и усыпляют бдительность. Во время разговора мошенники предлагают «проверить», какая льгота положена и какую сумму можно получить. Для этого абоненту нужно сообщить паспортные данные и информацию по банковской карте, на которую якобы переведут деньги. Дополнительно уточняют, к какому номеру телефона привязана карта.

Через некоторое время у владельца карты пропадает со счета крупная сумма или все деньги. Злоумышленники воспользовались информацией и оплатили дорогостоящую покупку с карты жертвы.

По-прежнему звонят мошенники, которые выдают себя за работников банков. Сначала владелец карты получает сообщение, что с карты списаны деньги. Сообщение не вызывает сомнения, потому что номер злоумышленников напоминает номер банка. Через несколько секунд злоумышленник звонит и выдает себя за работника службы безопасности банка. Мнимый сотрудник говорит, что прямо сейчас кто-то пытается снять деньги с вашей карты, нужно действовать быстро и сработать на опережение. После такого напора злоумышленник просит назвать одноразовый пароль из смс или кодовое слово — они якобы нужны, чтобы отменить операцию. Как только человек сообщает код, мошенник тут же списывает деньги. Отличительная черта мошенников — говорят уверенно, часто повторяют слово «безопасность» и торопят с ответом.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер. После чего происходит списание средств.

Имеют место случаи когда мошенник прикидывается сотрудником банка. А чтобы человек не распознал обман, запугивает его — говорит, что по карте произошла подозрительная операция и списались деньги. Затем злоумышленник интересуется, проводился ли платеж в ближайшее время. Чтобы отменить несанкционированное списание, «представитель банка» предлагает открыть резервный счет и перевести на него деньги. Клиента просят пройти «верификацию»: назвать номер банковской карты и срок ее действия после чего неправомерно завладевают его денежными средствами.

Часто мошенники, представляются сотрудниками полиции, прокуратуры, следственного комитета, другими сотрудниками правоохранительных органов, Центробанка, просят перевести денежные средства под каким-либо предлогом.

В настоящее время получает широкое распространение новый способ мошенничества, связанный с получением неправомерного доступа к личному кабинету портала «Госуслуг». Мошенники представляются сотрудниками «Госуслуг», называет свои фамилию, имя, отчество и сообщают, что личный кабинет атакуют мошенники. Обманщики якобы пытаются изменить номер телефона, который привязан к «Госуслугам», и им нужно срочно помешать. Далее собеседник обещает помочь и просит назвать код, который тут же приходит на телефон. Получив код, мошенники завладевают личным кабинетом и всей информацией, которая там есть. Лучший способ обезопасить себя в указанной ситуации — никому не доверять, даже если собеседник кажется очень убедительным. Никому не сообщать свой номер телефона, коды подтверждения, логины, пароли и другие данные. В любой ситуации, вызывающей сомнения, лучше обратиться в МФЦ и узнать о статусе аккаунта «Госуслуг» лично.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

– сотрудники любого банка никогда не просят сообщить данные банковской карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются эти данные;

– не при каких обстоятельствах никому не сообщать данные банковской карты, а так же секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бояться прервать разговор, положить трубку;

– внимательно читать СМС сообщения приходящие от банка;

– никогда и никому не сообщать пароли, и секретные коды, которые приходят в СМС сообщении от банка;

– помнить, что только мошенники спрашивают секретные пароли, которые приходят к в СМС сообщении от банка;

– сотрудники банка никогда никого не попросят пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

- при любых подозрениях, что в отношении вас возможно совершаются мошеннические действия, сообщить в полицию по телефону 02, или 020 с мобильного телефона, а так же по телефонам дежурной части УМВД России по г. Кургану 45-64-48, 49-57-97.

# Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

## Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

-Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;

-Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;

-Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

## Следует помнить!

-Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;

-Сотрудник банка может запросить у клиента только контрольное слово, ФИО;

-При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;

-Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

## При несанкционированном (незаконном) списании денежных средств рекомендуется:

-Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

-Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

-Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.