ПАМЯТКА
для граждан по профилактике хищений
денежных средств с банковских карт и счетов

В 2019 году на территории Калужской области значительно участились случаи хищения денежных средств с банковских карт и счетов граждан. Хищение денежных средств происходит путем заражения сотовых телефонов на операционной системе - «Андроид» вредоносным программным обеспечением (вирусом), которое самостоятельно, через услугу – «Мобильный банк», осуществляет перевод денежных средств.

В целях недопущения несанкционированного списания денежных средств необходимо помнить несколько простых правил:

1. Установить на телефоне/смартфоне антивирусную программу, доступную в магазинах мобильных приложений (не устанавливайте на свой телефон нелицензионные операционные системы, так как это отключает защитные механизмы, в результате телефон становится уязвимым к заражению вирусными программами)**.**

2. Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по СМС и электронной почте.

3. Если Вам пришло СМС-сообщение «Ваша банковская карта заблокирована», «Я случайно положил Вам 100 руб. на телефон», не могли бы Вы обратно переслать мне 100 рублей на номер 8-9XX-XXX-XX-XX» ни в коем случае не отвечайте на СМС-сообщение и не перезванивайте на номера, указанные в СМС-сообщении. Мошенник только этого и добивается, чтобы Вы перезвонили ему и в ходе разговора узнать от Вас всю информацию по Вашей банковской карте, в том числе и ее ПИН-код. Лучше сразу удалить данное сообщение. А проверить заблокирована ли Ваша карта можно в любом ближайшем отделении ПАО «Сбербанк России» (банка эмитента Вашей банковской карты) или по телефонам, указанным на оборотной стороне Вашей карты.

4. Не оставляйте свой телефон без присмотра, чтобы исключить возможность несанкционированного использования услуги «Мобильный банк». Установите на мобильном телефоне пароль доступа к устройству.

5. При утере либо хищении мобильного телефона с подключенной услугой – «Мобильный банк», следует незамедлительно обратится к оператору сотовой связи для блокировки SIM-карты и в отделении банка для приостановления действия услуги.

6. При смене номера телефона, на который подключена услуга – «Мобильный банк», незамедлительно обратиться в банк и оформить письменное заявление на отключение услуги от старого номера.

7. Если вы не планируете использовать приложение – «Мобильный банк», обратитесь в отделение банка с письменным заявлением об его отключении. В данном случае вы гарантировано сохраните свои сбережения.

8. Никому и ни при каких обстоятельствах не сообщайте номер своей банковской карты, который указан на лицевой и оборотной стороне карты. Так же не сообщайте никому свои персональные (имя, фамилию) и паспортные данные, срок действия карты, указанные на лицевой стороне карты, и тем более ПИН-код карты.

9. Ни в коем случае не соглашайтесь на предоплату по банковской карте при посещении интернет-сайтов бесплатных объявлений (интернет-магазинов), таких как «Авито.ру» и т.д. Вас уже должно насторожить то, что продавец или покупатель просит Вас сообщить ему Ваши персональные и паспортные данные, а также номер вашей банковской карты. Так же проявите осторожность если Ваш собеседник просит перевести ему определенную сумму денег на его банковскую карту в качестве предоплаты. Ни в коем случае не соглашайтесь — это мошенники.