Прокуратура Российской Федерации

Прокуратура Тульской области

Прокуратура Ленинского района

ПАМЯТКА
о безопасном использовании банковских карт

п. Ленинский
2020

В первом полугодии 2020 года на территории Тульской области зарегистрировано 1053 преступления, совершенных с использованием IT-технологий, в том числе в сфере безопасности компьютерной информации, участились случаи совершения в отношении граждан мошеннических действий с использованием банковских карт.

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счете, не требующий для этого присутствия в банке. Простота использования банковских карт делает их самым уязвимым звеном в любой «схеме» мошенничества.

Многочисленные способы обмана граждан преследуют цели заполучить данные банковской карты или убедить сделать перевод на счет мошенника.

Оградить от мошенников в первую очередь способны знания, внимательность, здравомыслие и критическая оценка ситуации. Поможет и знание типичных «схем» работы мошенников и соблюдение правил, изложенных в данной памятке.

Среди наиболее распространенных способов хищения можно выделить следующие «схемы»:

1) СМС или звонок из банка о блокировке карты.

Вам приходит сообщение о том, что банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации, либо дойти до ближайшего банкомата и следуя «подсказкам» оператора самостоятельно разблокировать карту.

Не стоит торопиться немедленно выполнять требования лица, представившегося сотрудником банка. Свяжитесь со службой поддержки клиентов самостоятельно. Скорее всего, Вам сообщат, что никаких сбоев и блокировок не происходило.

2) Хищение денег с использованием «мобильного банка».

Самый распространенный способ хищения денежных средств с использованием услуги «Мобильный банк» следующий: потерпевшим, при заключении договора, указывается абонентский номер, который подключается к «Мобильному банку». В дальнейшем, лицо перестает длительное время пользоваться данным абонентским номером по различным причинам, при этом не отключив от него услугу «Мобильный банк», после чего оператор сотовой связи перевыпускает сим-карту. Новый пользователь сим-карты продолжает получать СМС-сообщения об операциях по банковской карте и, соответственно, получает доступ к управлению счетом через «мобильный банк».

3) Заражение телефона вирусом, который дает злоумышленнику доступ к управлению СМС-сообщениями потерпевшего и, соответственно, доступ к «мобильному банку». Как правило, заражение происходит при переходе по ссылке, полученной в СМС-сообщении или «мессенджере».

Чтобы обезопасить себя своевременно уведомляйте банк о смене номера телефона, не открывайте с телефона сомнительные ссылки из сообщений, используйте антивирусные программы.

4) Хищение денежных средств с карты путем сообщения о несчастных случаях с близкими родственниками и вымогательством денежных средств под видом проведения неотложных операций, покупкой лекарств и т.д.

Данный способ остается наиболее распространенным, так как в момент получения сообщения вышеуказанного содержания не любой человек может справиться со своими чувствами и эмоциями и зачастую под их влиянием совершает необдуманные поступки и переводит денежные средства лишь бы помочь близкому человеку.

Не спешите сразу переводить денежные средства на указанные позвонившим лицом реквизиты. Успокойтесь, попробуйте перезвонить близкому человеку, о котором идет речь, другим родственникам и знакомым.

Прокуратура района призывает граждан внимательно относиться к использованию банковских карт.

Относитесь к своей банковской карте так же, как и к собственным деньгам и храните ее в безопасности.

Не следует оставлять карту без присмотра, ведь мошенникам достаточно считанных секунд для копирования всей необходимой информации для перевода средств, не передавайте саму карту третьим лицам, включая родных и близких. Именно для них большинство банков выпускают дополнительные карты. Но если кража состоялась, следует немедленно обращаться в службу поддержки и заблокировать карту.

Никому не сообщайте ПИН-код Вашей карты и пароли из СМС-сообщений от банка. Ни сотрудники банка, ни любой другой организации не вправе требовать их.

Не храните ПИН-код рядом с картой и не записывайте ПИН-код на неё – в этом случае Вы даже не успеете заблокировать счет в случае хищения или утери карты.

При возникновении каких-либо подозрений в мошенничестве связывайтесь с клиентской поддержкой банка, номер телефона которой сохраните заранее.

Оплачивайте покупки с использованием реквизитов банковской карты только в проверенных интернет-магазинах или кассах продажи билетов. Лучше всего завести для этих целей отдельную карту (либо получить виртуальную карту, уточните в банке такую возможность), на которую переводить средства исключительно для совершения покупки.

С осторожностью относитесь к предоставлению реквизитов своей банковской карты посторонним лицам.

На постоянной основе проверяйте выписки по банковскому счету Вашей карты. При возникновении вопросов, связанных с проведенными операциями по счету (несанкционированными списаниями или ошибочными начислениями), незамедлительно обратитесь в Банк.

Помните, что мошенники не спят и каждый день разрабатывают новые схемы для получения легких денежных средств.

За последнее время участились случаи, связанные с хищением безналичных денежных средств, в том числе использование мошенниками чужих банковских карт.

Обращаю внимание, что согласно позиции, Верховного Суда Российской от 29.09.2020 о квалификации действий виновных, совершивших хищение денежных средств потерпевших с использованием банковской карты последних путем оплаты с ее помощью товаров в торговых организациях без сообщения ее сотрудникам ложных сведений о принадлежности банковской карты, как тайное хищение чужого имущества, т.е. преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ. За данный вид преступления, предусмотрена уголовная ответственность в виде штрафа в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до полутора лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

Будьте бдительными и внимательными!