



МВД России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ БАШКОРТОСТАН
(МВД по Республике Башкортостан)
ул. Ленина, 7, Уфа, 450000

Министру финансов
Республики Башкортостан
Л.З. Игтисамовой

23.11.2014 № 1/6941

на № _____ от _____

О направлении информации

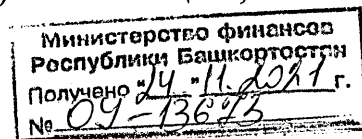
Уважаемая Лира Закуановна !

Министерство внутренних дел по Республике Башкортостан серьезно обеспокоено складывающейся криминогенной обстановкой, связанной с ростом количества регистрируемых преступлений по фактам хищений денежных средств с банковских карт граждан, совершаемых неустановленными лицами дистанционно, с использованием информационно-телекоммуникационных технологий.

Развитие современной цифровой экономики не только открывает новые возможности для личности, общества и государства по совершенствованию финансовых взаимоотношений, но, к сожалению, способствует формированию киберпреступности, масштабы которой все больше затрагивают многочисленные сферы общественной жизни, а жертвами преступлений становятся различные категории граждан, в том числе работники учреждений, организаций различных ведомств.

Ежегодно отмечается рост данных преступлений, как в нашей республике, так и в других регионах Российской Федерации. Так, за 10 месяцев т.г. в Республике Башкортостан зарегистрировано более 8 тысяч таких преступлений, в результате которых гражданам был причинен многомиллионный ущерб.

На сегодняшний день, одним из самых распространенных способов совершения преступлений являются случаи, когда неустановленное лицо, представляясь по телефону сотрудником Центрального банка России, либо сотрудником службы безопасности банков Сбербанк, ВТБ, Тинькофф, Альфа-банк и др., сообщает гражданину, что от его имени (по доверенности), некие лица оформили, либо пытались оформить кредит, в связи с чем необходимо срочно оформить такой же кредит в банке и погасить задолженность, либо перевести все имеющиеся на счету денежные средства на другой «безопасный счет», так как его счет стал известен третьим лицам. Затем, гражданину звонит другое лицо, представляется сотрудником правоохранительных органов (прокуратуры, полиции, следственного комитета, ФСБ) и сообщает, что



действительно ими проводятся мероприятия по поимке преступников, с которыми возможно связаны действующие работники банка, для чего необходимо строго следовать инструкциям, которые ему сообщит по телефону «сотрудник банка». После этого, гражданин, будучи введенный в заблуждение, выполняет все действия, которые ему диктуют по телефону псевдосотрудники банка, в результате которого гражданин самостоятельно, дистанционным образом оформляет на себя кредит и сам же осуществляет перевод данных денежных средств на указанные лицами номера банковских счетов, в том числе через банкоматы, либо происходит списание денежных средств со всех его счетов после того, как гражданин сообщает по телефону номер своей банковской карты, срок ее действия, СВС-код, а также пароли, направляемые посредством смс-уведомлений.

Как показывает анализ, звонки могут осуществляться с подменных абонентских номеров с имитацией известных номеров банка, дежурных частей правоохранительных органов и телефона доверия (900, 8-800-555-55-50, 279-32-92, 272-39-02, а также с кодом г.Москвы 495, 499). Как правило, злоумышленники находятся и звонят из стран СНГ и ближнего зарубежья, могут представляться от имени официальных должностных лиц правоохранительных органов (данные которых размещены и общедоступны на сайтах МВД, Следственного комитета, Прокуратуры и др.). Банковские карты, на которые гражданами переводятся денежные средства, числятся оформленными на третьих лиц по утерянным документам в других регионах страны и за ее пределами. Эти и другие обстоятельства в значительной мере затрудняют работу в раскрытии данных преступлений и возмещении ущерба гражданам.

К примеру, 20.05.2021 в 18.00 неустановленное лицо, позвонив Т. с абонентского номера 8-499-606-26-44, представившись сотрудником ПАО «Сбербанк», под предлогом того, что по ее банковским картам происходят подозрительные переводы в г.Ярославле, получило информацию об имеющихся у нее банковских картах, открытых в АО «Всероссийский банк развития регионов (ВБРР)» и «Тинькофф». После этого, с абонентского номера 8-901-906-10-64 позвонил неизвестный мужчина, который представился сотрудником банка АО «ВБРР», и сообщил, что якобы мошенники от ее имени оставили заявку на оформление кредита в сумме 700 000 рублей и, чтобы обезопасить денежные средства, необходимо оформить такую же заявку на кредит в банке. 21.05.2021 Т. в отделении банка оформила кредит в сумме 815 000 рублей. При этом, злоумышленники постоянно звонили и контролировали ее действия. После получения кредита ей последовала инструкция о необходимости зачисления денежных средств через банкомат на указанные ими счета. 24.05.2021 вновь поступил звонок от неустановленного лица, который представился сотрудником ПАО «Сбербанк» и пояснил, что у мошенников все еще есть возможность получения кредита от ее имени, и уточнил в каких банках у нее имеется кредитный потенциал. Т. сообщила, что в банке «ВБРР» кредитный потенциал составляет 3 000 000

рублей, после чего ей сообщили, что с ней свяжутся сотрудники данного банка. Далее, аналогичным способом, контролируя все ее действия по телефону, убедили подать заявку в офисе данного банка. Т. оформила кредит на сумму 2 221 000 рублей в отделении банка, полученные наличными денежными средствами перевела через банкомат «Альфа-банка» на указанные лицами номера счетов.

Распространены и другие способы и виды преступлений, при этом, все они совершаются при непосредственном участии потерпевшего, который, будучи введенным в заблуждение, сам предоставляет всю информацию по банковской карте неизвестным лицам, либо самостоятельно вводит данные реквизитов карт при осуществлении покупок на сомнительных Интернет-сайтах, а также при инвестировании в ценные бумаги, открытии брокерских счетов и т.п.

Министерством внутренних дел по Республике Башкортостан во взаимодействии со средствами массовой информации регулярно проводится разъяснительная работа среди населения республики о способах и методах совершения данных преступлений, однако, принимаемых мер недостаточно, по-прежнему, все больше граждан становятся потерпевшими от преступлений.

В соответствии с Федеральным законом от 23 июня 2016 года №182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», одной из форм профилактики правонарушений является тесное взаимодействие с гражданским обществом.

В связи с изложенным, в целях противодействия совершению преступлений с использованием информационно-коммуникационных технологий, прошу довести указанную информацию до сотрудников Вашего Министерства и подчиненных ему структурных подразделений, в том числе рассмотреть данный вопрос на проводимых собраниях и совещаниях, распространить прилагаемые видеоролики на официальных сайтах Министерства и подведомственных организаций, разместить профилактические агитационные материалы на сайтах, стендах, досках объявлений, принять иные меры по организации профилактической и разъяснительной работы, направленной на предупреждение преступлений данного вида.

О результатах и принятых мерах прошу проинформировать.

Приложение: на 2 листах, 1 диск.

Министр



Р.В. Деев

МВД по РБ предупреждает!!! Внимание!!! Мошенники!!!

Работники банков:

- не осуществляют звонки клиентам с просьбой предоставления персональных данных, номеров карт и другой информации;
- не просят коды из СМС для отмены совершенных «мошеннических операций»;
- не предлагают для сохранности перевести деньги на специальные счета или установить специальные программы для обеспечения удаленного доступа и управления компьютерами;
- не осуществляют СМС рассылки, например, «Ваша карта заблокирована», «Заблокирована сумма оплаты» и т.п. Ни при каких обстоятельствах не перезванивайте на указанные в таких сообщениях номера!
- никогда не сообщайте незнакомым людям номер своей банковской карты и CVC-код;
- не переходите по ссылкам на незнакомые ресурсы;
- сотрудники полиции, как и других правоохранительных и государственных органов не осуществляют звонки, в том числе и с «телефонов доверия», гражданам для подтверждения законности предлагаемых им финансовых операций с использованием банковских карт и других финансовых инструментов.

**Будьте бдительны и осторожны!!!
Берегите себя и своих близких!!!**

ВНИМАНИЕ! Интернет-мошенники!

Не станьте жертвой обмана!

КАК ОБМАНЫВАЮТ?

«ВАША КАРТА ЗАБЛОКИРОВАНА»

Работник банка НИКОГДА не запросит у Вас данные Вашей банковской карты. Они находятся в рабочей базе финансового учреждения.

«ПРИВЯЗКА БАНКОВСКОЙ КАРТЫ»

Если Вас просят подключить карту к чужому телефонному номеру или счету, задумайтесь о последствиях! Скорее всего, с Вами общается аферист!

«ПЕРЕВЕДИ МНЕ ДЕНЬГИ»

С взломанного аккаунта социальной сети Вашего знакомого может поступить просьба о переводе денег. Перезвоните Вашим друзьям и близким. Учтите, что с Вами могут общаться мошенники!

«ВНЕСИТЕ ПРЕДОПЛАТУ»

После перевода денег на указанный интернет-кошелек, покупатель рискует не получить ни товара, ни денег. Перепроверьте данные продавца или Интернет-магазина!

«ЗА РАЗБЛОКИРОВКУ НУЖНО ПЛАТИТЬ»

Вас просят перевести деньги на некий счет за разблокировку карты. Такого специалисты банков никогда не будут требовать!

«ПРИШЛО ИНТЕРНЕТ-СООБЩЕНИЕ С НЕИЗВЕСТНОГО АДРЕСА»

Внимание! Оно может содержать вирус, способный впоследствии передать Ваши персональные данные (пароли, логины) с целью похищения средств с банковской карты посторонним лицам. Воздержитесь от открытия подобных сообщений!

ЗАПОМНИТЕ! ЕСЛИ С ВАШЕГО ЭЛЕКТРОННОГО СЧЕТА НЕОЖИДАННО СТАЛИ ПРОПАДАТЬ ДЕНЬГИ, НЕМЕДЛЕННО ЗАБЛОКИРУЙТЕ ЕЕ! ПОДАЙТЕ ЗАЯВЛЕНИЕ В ПОЛИЦИЮ.

ВСЮ ИНФОРМАЦИЮ О ТОМ, КАК НЕ ПОПАСТЬ НА УЛОВКИ МОШЕННИКОВ, ВЫ МОЖЕТЕ УЗНАТЬ НА ОФИЦИАЛЬНОМ САЙТЕ МВД ПО РЕСПУБЛИКЕ БАШКОРТОСТАН ПО АДРЕСУ:

www.02.mvd.rf