При оплате услуг картой в сети «Интернет» необходимо использовать только проверенные сайты, внимательно прочитывать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операции.

Для минимизации возможных хищений при проведении операций с использованием Интернета рекомендуется оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции для данного вида карты, в том числе с использованием других банковских карт, выпущенных на имя держателя карты.

Когда банк считает подозрительными операции, которые совершаются от имени клиента, он может по своей инициативе временно заблокировать доступ к сервисам СМС-банка и онлайн-кабинета. Если операции совершены держателем карты, для быстрого возобновления доступа к денежным средствам достаточно позвонить в контактный центр банка.

В случае смены номера мобильного телефона или его утери свяжитесь с банком для отключения и блокировки доступа к СМС-банку и заблокируйте сим-карту, обратившись к сотовому оператору.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

СОБЛЮДЕНИЕ ПРИВЕДЕННЫХ МЕР И РЕКОМЕНДАЦИЙ ПОЗВОЛИТ ПРЕДОТВРАТИТЬ СЛУЧАИ ДИСТАНЦИОННОГО ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

ПРОКУРАТУРА РЕСПУБЛИКИ БАШКОРТОСТАН

РЕСПЕКТ
Мы делаем законодательство доступным!

ПАМЯТКА ДЛЯ ГРАЖДАН

О МЕРАХ ПО ПРЕДУПРЕЖДЕНИЮ ДИСТАНЦИОННЫХ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ

8 (347) 272-85-60

В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ, ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ, ПЕРСОНАЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ, ИНТЕРНЕТА СТРЕМИТЕЛЬНО ВОЗРОСЛО КОЛИЧЕСТВО СОВЕРШЕННЫХ С ИХ ИСПОЛЬЗОВАНИЕМ ПРЕСТУПЛЕНИЙ.

Для предотвращения дистанционных хищений денежных средств необходимо знать, что сотрудники банка НИКОГДА по телефону или в электронном письме НЕ ЗАПРАШИВАЮТ:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);

- реквизиты и срок действия карты;

- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

- логин, ПИН-код и CVV-код банковских карт.

СОТРУДНИКИ БАНКА ТАКЖЕ НЕ ПРЕДЛАГАЮТ:

- установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

- перейти по ссылке из СМС-сообщения;

- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

- под их руководством перевести для сохранности денежные средства на «защищённый счёт»;

- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах.

ДЕРЖАТЕЛЮ КАРТЫ НЕОБХОДИМО ИЗБЕГАТЬ:

- подключения к общедоступным сетям Wi-Fi;

- использования ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);

- сообщения кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищённых местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

Перед использованием банкомата убедитесь, что все операции, совершаемые предыдущим клиентом, завершены; что на клавиатуре и в месте для приема карт нет дополнительных устройств; обращайте внимание на неисправности и повреждения.

Совершая операции, не прислушивайтесь к советам незнакомых людей и не принимайте их помощь.

ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ТЕЛЕФОНА СОБЛЮДАЙТЕ СЛЕДУЮЩИЕ ПРАВИЛА:

- при установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;

- отключите в настройках возможность использования голосового управления при заблокированном экране.

Применяя сервисы СМС-банка, сверяйте реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.