



ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА РЕСПУБЛИКИ БАШКОРТОСТАН

ПРОКУРАТУРА
ШАРАНСКОГО РАЙОНА

ШАРАН РАЙОНЫ
ПРОКУРАТУРАҒЫ

ул. Красная, 7, с. Шаран, 452630,
тел.: (34769)2-24-77, факс: (34769)2-24-77

25.05.21 № 3-2-2021



810816 934210

Главе администрации
муниципального района
Шаранский район РБ

Ишемгулову Ф.А.

На протяжении последних лет в республике отмечается стремительный рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий (2018 г. – 3,6 тыс., 2020 г.- 13,3 тыс., 4 мес. 2021 г. – 4,9 тыс.), в основном состоящих из дистанционных хищений денежных средств граждан.

Мошенники выдают себя за банковских работников, сотрудников правоохранительных органов, специалистов служб социальной защиты и, вводя в заблуждение граждан, выясняют у них персональные данные, информацию о банковской карте (счете), используют полученные сведения в корыстных целях.

С учетом высокой социальной значимости работы по профилактике названных преступных деяний прокуратурой Республики Башкортостан при содействии сервисного центра «Респект» разработана памятка для граждан «О мерах по предупреждению дистанционных хищений денежных средств».

Направляя указанную Памятку предлагаю, распространять ее среди населения путем размещения в зданиях органов местного самоуправления, организаций и учреждений района и др., вручения заявителям в ходе осуществления личных приемов.

Приложение: на 1 л.

И.о. прокурора района

Э.О. Макашева



AA № 0015143
Прокуратура Шаранского района Республики Башкортостан
№ 3-2-2021/111-21-20800069

При оплате услуг картой в сети «Интернет» необходимо использовать только проверенные сайты, внимательно прочитывать тексты СМС-сообщений с кодами подтверждения, 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 своему 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**

РЕСПЕКТ СЕРВИСНЫЙ ЦЕНТР

**ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ ДЛЯ ФИЗИЧЕСКИХ
ЛИЦ ПРИЗНАЕТСЯ РАВНОЗНАЧНОЙ СОБСТВЕННОРУЧНОЙ
ПОДПИСИ В ДОКУМЕНТЕ НА БУМАЖНОМ НОСИТЕЛЕ**

ЭЦП МОЖНО ИСПОЛЬЗОВАТЬ ДЛЯ:

- Оформления загранпаспорта, водительского удостоверения, записи к врачу и т.д.
- Подачи заявления в вузы разных городов, не выходя из дома.
- Подачи документов на регистрацию ИП или ООО, на сайте налоговой инспекции.
- Закрепления трудовых отношений с работодателем, подписав договор электронной подписью.

Выпуском сертификатов занимаются удостоверяющие центры. При выборе удостоверяющего центра ориентируйтесь на несколько показателей:

- имеет ли все необходимые лицензии и аккредитации,
- как долго работает,
- есть ли круглосуточная техподдержка.

С оригиналами документов (или их заверенными копиями) и паспортом вы должны лично прийти в сервисный центр, чтобы подписать договор и получить сертификат подписи. Если предлагают выпустить ЭЦП без удостоверения личности – это грубое нарушение законодательства, в этом случае может произойти утечка персональных данных. За услугой выпуска ЭЦП обращайтесь к проверенным и надежным компаниям.

**Сервисный центр «Респект» - официальный
центр выдачи ЭЦП аккредитованного
Удостоверяющего центра СКБ Контур – одного
из крупнейших разработчиков программного
обеспечения в России.**

Звоните 8 (347) 292-77-96,
или на мобильный 8 906 371 51 07



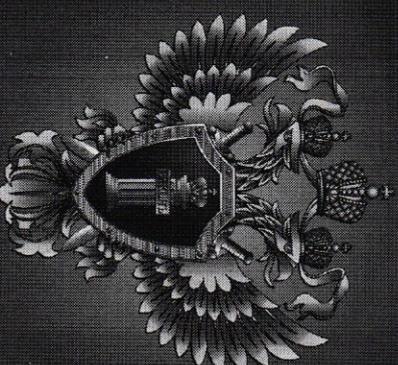
ПРОКУРАТУРА
РЕСПУБЛИКИ
БАШКОРТОСТАН



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 SMS-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 SMS-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 «защитный счёт»;

- зайти в онлайн-кабинет по ссылке из SMS-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; обращайтесь 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 SMS-сообщений и доступ к сети «Интернет»;

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

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