

Microsoft Store. Microsoft Store.

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи 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 защищенных местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

Перед использованием банкомата осмотрите его и 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 обращайтесь 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.

При оплате услуг картой в сети «Интернет» (особенно при привязке к регулярным платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные.

Необходимо использовать только проверенные сайты, внимательно изучать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операций.

Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» 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.

Неукоснительное соблюдение отмеченных в настоящей памятке рекомендаций поможет обезопасить себя и ваши сбережения от действий кибермошенников.

В случае совершения в отношении Вас мошенничества звоните по номеру 102, либо обратитесь в ближайшее отделение полиции.



Прокуратура Тюльганского района Оренбургской области

ПАМЯТКА

«О необходимых мерах
личной безопасности в
целях противодействия
киберпреступникам»

2021 год

В последние годы складывается негативная тенденция резкого всплеска хищений денежных средств добропорядочных граждан с банковских карт и счетов мобильных телефонов.

Мошенники, умело используя возросший потенциал информационно-телекоммуникационных технологий, психологические аспекты и недостаточную осведомленность граждан в данной сфере, путем всякого рода манипуляций, похищают значительные денежные средства.

Такие случаи на территории района фиксируются, зачастую суммы похищенных у пострадавших денег исчисляются в сотнях тысяч рублей.

Правоохранительными органами ведется последовательная и целенаправленная работа по изобличению преступников и привлечению их к уголовной ответственности.

Наряду с этим, чтобы не стать жертвой преступников, необходимо исходить из следующего.

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 CVC-код (трехзначный номер на оборотной стороне карты) банковских карт.

Сотрудники банка также не предлагают по телефону:

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 «защищенный или резервный счет»;

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. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чат-боты в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store.

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

подключения к общедоступным сетям Wi-Fi;

использования ПИН-кода или CVC-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 CVC-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищенных местах (например, в госучреждениях, офисах банков, крупных

торговых центрах).

Перед использованием банкомата осмотрите его и 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.

При оплате услуг картой в сети «Интернет» (особенно при привязке к регулярным платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чат-боты в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play,