



ПАМЯТКА О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

Соблюдение рекомендаций, содержащихся в памятке, позволит обеспечить максимальную сохранность ваших денежных средств



СУРГУТНЕФТЕГАЗБАНК
8 800 775 88 04 | www.sngb.ru

АО БАНК «СНГБ». Генеральная лицензия Банка России №588 от 05.09.2016 г.

В течение последних десятилетий технический прогресс кардинально изменил жизнь людей. Появилось множество высокотехнологичных устройств — персональные компьютеры, ноутбуки, спутниковые и мобильные телефоны, навигаторы, цифровое телевидение, банковские карты, взамен реальных денег люди придумали виртуальные платежные системы и виртуальные деньги, и прочее. Постоянно появляются новые модели этих устройств, программы и сервисы для них. Все это делает нашу жизнь комфортнее, но требует грамотного подхода к использованию новинок технического прогресса.

Чтобы не поддаваться на уловки злоумышленников, необходимо соблюдать простые правила безопасности по использованию банковских карт, которые позволят минимизировать потери или вовсе избежать их.



ОБЩИЕ РЕКОМЕНДАЦИИ:

1. Получив новую карту, обязательно поставьте подпись на оборотной стороне карты на специальной полосе для подписи.



При получении карты поставьте свою подпись шариковой ручкой на оборотной стороне карты в специально отведенном месте. Это снизит риск использования карты в случае ее утраты.



Ваша карта действует до последнего дня месяца, указанного на лицевой стороне карты, включительно (на примере выше — до 31 декабря 2021 года).

2. Обеспечивайте такие условия владения картой (персональными данными карты), которые исключают всякую возможность ее утраты, порчи, копирования данных с карты, ее несанкционированного и незаконного использования.
3. Не передавайте карту другим лицам, в том числе родственникам. Только держатель банковской карты имеет право ее использовать.
4. Храните в тайне от других лиц конфиденциальные данные вашей карты (номер и срок действия карты, дополнительный код проверки подлинности карты — 3 цифры на оборотной стороне карты, кодовое слово). Данные о номере карты и кодовое слово могут запросить только сотрудник банка при вашем личном обращении по телефону,

указанному на оборотной стороне карты и, только при необходимости получения информации по вашему картсчету.

5. Ваш персональный идентификационный номер (ПИН-код) является электронным аналогом вашей собственноручной подписи и инструментом для доступа к денежным средствам, находящимся на вашем картсчете.
 - Запомните ваш ПИН-код.
 - Не записывайте ваш ПИН-код.
 - Никому не сообщайте ваш ПИН-код, в том числе сотрудникам АО БАНК «СНГБ» или других банков, сотрудникам полиции или работникам предприятий торговли (услуг).
 - Регулярно меняйте ПИН-код вашей карты. **Помните: хранение ПИН-кода — это Ваша ответственность и обязанность.**
6. Никогда не отвечайте на электронные письма, в которых от имени кредитной организации предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники. В целях информационного взаимодействия с кредитной организацией рекомендуется использовать только реквизиты средств связи (телефонов, факсов, интерактивных веб-сайтов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в банке при оформлении карты.
7. Обязательно подключите услугу уведомления о движении денежных средств по вашей банковской карте (СМС/Push и/или e-mail оповещения) — это позволит отслеживать все операции, проводимые по вашей банковской карте.
8. При получении СМС-сообщения / Push-уведомления о якобы блокировании карты / приостановлении расчетов по карте / получении выигрыша и прочем не звоните на номер, указанный в СМС-сообщении / Push-уведомления. Вероятно, вы получили ложное сообщение, направленное мошенниками. Для уточнения информации по Вашей банковской карте звоните по официальному телефону банка, указанному на обороте карты.

Помните, что никакое кредитное учреждение, включая Центральный Банк РФ, не может отправлять держателю карты уведомления посредством СМС-сообщения, если держатель не является клиентом данного банка. Данным правом обладает только кредитное учреждение, клиентом которого вы являетесь. При этом используется только уникальный банковский идентификатор кредитного учреждения в АО БАНК «СНГБ» — это SNGB.
9. Если на Ваш номер телефона поступил звонок от якобы представителя банка, который запрашивает у вас конфиденциальную информацию по карте, попросите его назвать имя и службу банка. Не продолжайте разговор и не выполняйте какие-либо команды звонящего, перезвоните в Банк самостоятельно, сообщите о звонке.

10. Регулярно проверяйте движение денежных средств, находящихся на вашем картсчете. Вы можете сделать это непосредственно в банке, через СМС-запрос на банковский номер +7-922-253-07-15, а также с использованием систем дистанционного банковского обслуживания.
11. Установите ежедневный лимит снятия наличных денежных средств. Если вам понадобится снять сумму, превышающую разрешенную, звоните в банк по телефонам, указанным на оборотной стороне карты, и измените лимит.
12. Если вы утратили карту или полагаете, что данные вашей карты скомпрометированы (стали известны третьим лицам), немедленно заблокируйте карту по телефону круглосуточной службы поддержки клиентов (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04 или через системы дистанционного банковского обслуживания и впоследствии оформите в банке банковскую карту с новыми реквизитами.
13. Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Для получения любой информации по вашей банковской карте связывайтесь с банком по телефонам, указанным на оборотной стороне вашей карты.

ПРАКТИЧЕСКИЕ СОВЕТЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ В БАНКОМАТЕ

1. Осуществляйте операции в банкоматах и терминалах, имеющих наклейки с логотипами, идентичными логотипу на вашей банковской карте.
2. Старайтесь пользоваться одними и теми же банкоматами, которые вам хорошо известны. В случае необходимости использовать новый банкомат, выбирайте хорошо освещенный и установленный в удобном (находящемся под наблюдением) месте или в подразделениях банков.
3. **Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.**
4. Прежде чем подойти к банкомату, осмотрите окружающее пространство. В случае нахождения поблизости подозрительных людей, воспользуйтесь другим банкоматом.
5. Перед использованием банкомата осмотрите его внешний вид. Если вы обнаружите наличие каких-либо посторонних предметов, проводов, следов конструктивных изменений, воспользуйтесь другим банкоматом.
6. **Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.**
7. Если у банкомата за вами находится очередь, убедитесь, что никто не видит, каким образом вы вводите ПИН-код.

8. Вводите ПИН-код только после того, как появится соответствующая запись на экране банкомата.
9. При смене ПИН-кода **не выбирайте легкие значения (1111, 1234 или даты рождения)**. Чаще изменяйте ПИН-код, в частности, обязательно измените его, если вы осуществляли операции с введением ПИН-кода в других городах и/или странах.
10. Если вам кажется, что банкомат работает некорректно, отмените осуществление операции, заберите свою карту и воспользуйтесь другим банкоматом.
11. После совершения операций с использованием банкомата, убедитесь в том, что банковская карта была возвращена банкоматом, дождитесь выдачи квитанции при ее запросе, в случае если Вы получали наличные, положите их в сумку (кошелек, карман) и только после этого отходите от банкомата.
12. Будьте очень внимательны, если кто-то посторонний предлагает вам помощь при осуществлении операций в банкомате, даже если ваша карта не возвращается банкоматом или возникли проблемы с проведением операции. Не позволяйте «помощникам» себя отвлечь, не отходите от банкомата, обратитесь за помощью в круглосуточную службу поддержки банка по телефонам, указанным на банкомате.

ПРАКТИЧЕСКИЕ СОВЕТЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ В ТОРГОВОМ ТЕРМИНАЛЕ ПРИ ОПЛАТЕ ТОВАРОВ И УСЛУГ


1. **Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.**
2. При оплате банковской картой товаров (услуг) следите, чтобы карта не исчезала из вашего поля зрения. При необходимости ввести ПИН-код, закройте клавиатуру рукой так, чтобы ни продавец, ни находящиеся рядом с вами люди не видели введенных цифр.
3. Во избежание использования работниками предприятий торговли (услуг) конфиденциальных данных вашей карты в мошеннических целях требуйте проводить все операции с вашей картой только в вашем присутствии и внимательно следите за всеми действиями кассира или продавца. Не позволяйте уносить карту для проведения оплаты, при необходимости последуйте за продавцом (кассиром, официантом и т.п.).
4. Требуйте оформления расчетного документа (чека терминала).
Прежде чем поставить подпись на чеке, всегда проверяйте указанную в чеке сумму операции.

Убедитесь в том, что указанная в чеке сумма соответствует стоимости товара (работы, услуги).

Никогда не подписывайте чек, в котором не указана либо неверно указана сумма операции.

Сумма операции

Место
для вашей подписи

АО БАНК «СНГБ» Торговый центр Сургут, RUSSIA ID терминала: 001101999 ЧЕК 0085
ОПЛАТА ТОВАРА СУММА: 20.600.00 RUR 5578 0412 3456 7890
ОПЕРАЦИЯ ВЫПОЛНЕНА КОД АВТОРИЗАЦИИ: НОМЕР ССЫЛКИ: ДАТА: 10/08/2012
 (ПОДПИСЬ КЛИЕНТА)

5. Сохраняйте расчетные документы (чек терминала, квитанция банкомата), подтверждающие проведение расчетной операции по вашему картсчету, минимум в течение 6 месяцев с даты совершения операции. По истечении указанного срока обязательно уничтожьте ненужные вам чеки, квитанции и иные документы, в которых указаны конфиденциальные данные вашей карты.
6. В случае если при попытке оплаты банковской картой имела место «неуспешная» операция, сохраните один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

ПРАКТИЧЕСКИЕ СОВЕТЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ В СЕТИ ИНТЕРНЕТ

1. Не вводите данные ПИН-кода при заказе товаров и услуг через сеть Интернет, а также не сообщайте ваш ПИН-код по телефону/факсу. Никакие операции в сфере электронной коммерции не требуют введения ПИН-кода.
2. Не сообщайте третьим лицам персональные данные или информацию о банковской(-ом) карте (счете) через сеть Интернет, например, пароли доступа к ресурсам банка, реквизиты банковской карты, одноразовые пароли для совершения интернет-операций и/или для привязки карты к мобильному устройству, кредитные лимиты, историю операций.
3. Откройте для оплаты товаров и услуг в сети Интернет отдельную карту, пополнять которую целесообразно непосредственно перед проведением операции в сети Интернет на сумму предполагаемой стоимости товара или услуги, которую вы намерены оплатить по карте. Не используйте для этих целей вашу зарплатную карту.
4. Установите на свой компьютер/смартфон/планшет антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых вами программных продуктов. Это поможет защитить вас от проникновения вредоносного программного обеспечения.

5. В целях безопасности пользуйтесь интернет-сайтами только известных и проверенных организаций торговли (услуг). Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий.
6. Совершайте покупки только сличных устройств в целях сохранения конфиденциальности персональных данных и (или) информации о картсчете. В случае если вы совершаете покупку с использованием чужого устройства, не сохраняйте на нем персональные данные и другую информацию.
7. Никогда не отвечайте на письма с просьбой обновить данные вашей карты через интернет-сайт. Любое подтверждение или обновление информации происходит только при личном обращении клиента в банк.
8. Находясь в людных местах (кафе, кинотеатрах, торговых центрах, гостиницах и пр.), везде, где есть общедоступная сеть WI-FI, обращайте внимание на тип Интернет-соединения. Соединение должно быть безопасным и начинаться с префикса https. Если подключение к общедоступной сети WI-FI небезопасно, не совершайте финансовые операции, не допускайте введения реквизитов карт, имен и паролей от ваших личных кабинетов.

ДОПОЛНИТЕЛЬНЫЕ МЕРЫ БЕЗОПАСНОСТИ

Уважаемые Клиенты АО БАНК «СНГБ» в дополнение к вышеописанным рекомендациям у вас есть возможность воспользоваться следующими услугами, обеспечивающими защиту денежных средств

1. Безопасные интернет-платежи.

Интернет-платежи держателей карт Сургутнефтегазбанка защищены с помощью новейших технологий — программ на базе международного протокола аутентификации 3DS MasterCard SecureCode, Verified by Visa и MirAccept.

Mastercard
SecureCode

VERIFIED
by VISA

MIRACCEPT

Программы MasterCard SecureCode, Verified by Visa и MirAccept предусматривают при проведении платежа ввод держателем карты одноразового секретного кода, который направляется банком посредством СМС-сообщения/ Push-уведомления на указанный клиентом номер телефона и требуется при совершении интернет-операций.

Внимание! НЕ СООБЩАЙТЕ НИКОМУ одноразовый секретный код, направленный Банком. Его могут запрашивать только мошенники.

2. Ограничение региона обслуживания банковской карты.

В Сургутнефтегазбанке реализован уникальный способ защиты от несанкционированного использования банковских карт, предлагающий держателям

банковских карт простое и эффективное средство безопасности — возможность самостоятельно ограничивать регионы обслуживания карты.

Например, вы находитесь в России и не планируете выезжать за границу — позвоните по телефонам круглосуточной службы поддержки клиентов, указанным на оборотной стороне вашей банковской карты, и отключите проведение операций по вашей карте во всех странах, кроме России. Планируете поехать в Европу — включите проведение операций в этом регионе, а по возвращении домой вновь отключите.

Внимание! Данный сервис не распространяется на проведение операций в сети Интернет.

3. Страхование пластиковых карт Сургутнефтегазбанка.

Держатели карт АО БАНК «СНГБ» имеют возможность застраховать денежные средства, находящиеся на карсчете по программе Страхового Общества «Сургутнефтегаз».

Страховой полис предполагает защиту от самых распространенных рисков, связанных с использованием банковских карт, 24 часа в сутки и по всему миру.

Страхованию подлежат пластиковые карты Сургутнефтегазбанка всех категорий.

С помощью рекомендаций по безопасности и новейших сервисов Сургутнефтегазбанка ваши потери будут сведены к минимуму или вовсе исключены!

Более полные рекомендации и практические советы по безопасному использованию банковских карт, правила пользования банковской картой, а также информацию о дополнительных сервисах вы можете найти на сайте банка: www.sngb.ru.

СЛУЖБА ПОДДЕРЖКИ ДЕРЖАТЕЛЕЙ БАНКОВСКИХ КАРТ

■ для физических лиц

(3462) 39-88-04 | 8-800-200-88-04 | 8-800-775-88-04
(по России звонок бесплатный)

■ для юридических лиц

(3462) 39-83-00 | 8-800-775-83-00
(по России звонок бесплатный)

<https://feedback.sngb.ru/>
www.sngb.ru

Информация носит справочный характер и не является публичной офертой.

Акционерное общество «Сургутнефтегазбанк»
8 800 775 88 04 | www.sngb.ru

Генеральная лицензия Банка России №588 от 05.09.2016 г.

628400, Тюменская область, Ханты-Мансийский автономный округ - Югра,
г. Сургут, ул. Григория Кукуевецкого, 19