Приложение № 1 Рекомендации по снижению рисков перевода денежных средств без добровольного согласия клиента и безопасному использованию банковских карт

МОСКОМБАНК
Commercial Bank of Moscow

РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА И БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ

В области информационной безопасности АО «МОСКОМБАНК» рекомендует Клиенту:

1. Никогда не оставляйте Карту в местах, где посторонние имеют возможность скопировать номер карты и/или образец Вашей подписи;
2. Никогда не пишите ПИН на Карте и не храните его вместе с Картой;
3. Не допускайте присутствия сторонних наблюдателей при вводе ПИН, а также не прибегайте к помощи посторонних лиц;
4. Помните, что ПИН является аналогом собственноручной подписи и инструментом для доступа к денежным средствам на Вашем счете;
5. Не передавайте Карту другому лицу за исключением кассира при ее использовании в качестве средства платежа или для получения наличных, при этом следите, чтобы Карта не покидала Вашего поля зрения;
6. Сохраняйте все документы по операциям с использованием карты;
7. Регулярно проверяйте совершенные операции и остаток денежных средств;
8. Никогда не давайте информацию о Карте (номер карты, срок действия, три последние цифры на полосе для подписи (так называемые CVV2/CVC2), ПИН для участия в лотерее, рекламных акциях, при телемаркетинге, в том числе при попытке узнать их с помощью телефона (обычного или мобильного), письма, программ передачи сообщений в сети интернет и т.п.;
9. Требуйте проводить операции оплаты товаров и услуг по Карте в Вашем присутствии. Не допускайте исчезновения Карты из Вашего поля зрения даже на незначительное время, чтобы предотвратить возможные мошеннические действия (информация о Карте может быть скопирована и использована для изготовления поддельной карты);
10. Не используйте Карту для оплаты, если кассир или торговая точка не вызывают у Вас доверия;
11. Не используйте Карту для получения наличных в банкомате, если он не вызывает у Вас доверия;
12. Старайтесь пользоваться банкоматами, расположенными в офисах банков, а не на улицах — это уменьшит риск копирования магнитной полосы и ПИН Карты;
13. Перед тем как вставить Карту в банкомат, проведите рукой по клавиатуре, гнезду для приема карт, убедитесь, что на клавиатуру не наклеена пленка, а в гнездо для приема крат не вставлено ничего постороннего;
14. При расчетах в интернете всегда пользуйтесь услугами интернет-магазинов, которые вызывают у Вас доверие, и на платежных страницах которых имеются логотипы «MIRAccept», «MasterCard SecureCode»;
15. При совершении платежей, оплаты услуг, мобильной связи, коммунальных услуг и т.п. через интернет отдавайте предпочтение системе дистанционного банковского обслуживания АО «МОС КОМБАНК» так, как только в этом случае исключается передача данных Карты через открытые сети интернета.
16. Используйте «СМС-информирование» для контроля операций по Вашей карте в режиме реального времени;
17. Подключите сервис «MIRAccept», «3D-Secure» для безопасных расчетов в интернете;
18. Установите индивидуальные ограничения по максимальным суммам операций по снятию наличных денежных средств (например, 10 000 рублей в день);
19. Используйте систему ДБО на сайте Банка *москомбанк.рф*.

В области социальной инженерии АО «МОСКОМБАНК» рекомендует Клиенту:

1. Обращать внимание на следующие признаки мошенничества:

- мошенник обращается с неизвестного номера телефона;
- мошенник представляется сотрудником Банка, Центрального Банка, Федеральных органов исполнительной власти (полиция, следователи, сотрудники Федеральной службы безопасности), операторов связи;
- Клиенту предлагается или какая-то выгода, или описывается проблема и предлагается путь решения;
- от Клиента требуют сообщить номера карты, ПИН-код, логин и пароль от банковских приложений, подтвердить код по СМС, перейти по ссылке в СМС или e-mail сообщении, т.е. провести компрометацию конфиденциальных данных;
- от Клиента требуют провести мгновенную оплату, перевод денежных средств;
- от Клиента требуют быстрого принятия решения, немедленной реакции;
- возражают против того, чтобы Клиент позвонил позже, препятствуют разъединению телефонного звонка.

Учитывать следующие типичные случаи мошенничества:

Предложение мошенника	Ваши действия
Ваша карта заблокирована СМС-сообщение о якобы заблокированной карте, требуют сообщить ПИН-код или совершить действия в банкомате	Не переходите по ссылкам, перезвоните в Ваш банк. Помните, банк никогда не будет запрашивать номер карты, ПИН, иные коды
Родственник в беде Требование крупной суммы денег за решение проблем родственника, который якобы попал в беду. Мошенник представляется сотрудником полиции.	Обратите внимание на входящий телефон, наверняка он мобильный. Положите трубку и свяжитесь с Вашим родственником напрямую.
Требуется помощь в социальной сети Ваш знакомый по социальной сети описывает несчастье, которое случилось с ним или его родственниками, знакомыми и публикую номер карты/телефона, на которую идет сбор средств.	Перезвоните Вашему знакомому, не вступайте в переписку, аккаунт под контролем мошенника.
Выигрыш СМС/e-mail-сообщение о крупном выигрыше, предлагают перейти по ссылке	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вирусная атака СМС/ e-mail-сообщение содержит ссылку на какой-либо интернет ресурс, содержащий вредоносную программу, дающую доступ к карте	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вам положена компенсация Для получения компенсации Вам предлагают авансом оплатить пошлины, проценты, доставку, страховку и т.п.	Все предложения, требующие каких-то немедленных платежей являются мошенническими, положите трубку
Ошибочный перевод средств просят вернуть денежный средства за якобы ошибочный перевод	Не делайте поспешных действий, вначале проверьте действительно ли Вам приходила неизвестная сумма.
Карта заблокирована звонок «сотрудника банка», предлагают разблокировать карту, для чего просят сообщить реквизиты карты, код на обратной стороне, ПИН-код.	Положите трубку. Сотрудник банка не будет запрашивать реквизиты карты и коды.
«Сотрудник банка» проводит проверку данных или оказывает услугу и просит подтвердить «проверочный код» «Вам по СМС должен поступить код, сообщите и проблема будет решена»	Положите трубку, сотрудники банка не высылают никаких СМС-кодов. Если Вы подтвердите код с Вас спишут деньги.
Звонок из банка — просят перевести деньги на безопасный счет «Сотрудник банка» сообщает, что поступило заявление на закрытие счета, как будете забирать деньги. Потом говорят, что это мошенничество и	Положите трубку, сотрудники банка не высылают никаких СМС-кодов.

предлагают сделать немедленно перевод на «безопасный счет», предлагают диктовать номер карты, ПИН-код, код на обратной стороне карты	
Предоплата товара на сайте На различных площадках в интернете Вы обнаружили товар по привлекательной цене, но требуется перевод авансом на карту, по телефону.	Изучите продавца, отзывы о нем, историю, позвоните, предложите оплату при доставке. Ни в коем случае не оплачивайте авансы.
Просьба дать в долг От Ваших, друзей знакомых по социальной сети приходит просьба срочно прислать денег в долг	Перезвоните Вашему знакомому, уточните информацию. Не вступайте в переписку в этой же социальной сети, аккаунт Вашего знакомого скорее всего мошеннический.
Одобрение кредита «Сотрудник банка» сообщает об одобрении кредита на выгодных условиях. Для доступа к кредиту, надо внести плату за рассмотрение, за страхование, за выезд курьера и т. п. Плату внести предлагают через терминал/банкомат.	Банк никогда не предлагает кредиты с предварительной оплатой каких-либо сопутствующих услуг.
Продление договора оператора связи «Сотрудник оператора связи» сообщает об окончании договора на мобильную связь и предлагает продлить его онлайн присылая ссылку, либо просит ввести код, который он уже выслал. В это время мошенник уже пытается взломать личный кабинет ЕСИА «Госуслуги» и код это от двухфакторной аутентификации при входе на портал.	Немедленно положите трубку. Зайдите на портал ЕСИА «Госуслуги» и сбросьте пароль от входа. Позвоните на горячую линию портала ЕСИА «Госуслуги» и расскажите об инциденте для быстрой блокировки личного кабинете и смены пароля.

В случае мошенничества или подозрения в мошенничестве по Вашей карте немедленно блокируйте ее, позвонив по телефонам:
+7 (495) 232-37-23 ежедневно и круглосуточно;
+7 (499) 246-14-40; +7 (495) 109-00-14 (многоканальный);
+7 (495) 109-00-14 по рабочим дням в рабочее время.