Памятка пользователю системы дистанционного банковского обслуживания

Уважаемые Клиенты!

КБ «МОСКОММЕРЦБАНК» (АО) информирует Вас о том, что в последнее время участились попытки неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (паролей, секретных ключей средств шифрования и аналогов собственноручной подписи). Также в сети Интернет появились сайты, имитирующие представительства ряда российских кредитных организаций. Имена и стиль оформления таких сайтов, как правило, сходны с именами подлинных сайтов банков, а содержание прямо указывает на их якобы принадлежность соответствующим кредитным организациям. Посетителям таких сайтов сообщаются заведомо ложные банковские реквизиты и контактная информация. Использование подобных реквизитов, а также вступление в какие-либо деловые отношения с лицами, фактически представляющими ложные банки, связано с риском и может привести к нежелательным последствиям для клиентов кредитных организаций.

Для повышения безопасности дистанционного банковского обслуживания КБ «МОСКОММЕРЦБАНК» (АО) рекомендует соблюдать следующие меры предосторожности:

- При работе в сети Интернет рекомендуется установить и регулярно обновлять антивирусное программное обеспечение;
- Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.
- Своевременно обновляйте операционную систему и используемое для работы в сети Интернет программное обеспечение (браузеры Explorer, Opera, Firefox; почтовые Клиенты Outlook, The Bat, Thunderbird и т.д.).
- При работе в сети Интернет будьте бдительны, устанавливайте дополнительные приложения, только если вы доверяете их разработчику;
- При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- Наш Банк никогда не отправляет электронные письма или SMS-сообщения с предложением сообщить пароли либо передать компоненты электронной подписи. При получении подобных сообщений просьба проинформировать наш Банк по телефону, либо отправить сообщение по электронной почте;
- При использовании документов, полученных с Web-сайта нашего Банка, в случае подозрений на их содержание либо авторство необходимо позвонить в соответствующий отдел по телефону;
- При посещении Web-сайта нашего Банка пользуйтесь прямым адресом: http://www.moskb.ru, либо воспользуйтесь ссылкой расположенной на сайте ЦБ РФ http://www.cbr.ru/credit/coinfo.asp?id=450039645; Старайтесь избегать перехода на сайт нашего Банка по ссылке со стороннего сайта;
- Интернет-адрес системы дистанционного банковского обслуживания должен строго соответствовать, указанному адресу в договоре на обслуживание. В случае обнаружения изменения в строке адреса, необходимо немедленно прекратить сеанс связи и связаться со службой технической поддержки банка по телефону, либо отправить сообщение по электронной почте;
- Осуществлять информационное взаимодействие с банком только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты/порталы, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в банке;
- Сотрудничать с Банком в принятии последним мер, направленных на минимизацию рисков при дистанционном банковском обслуживании.

При возникновении следующих ситуаций, просим незамедлительно обращаться в Банк, с целью оперативного блокирования доступа:

- На компьютере или электронном устройстве, используемом для работы в Системе, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
- В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
- В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS уведомление об операции, которую не совершали.
- Вы получили SMS или e-mail уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.