ПРАВИЛА
информационной безопасности при использовании Системы Интернет – банк

1. Общие положения

1.1. Настоящие Правила информационной безопасности при использовании Системы Интернет - банк составлены в соответствии с требованиями действующего законодательства Российской Федерации, Положением Банка России «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» от 09.06.2012 №382-П, стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», Письмом Банка России от 05.08.2013 N 146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети Интернет» и другими нормативными документами Банка России, Методическими рекомендациями Ассоциации российских банков и НП «Национальный платежный совет» «О порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента», Международными стандартами ISO 27001:2005 и ISO 17799.

1.2. Настоящие Правила определяют рекомендуемые Банком действия Клиентов по обработке рисков нарушения информационной безопасности при использовании Системы Интернет - банк.

1.3. При работе с Системой Интернет – банк через сеть Интернет необходимо учитывать следующее:

1.3.1. Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими.

1.3.2. Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет.

1.3.3. Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные к/из сети Интернет.

1.3.4. Гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

2. Ответственность сторон

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему Интернет – банк, Клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

2.2. Клиент уведомлен о том, что за пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 Уголовного Кодекса Российской Федерации.

2.3. Окончательное решение об использовании Защитных мер, предлагаемых Банком в разделе 3 Правил информационной безопасности при использовании Системы Интернет – банк, принимает сам Клиент.

2.4. Банк вправе устанавливать ограничения по составу услуг доступных при использовании той или иной Защитной меры.

2.5. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы Интернет – банк. Содержимое журнала Системы Интернет – банк используется при разрешении спорных ситуаций.

3. Рекомендуемые Клиенту Защитные меры:

3.1. Не используйте Сеансовый ключ для подтверждения каких – либо действий, кроме подтверждения Операций в Системе Интернет – банк. Не вводите Сеансовый ключ в иную программу/ сайт, и ни при каких условиях не сообщайте информацию о Сеансовом ключе лицам, представляющимся работниками Банка. При возникновении подобных ситуаций незамедлительно обратитесь в Банк по телефону 8-800-200-14-15.

3.2. Не сообщайте посторонним лицам персональные данные или информацию о Карте/Счете через сеть Интернет, Имя пользователя и/или Постоянный пароль доступа к ресурсам Банка, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Счету(ам) Клиента.

3.3. Не записывайте Имя пользователя и Постоянный пароль на бумаге, мониторе или клавиатуре.

3.4. Не используйте функцию запоминания Имени пользователя и Постоянного пароля в браузерах.

3.5. Не используйте одинаковые Имя пользователя и Постоянный пароль в различных системах.

3.6. Не пользуйтесь системами, требующими ввода Имени пользователя и Постоянного пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте Операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о Карте/Счете;

3.7. Не используйте бесплатную или не защищенную паролем сеть Wi – Fi для доступа к Системе Интернет – банк. Общественные сети не могут гарантировать полную защищенность Ваших данных. Любая информация может быть перехвачена Злоумышленниками. Не допускайте автоматического подключения к сети Wi – Fi.

3.8. Всегда явным образом завершайте Сеанс соединения с Системой Интернет - банк, используя пункт меню «Выход».

3.9. В случае если Операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех Операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web – страницу). После возвращения к своему средству доступа обязательно смените Имя пользователя и Постоянный пароль.

3.10. Если Вы получили на электронную почту или по иным каналам электронных коммуникаций сообщение с предложением обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка), перезвоните в службу поддержки держателей банковских карт Банка по телефонам:

– 8-800-200-14-15 для звонков из России (звонок по России бесплатный);
– +7-495-626-47-66 для звонков из-за границы;

и сообщите о данном факте или перешлите сообщение на адрес ib-support@mosoblbank.ru. Банк никогда не предлагает передать данные подобным образом.

Обновление ключевых персональных данных осуществляется только работником Банка и только по обращению Клиента.

3.11. Не открывайте приложения от незнакомых отправителей, так как в них может находиться вредоносное программное обеспечение, способное передать доступ к Вашим Базовым идентификационным данным Злоумышленникам, которые могут их использовать их для входа в Систему Интернет – банк от имени Клиента.

3.12. Регулярно, не реже одного раза в месяц, меняйте Постоянный пароль.

3.13. При составлении Постоянного пароля используйте прописные и строчные буквы, цифры, а также различные символы. Настоятельно рекомендуется использовать специализированные программы – генераторы паролей (http://www.infotecs.ru/Soft/pass.htm).

3.14. Не использовать в качестве Постоянного пароля имена, памятные даты, номера телефонов.

3.15. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что за пользование нелицензированным программным обеспечением предусмотрена уголовная ответственность в соответствии со статьей 146 Уголовного Кодекса Российской Федерации, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

3.16. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий используемого на Вашем техническом устройстве, с которого осуществляется доступ к Системе Интернет – банк, программного обеспечения и обновляйте антивирусные базы. В случае

обнаружения вредоносного программного обеспечения на компьютере после его удаления незамедлительно смените Имя пользователя и Постоянный пароль в Системе Интернет – банк.
3.17. Защищайте свой техническое устройство, на которое получаете информацию о Сеансовом ключе, паролем на вход. Не допускайте попадания этого технического устройства/ sim – карты в руки третьих лиц.
3.18. Если Вы используете техническое устройство для получения Сеансовых ключей с операционной системой, такой как Android, iOS, Symbian, Windows Mobile, то установите на нем мобильный антивирус.
3.19. Защищайтесь от фальсификаций sim – карты. Не используйте для получения SMS – сообщений Банка sim – карты, полученные из сомнительных источников. Sim – карта должна быть оформлена на Ваше имя. При обнаружении признаков потери работоспособности (нет связи), а также в случае утраты или кражи sim – карты, незамедлительно обратитесь в Банк для блокирования доступа к Системе Интернет – банк.
3.20. Не запускайте на своем техническом устройстве, с которого осуществляется доступ к Системе Интернет – банк, программы, полученные из незаслуживающих доверия источников.
3.21. Не устанавливайте на свое техническое устройство, с которого осуществляется доступ к Системе Интернет – банк, средства удаленного управления.
3.22. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.
3.23. Не храните незашифрованные личные данные в электронной почте, «облачных» хранилищах, технических устройствах, подключенных к сети, так как эти данные могут быть похищены Злоумышленниками и использованы для получения доступа к Вашим Счетам.
3.24. Если Вам пришло электронное сообщение или SMS-сообщение о выигрыше в акции, лотерее, розыгрыше удостоверьтесь в его подлинности, прежде чем отсылать деньги на чей-то счет с использованием Системы Интернет – банк. Все акции, проводимые Банком, не требуют от Клиента перевода денежных средств для получения приза.
3.25. Перед вводом своего Имени пользователя и Постоянного пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверить правильность указания адреса сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в Систему Интернет – банк. В случае обнаружения подозрительных web – сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официального сайта ПАО МОСОБЛБАНК, сообщить об этом по электронной почте ib-support@mosoblbank.ru.
3.26. Используйте предлагаемые Банком услуги по дополнительному информированию о входе в Систему и совершаемых Операциях. Регулярно проверяйте входящую электронную почту, а также контролируйте выписки по Счетам. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.
3.27. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе Интернет – банк, незамедлительно смените Имя пользователя и Постоянный пароль и сообщить об Инциденте информационной безопасности в службу поддержки держателей банковских карт Банка. Следуйте указаниям специалистов Банка.
3.28. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших Счетах, необходимо подать заявление на временное блокирование доступа в Систему Интернет - банк, подать заявление о преступлении в правоохранительные органы и прекратить использование (обесточить) техническое устройство, с которого осуществляется доступ в Систему Интернет – банк, в целях сохранения доказательной базы. Если Вы пользуетесь аналогичными системами других банков – заблокируйте их до выяснения обстоятельств происшествия. Эти учетные записи также могут оказаться скомпрометированными.
3.29. В сети Интернет существует много ресурсов по вопросам информационной безопасности. Регулярно знакомьтесь с их содержимым. Помните, Угрозы постоянно видоизменяются и развиваются.