Приложение № 9 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ БАНКЕ

В целях обеспечения информационной безопасности при работе в Электронном банке **Клиент обязуется**:

1. Осуществлять вход в Электронный банк только через корпоративный сайт АО «МОСКОМБАНК», используя адрес https:\\mypay.moscombank.ru, либо через специальное приложение, которое может быть установлено на мобильное устройство из магазинов AppStore или GooglePlay.
2. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену москомбанк.рф, www.moscombank.ru, сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефону (495) 609-19-19 доб.511. Банк не осуществляет рассылку подобных электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Электронного банка.
3. Не отлучаться от компьютера в период активной сессии с Электронным банком, особенно пока к нему подключен USB-токен или другой носитель, содержащий ключ ЭП.
4. Извлекать из компьютера USB-токен или другой носитель, содержащий ключ ЭП, сразу после завершения работы в Электронном банке.
5. Не передавать пароли, PIN-коды и коды доступа, USB- и OTP-токены или другие устройства, содержащие ключ ЭП, другим лицам, в том числе сотрудникам Банка для проверки работоспособности или настройки Электронного банка, хранить их в надежном месте, исключающем доступ к ним посторонних лиц. Вся ответственность за сохранность и использование ключей ЭП, одноразовых паролей, а также логина, пароля, PIN-кода для доступа к Электронному банку, полностью лежит на Клиенте, как единственном их владельце.
6. В случае выявления явных или косвенных признаков компрометации ключа ЭП, а также обнаружения вредоносных программ в компьютере, используемом для работы в Электронном банке, незамедлительно уведомить об этом Банк по телефону: (495) 609-19-19 доб.511, либо лично явиться в Банк с целью блокирования скомпрометированных данных с последующей их заменой. К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

- утеря USB- или OTP-токена или другого устройства, содержащего ключ ЭП, в том числе с последующим обнаружением;
- выход из строя USB- или OTP-токена или другого устройства, содержащего ключ ЭП, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- обнаружение факта или угрозы использования (копирования) идентификаторов учетной записи или одноразовых паролей доступа к Электронному банку неуполномоченных лиц (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Электронного банка, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение воздействия вредоносного кода в компьютере, используемом для работы в Электронном банке.

7. В случае выявления явных или косвенных признаков компрометации пароля учетной записи менять данный пароль самостоятельно.
8. Обеспечивать конфиденциальность использования паролей доступа, PIN-кодов, одноразовых паролей, которые не требуется сотрудникам Банка для обслуживания Клиента и поддержки Электронного банка в работоспособном состоянии.
9. Применять на компьютерах, используемых для работы Электронного банка, лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, антиспам-фильтры и т.п.
10. Производить периодическую (не реже 1 раза в 3 месяца) смену долговременного пароля и/или смену ключей ЭП, а также по требованию Банка и в случае компрометации. Не использовать простые пароли (123, qwerty, имена, даты рождения и т.д.).
11. Самостоятельно настроить используемое оборудование и программное обеспечение для работы с сетью Интернет по защищенному протоколу https.
12. Не использовать на своем компьютере любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer и др.). Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).
13. При использовании мобильного устройства установить на него антивирусное программное обеспечение и пароль доступа к устройству, не использовать мобильное устройство с расширенными правами (Jailbreak/Root), так как это значительно снижает уровень обеспечения безопасности устройства, регулярно устанавливать обновления для Вашего устройства и установленного антивирусного программного обеспечения, защитить свое мобильное устройство кодом блокировки экрана.
14. Не заходить в Электронный банк через приложения для мобильных устройств на базе Android и iOS с того же мобильного устройства, на которое приходят СМС-сообщения с подтверждающим одноразовым паролем. Использовать в таких ситуациях OTP-токены для генерации одноразовых паролей.
15. Не устанавливать на мобильное устройство, используемое для приема СМС-сообщений с подтверждающим одноразовым паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email сообщения.
16. При утрате мобильного устройства, используемого для приема СМС-сообщений с подтверждающим одноразовым паролем, немедленно обратиться к оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Электронному банку и проверки последних платежей.

Помимо указанных выше требований **Банк рекомендует**:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Электронного банка: символ замка и буква «S» в адресной строке – https://mypay.moscombank.ru, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.
2. Исключить доступ посторонних лиц к компьютеру, использующегося для работы в Электронном банке. Осуществлять постоянный контроль отправляемых платежных электронных документов при работе в Электронном банке, а также состояние своего личного счета.
3. Избегать работы в Электронном банке при подключении к публичным точкам доступа Wi-Fi, в интернет-кафе и на других компьютерах общего пользования, контролировать информацию об IP-адресе, с которого осуществлялся предыдущий вход в Электронный банк.
4. Не использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, имена, фамилии, даты рождения и т.д., не записывать его там, где доступ к нему могут получить посторонние лица.
5. Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО, исключить использование самодельных «сборок» и взломанного программного обеспечения.

6. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Электронному банку только с указанных Клиентом IP-адресов/сетей).