Приложение 9

к Общим условиям и правилами предоставления услуг с использованием системы «Мой МСП» в АО «МСП Банк»

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СИСТЕМЫ

1. Для доступа к Системе на ПЭВМ используйте пароль, отвечающий следующим требованиям:

– Длина пароля должна быть не менее 8 и не более 14 символов.

– Пароль должен состоять из букв латинского алфавита (A-z), арабских цифр (0-9) и специальных символов, приведенных в настоящем пункте.

– Буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы.

– Пароль должен содержать не менее одного из следующих символов:

(. , : ; ? ! * + % - < > @ [ ] { } / \ _ {} $ #).

Рекомендуется изменять пароль доступа в Систему не реже одного раза в три месяца.

2. На ПЭВМ/мобильном устройстве, использующемся для доступа к Системе «Мой МСП» должно использоваться только лицензионное антивирусное программное обеспечение. Регулярно производите его обновление и полную антивирусную проверку ПЭВМ/мобильного устройства, а также обновление операционной системы и используемых программ (Браузера и иных прикладных программ). Используйте программное обеспечение только из проверенных и надежных источников.
3. Не храните на ПЭВМ и/или мобильном устройстве конфиденциальную информацию о логине и пароле для доступа к Системе. Если такая необходимость все же есть, то не храните информацию в явном виде.
4. Удаляйте конфиденциальную информацию в случае передачи ПЭВМ и/или мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек, форматирования жесткого диска и др.
5. Обязательно сверяйте данные об операциях, указанные в полученных от Банка SMS-сообщениях, с данными по фактически совершенным операциям, на предмет выявления несанкционированных платежных операций.
6. При получении временных паролей/одноразовых паролей по SMS обращать внимание на отправителя. Банк отправляет сообщения только от абонента MSPBank.
7. После окончания работы в Системе обязательно завершайте сеанс, используя кнопку «Выход».
8. Ни при каких условиях не сообщайте /не передавайте информацию о Вашем логине, пароле, одноразовых паролях и иных сведениях, используемых для авторизации в каналах ДБО никому, включая сотрудников Банка. Также никому не сообщайте / не передавайте сведения о своем коде доступа (одноразовом пароле, полученном в sms-сообщении).
9. Не храните в мобильном телефоне информацию, полученную от Банка в виде SMS-сообщений.
10. При возникновении подозрений, что Ваши данные для доступа (логин или пароль) стали известны посторонним и/или в случае утери мобильного устройства заблокируйте доступ к Системе, **обратившись в Банк по телефону +7 (495) 783-79-70 <u>в рабочее время Банка</u>** и обязательно принудительно смените пароль доступа к Системе.
11. Заходите в Систему только с Официального сайта Банка. Прежде чем пройти авторизацию в Системе, убедитесь, что соединение происходит в защищенном режиме с использованием протокола HTTPS (появляется буква S в адресной строке, удостоверьтесь в правильности сертификата TLS-соединения).
12. При каждом входе проверяйте дату и время последнего входа в Систему.

13. Для осуществления входа в Систему рекомендуется использовать виртуальную клавиатуру, предоставляемую Системой.
14. Не пользуйтесь Системой в общедоступных местах, на компьютерах, безопасность которых вызывает сомнения (например, в Интернет-кафе, чужой компьютер). Если Вы все же заходили с чужого компьютера, смените пароль для входа в Интернет-банк с Вашего ПЭВМ, как только будет такая возможность.
15. Установите и используйте персональный брандмауэр (firewall) для входа в сеть Интернет, это позволит предотвратить несанкционированный доступ к информации на Вашем компьютере.
16. Не пользуйтесь Системой на компьютере, который используется под учетной записью, имеющей права администратора операционной системы, а также если имеется подозрение, что компьютер заражен вирусной программой. Симптомы заражения:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в сеть Интернет, хотя пользователь этого не инициировал;
- частые зависания и сбои в работе компьютера, медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.

17. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web-сайты, имеющие похожие адреса, или перенаправление на них с других ресурсов. К примеру, msp-bank.ru, mspbahk.ru, mspbamk.ru вместо верного mspbank.ru. Внимательно проверяйте адрес сайта перед авторизацией или совершением операций. Если он отличается от https://www.mspbank.ru/ – не используйте данный сайт. Для входа в Систему перейдите по ссылке с Официального сайта Банка www.mspbank.ru или наберите адрес Системы в Браузере вручную.
18. Не отвечайте на подозрительные звонки и звонки с неизвестных номеров или номера, которые не определяются, электронные письма (в т.ч. не переходите по ссылкам в электронных письмах) и сообщения из социальных сетей, которые запрашивают конфиденциальную информацию (логин, пароль, одноразовый пароль и т.п. информацию), в том числе от работников Банка и их родственников. Банк никогда не обращается к Клиентам с подобными просьбами.

Дополнительные рекомендации:

Банк рекомендует отслеживать информацию по вопросам информационной безопасности в связи с видоизменением способов мошеннических действий и информационных угроз.

Вам могут быть полезны следующие ресурсы:

«Управление «К» предупреждает: будьте осторожны и внимательны!»:
http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf
«Вредоносные программы в интернете»:
http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf
«Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf
«Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf
Для обнаружения необходимости установки обновлений Браузера рекомендуем Вам использовать сервис обнаружения уязвимостей: http://www.surfpatrol.ru/.

Внимание! По всем вопросам, связанным с обеспечением безопасности в системе «Мой МСП», Вы можете обратиться с 09-00 до 18-00 в Службу информационной безопасности Банка по одному из следующих телефонов: +7 (495) 783-79-70, +7 (800) 30-20-100