Памятка Пользователю по безопасной работе с системой дистанционного банковского обслуживания «ОРГБАНК Retail» МБО «ОРГБАНК (ООО)

Соблюдение рекомендаций, содержащихся в настоящей Памятке, снизит риски совершения несанкционированных операций при использовании системы «ОРГБАНК Retail» (далее по тексту – Система) и обеспечит сохранность денежных средств, размещенных на счетах Пользователя.

МБО «ОРГБАНК (ООО) (далее по тексту – Банк) обеспечивает защиту центральной части Системы, однако для надежной и безопасной работы необходимо участие в этом процессе и Пользователя.

1. Общие рекомендации

1.1. Осуществляйте вход в Систему только с официального сайта Банка «ОРГБАНК» (ООО) (далее по тексту – Банк) https://www.orgbank.ru.

1.2. При входе в Систему убедитесь в наличии символа закрытого замка в адресной строке браузера или в правом нижнем углу страницы. В адресной строке Вашего браузера должен отображаться адрес: https://retail.orgbank.ru. Если Вы видите другой адрес, ни в коем случае не вводите свои логин и пароль в представленную форму, закройте окно и сообщите об этом в Банк.

1.3. Устанавливайте разработанный для портативных персональных компьютеров или устройств мобильной связи вариант Системы (Мобильное приложение) только через официальные магазины приложений (Google Play https://play.google.com, Apple AppStore https://appstore.com).

1.4. Используйте Систему, руководствуясь инструкциями Банка, размещенными на официальном сайте Банка в сети Интернет по адресу: https://www.orgbank.ru.

1.5. При осуществлении первого входа в Систему измените временный пароль на пароль, который сможете запомнить.

1.6. Используйте в качестве паролей сложные комбинации заглавных и строчных букв и цифр.

1.7. Не используйте в качестве паролей простые последовательности букв и цифр, номера телефонов и паспортов, даты рождения ближайших родственников, названия оргтехники, компаний и т.п.

1.8. Пользуйтесь при вводе пароля виртуальной клавиатурой.

1.9. Храните в секрете информацию, необходимую для осуществления аутентификации в Системе: логин, временный пароль, пароль, одноразовый пароль.

1.10. Изменяйте пароль, необходимый для аутентификации в Системе, не реже одного раза в месяц.

1.11. Не отвечайте на подозрительные звонки, электронные письма и сообщения, которые запрашивают конфиденциальную информацию. Помните, что Банк никогда не запрашивает подобную информацию у своих клиентов.

1.12. Не осуществляйте вход в Систему используя публичные услуги доступа к сети Интернет, например, в Интернет – кафе или в общественном транспорте.

1.13. Используйте системное программное обеспечение официальных производителей Устройства. Не видоизменяйте его (например, через Jailbreaking), так как это отключает защитные механизмы, заложенные производителем; не используйте на Устройстве с установленной Системой режим суперпользователя.

1.14. Не устанавливайте из недостоверных источников программное обеспечение на устройство, с которого осуществляется работа в Системе (далее по тексту – Устройство), не открывайте на нем электронные письма и вложения в электронные письма от незнакомых отправителей или в случаях, когда нет уверенности в подлинности отправителя/безопасности содержимого письма.

1.15. Включите (если не был включен) парольный доступ к Устройству. Используйте надежные сложные пароли и регулярно их меняйте.

1.16. При установке новой программы обращайте внимание на разрешения, которые требует программа для своей работы, особенно на возможности доступа к SMS-сообщениям. Если

разрешения вызывают подозрения или явно не соответствуют функционалу программы, лучше отказаться от ее установки.

1.17. При утере, краже или смене Зарегистрированного номера, немедленно сообщите об этом в Банк.
1.18. При необходимости передачи Устройства другому лицу для ремонта обратитесь в Банк для временного блокирования дистанционного банковского обслуживания.
1.19. Отключите в настройках своего Устройства возможность использовать голосовое управление при заблокированном экране.
1.20. Настройте блокировку экрана на Устройстве при отсутствии активности.
1.21. Предпринимайте все необходимые меры для исключения доступа третьих лиц к изменению программной среды и настроек Устройства.
1.22. Используйте лицензированную версию операционной системы на Устройстве с автоматическим обновлением.
1.23. Используйте на Устройстве лицензионное антивирусное программное обеспечение с автоматическим обновлением.
1.24. Осуществляйте вход в Систему только с Устройств, находящихся в личном пользовании.
1.25. При каждом входе в Систему проверяйте на соответствие дату и время последнего входа.
1.26. Отключите в настройках операционной системы Устройства кеширование паролей.
1.27. Установите запрет на доступ сторонних пользователей к файлам и папкам Устройства, исключите возможность установки программ, обеспечивающих удаленное подключение к Устройству.
1.28. При проведении платежей сверяйте сумму перевода, отраженную на экране монитора, с информацией в SMS – уведомлении. При обнаружении расхождений между данными Системы и фактически выполненными Вами платежами, немедленно информируйте об этом Банк.
1.29. Решив закончить работу с Системой, нажмите соответствующие пункты меню для выхода из Системы.
1.30. Не храните в мобильном телефоне информацию, полученную от Банка в виде SMS-сообщений.
1.31. При получении одноразовых паролей в виде SMS-сообщений, обращайте внимание на отправителя. Банк отправляет сообщения только от абонента – ORGBANK.
1.32. В случае внезапного приостановления работы SIM-карты, номер которой является зарегистрированным номером для направления Банком SMS-сообщений, незамедлительно обратитесь к оператору мобильной связи для выяснения причин (с целью предотвращения использования незаконно изготовленного третьими лицами дубликата SIM-карты). При необходимости осуществите блокировку дистанционного банковского обслуживания, обратившись в Банк.
1.33. Бережно относитесь к устройству, выданному Банком в качестве генератора одноразовых паролей. Не передавайте Генератор одноразовых паролей третьим лицам и незамедлительно информируйте Банк обо всех случаях его утраты, случайной гибели, повреждения, технических неисправностях и т.п.

2. Служба поддержки

2.1. Телефон технической поддержки Системы (495) 956-15-88 (Понедельник – пятница с 9.00 до 18.00).
2.2. Телефон поддержки по совершенным операциям (495) 234-47-57 (Понедельник – пятница с 9.00 до 18.00).
2.3. Телефон для устного блокирования дистанционного банковского обслуживания с использованием кодового слова (495) 234-47-57 (Понедельник – пятница с 9.00 до 18.00), телефон для блокирования путем отправки SMS с текстом «block» с Зарегистрированного номера (903)767-62-60 (круглосуточно).
2.4. Телефон для блокирования платежной карты (495) 234-47-37 (круглосуточно).

3. Действия Клиента при обнаружении факта доступа постороннего лица к Системе/к защищаемой информации о Пароле/Временном пароле/Одноразовом пароле или подозрении на такой факт

3.1. При обнаружении факта доступа постороннего лица к Системе/к защищаемой информации о Пароле/Временном пароле/Одноразовом пароле или подозрении на такой факт, а также в случае несанкционированного списания денежных средств, незамедлительно заблокируйте Систему и все платежные карты, счета которых подключены к дистанционному банковскому обслуживанию, обратившись по телефонам, указанным в п.2.3. и 2.4. настоящей Памятки.

3.2. Информирование Банка производите в порядке, предусмотренном «Условиями дистанционного банковского обслуживания физических лиц МБО «ОРГБАНК» (ООО) в системе «ОРГБАНК Retail».

3.3. После получения информации согласно п. 3.1. Банком предпринимаются соответствующие действия по блокировке платежных карт и доступа Пользователя в Систему с дальнейшей заменой параметров аутентификации Пользователя, а также, в случае необходимости Банком собирается разрешительная комиссия с участием независимой стороны для анализа спорных ситуаций.