Приложение№ 8

к Правилам дистанционного банковского обслуживания
физических лиц в АКБ «Энергобанк» (АО) с
использованием Системы «Энергобанк»

Рекомендации по безопасному использованию системы дистанционного банковского обслуживания «Энергобанк»

г. Казань

Уважаемый Клиент!

АКБ «Энергобанк» (АО) (далее - Банк) обеспечивает безопасность системы дистанционного банковского обслуживания «Энергобанк» (далее - Система) со своей стороны, вместе с тем, рекомендуем Вам соблюдать следующие рекомендации, которые позволят максимально безопасно работать с Системой и свести риски мошенничества к минимуму.

Общие рекомендации по обеспечению безопасности Системы

1. Убедиться, что установлено безопасное соединение с сайтом Системы, адресная строка начинается с «https://», и соединение установлено именно с сайтом Системы Банка, в адресной строке браузера указано **https://digital.energobank.ru.**

2. Проверить дату и время последнего успешного входа в Систему.

3. В целях предотвращения несанкционированного доступа посторонних лиц к Системе Клиент осуществлять периодическую (минимум раз в квартал, но не менее одного раза в год) замену пароля.

4. Не передавайте/не сообщайте средства доступа к Системе (логин, пароль, одноразовых паролях и иных средствах доступа) другим лицам (родственникам, знакомым, работникам Банка).

5. Не храните пароль в текстовых файлах на компьютере или на съемных носителях, а также на бумажном носителе**, постарайтесь запомнить свой пароль**.

6. Используйте надежные пароли - длиной не менее 8 символов, содержащие буквы из различных регистров (заглавные и строчные), специальные символы (*, &, ^, % и т.п.) и цифры. Не используйте очевидные сочетания (имя, фамилия, дата рождения, номер телефона).

7. Не следуйте по «ссылкам», указанных в письмах (включая ссылки на сайт Банка), так как они могут вести на сайты-двойники.

8. Избегайте работы с Системой в публичной среде (интернет-кафе, социальные точки доступа в интернет и др.).

9. Применяйте на своем электронном устройстве (компьютер/ноутбук/планшет) лицензионное системное, прикладное и антивирусное программное обеспечение.

10. Регулярно производите полную проверку электронных устройств на наличие/отсутствие вредоносных программ.

11. При работе в сети Интернет никогда не соглашайтесь на установку каких-либо дополнительных программ, если Вы не знаете для чего это нужно. Исключите посещение сайтов сомнительного содержания.

12. Регулярно проверяйте состояние своих счетов в Системе. и незамедлительно сообщайте сотрудникам Банка по телефону Контакт - Центра **8 (800) 350-54-58** обо всех подозрительных операциях.

13. При длительном бездействии в Системе ДБО выходите из нее.

14. Подключите услугу «СМС-информирование». Услугу «СМС-информирование» можно подключить в дополнительных офисах Банка и в Системе. Это позволит Вам в реальном времени получать информацию об операциях по картам.

15. Обязательно сверяйте данные об операциях, указанные в полученных от Банка СМС-сообщениях, с данными по фактически совершенным операциям на предмет выявления несанкционированных операций.

16. При завершении работы с Системой используйте кнопку «Выход».

Меры безопасности при использовании Мобильного приложения

1. Устанавливайте мобильное приложение «Энергобанк» и его обновления только из приложений Apple AppStore / Google Play Market. Ссылки для установки указаны на сайте Банка www.energobank.ru.

2. При потере мобильного телефона с подключенным Мобильным сервисом «Энергобанк» (приложение для доступа к Системе при помощи мобильного устройства) следует срочно обратиться к оператору сотовой связи для блокировки SIM – карты и в Контакт – Центр Банка по номеру **8 (800)350-54-58** для блокировки мобильного сервиса «Энергобанк».

3. Будьте внимательны – не оставляйте свой телефон без присмотра, чтобы исключить несанкционированный доступ посторонних лиц к Системе. Установите на телефоне пароль.

4. При установке на телефон дополнительных программ обращайте внимание на полномочия, которые необходимы программе. Если программе требуются излишние полномочия это повод проявить настороженность. Обращайте внимание на такие опасные разрешения: доступ и отправка sms, доступ к сети Интернет.

5. Установите на телефон антивирусное программное обеспечение и своевременно его обновляйте.

6. При внезапном прекращении работы или блокировке SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин. Возможно, в отношении Вас произведены мошеннические действия третьими лицами.

7. Не «взламывайте» систему защиты iPhone (jailbreak) и не открывайте «root» доступ для устройств на операционной системе Android, так как это отключает защитные механизмы, заложенные производителем. В результате этой операции телефон становится уязвимым к заражению вирусным программным обеспечением.

8. Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по SMS/электронной почте.

Остерегайтесь мошенничества.

1. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли, параметры банковских карт и другие конфиденциальные данные). Не отвечайте на такие сообщения.

2. Не открывайте подозрительные файлы, присланные Вам по электронной почте. При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении.

3. При работе с Системой обращайте внимание на страницу входа и интерфейс системы. Если у Вас возникли подозрения в подлинности сайта, необходимо незамедлительно прекратить работу и связаться с Банком по телефону **8 (800) 350 54 58** (никогда не связывайтесь по телефону, указанному на подозрительной странице).

4. Банк никогда не запрашивает одноразовый пароль или пароль на вход в Систему для отмены операций. При вводе пароля Вы даете Банку право на проведение операции, отменить ее с помощью пароля нельзя.

5. Если Вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему или одноразовый пароль

6. Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Системе. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности Системы вследствие проведения каких-либо регламентных работ. Если Вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то

рекомендуется сообщить о данном факте в Банк по телефону **8 (800) 350 54 58** (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).

Помните! Вся ответственность за конфиденциальность и сохранность паролей лежит на Клиенте.