Приложение № 1
к Условиям дистанционного банковского обслуживания физических лиц
в ООО «Хакасский муниципальный банк» с использованием системы Интернет-банк ХМБ-онлайн

Правила безопасности пользователей системы Интернет-банк ХМБ-онлайн

- Не сообщайте свою персональную информацию (номер Банковской карты, номера счетов, реквизиты документа, удостоверяющего личность и т.д.) посторонним. Сотрудник ООО «Хакасский муниципальный банк» имеет право спрашивать Вас подобную информацию только в случае, если Вы самостоятельно обратились в Банк;
- Банк не направляет своим клиентам электронные письма и СМС-сообщения с просьбой уточнить их персональные данные. Будьте бдительны: не отвечайте на подобные запросы. В случае получения такого сообщения просим Вас незамедлительно сообщить об этом, по телефону: 8-800-755-88-00 с понедельника по пятницу: с 08:00 – 18:00 часов, Служба поддержки: 8 (800) 200-92-50 (круглосуточно, бесплатно по России);
- Не передавайте никому свой Логин. Обязательно, после первичного входа в систему, используя временный пароль, направленный Вам в СМС-сообщении, измените его;
- Не записывайте и не храните Логин и пароль для доступа к системе Интернет-банк ХМБ-онлайн там, где доступ к нему могут получить посторонние (включая мобильный телефон и компьютер);
- Не используйте в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в других системах. пароль должен быть от 8 до 15 символов и содержать строчные и прописные латинские буквы и цифры;
- Клиент может изменять свой пароль для доступа в систему Интернет-банк ХМБ-онлайн. Смена пароля должна производиться Клиентом не реже одного раза в квартал. Изменить пароль Вы можете самостоятельно, обратившись на страницу Вашего «Профиля» в системе Интернет-банк ХМБ-онлайн и нажав кнопку Настройки - «Изменить пароль». Для изменения пароля необходимо ввести текущий пароль;
- Запомните, что для входа в Интернет-банк ХМБ-онлайн требуется вводить только Ваш Логин и пароль. Не нужно вводить номер Вашего мобильного телефона, номер Вашей Банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации;
- При появлении подозрений, что Логин или пароль стали известны третьим лицам, незамедлительно сообщите об этом по телефону: 8-800-755-88-00 с понедельника по пятницу: с 08:00 – 18:00 часов, Служба поддержки: 8 (800) 200-92-50 (круглосуточно, бесплатно по России), либо в офис Банка для отключения доступа в систему Интернет-банк ХМБ-онлайн;
- В случае утраты Логина и/или пароля, Клиенту необходимо незамедлительно отключить доступ в систему, обратившись по телефону: 8-800-755-88-00 с понедельника по пятницу: с 08:00 – 18:00 часов, Служба поддержки: 8 (800) 200-92-50 (круглосуточно, бесплатно по России), либо обратившись в офис Банка;
- Рекомендуется установить пароль на доступ к телефону и/или на доступ к СМС-сообщениям (при наличии технической возможности). В случае утери телефонного аппарата или SIM-карты необходимо незамедлительно обратиться в Банк для отключения доступа к системе Интернет-банк ХМБ-онлайн по телефону:–8-800-755-88-00 с понедельника по пятницу: с 08:00 – 18:00 часов, Служба поддержки: 8 (800) 200-92-50 (круглосуточно, бесплатно по России) или в офис Банка;
- Прежде чем начать работу в системе Интернет-банк ХМБ-онлайн, убедитесь, что находитесь на стартовой странице системы Интернет-банк ХМБ-онлайн. Помните, что сайты, визуально напоминающие банковский сайт, создаются специально для незаконного получения Вашей персональной информации;
- При вводе личной информации помните, что любой веб-адрес в адресной строке Интернет-банка ХМБ-онлайн должен начинаться с «https». Если в адресе не указано «https», это значит, что Вы находитесь на незащищенном веб-сайте, и вводить данные нельзя;
- Банк не рекомендует работать с системой Интернет-банк ХМБ-онлайн на компьютерах в Интернет-кафе или на других компьютерах общего пользования. Если возможность выполнить данную рекомендацию отсутствует, то при первой же возможности измените

пароль, войдя в систему Интернет-банк ХМБ-онлайн с личного компьютера;

- При совершении операции в Интернет-банк ХМБ-онлайн, требующей подтверждения Одноразовым паролем, обязательно сверяйте текст СМС-сообщений, содержащий пароль, с деталями выполняемой Вами операции. Если в СМС-сообщении указан пароль для платежа, который Вы не совершали или Вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по Вашему счету платеж, ни в коем случае не вводите его в Интернет-банке ХМБ-онлайн и не называйте его, в том числе сотрудникам Банка;
- Будьте внимательны. В случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа к Интернет-банку ХМБ-онлайн;
- Мобильную версию Интернет-банк ХМБ-онлайн устанавливайте только из авторизованных интернет-магазинов App Store и Google Play. Перед установкой убедитесь, что разработчиком является ООО «Хакасский муниципальный банк». Используйте при установке антивирусное программное обеспечение в случае, если оно доступно для Вашего телефона/смартфона;
- Не забывайте корректно завершать работу в системе Интернет-банк ХМБ-онлайн – используйте всегда для этого пункт меню «Выйти»;
- В системе Интернет-банк ХМБ-онлайн установлен Таймаут. Данное ограничение означает, что если пользователь не совершает никаких действий в системе, например, переходы между разделами системы, поиск/добавление/изменение данных и т.п. действия, то через установленное Банком время работа в системе будет автоматически завершена. При этом для продолжения работы в системе Интернет-банк ХМБ-онлайн пользователю необходимо выполнить повторный вход.

Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах:

- Установите на своем компьютере и регулярно обновляйте программное обеспечение, защищающее компьютер от вирусов, сетевых атак, установки вредоносных программ и кражи персональной информации;
- Не рекомендуется загружать и устанавливать на телефонный аппарат программное обеспечение, полученное из подозрительного источника (интернет-сайты, ссылки в СМС и ММС-сообщениях и т.д.);
- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора;
- При работе в сети Интернет не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.