Памятка по информационной безопасности
в системе Дистанционного банковского обслуживания ПАО «Бест Эффортс Банк»

В связи с участившимися попытками злоумышленников получения доступа к системам Дистанционного банковского обслуживания (ДБО) и проведения несанкционированных финансовых операций, Банк считает необходимым соблюдать приведенные ниже рекомендации по информационной безопасности в системе ДБО:

- Храните ключи только на съемном носителе (eToken или USB-флеш-носителе). Хранение ключевых носителей должно быть организовано в месте, недоступном для посторонних лиц. Установка ключевых носителей на АРМ допускается только непосредственно на время работы с системой ДБО; после окончания сеанса работы в ДБО ключи должны быть извлечены.

- Для контроля доступа к ключевому носителю eToken установлен (пин-код) пароль на ключевой носитель. Не сообщайте никому пароль для доступа к ключевому носителю, включая сотрудников Банка и сотрудников Вашей организации или Ваших родственников.

- Категорически не рекомендуется работать с системой ДБО с не доверенных компьютеров (интернет-кафе и т.п.), так как это существенно увеличивает риск кражи Ваших учетных и ключевых данных.

- После окончания работы в системе ДБО обязательно корректно завершите работу (выйдите из системы ДБО с использованием кнопки «Выход») и/или закройте приложение Internet explorer. Извлеките из компьютера съемный ключевой носитель.

- Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на Вашем компьютере. Действие вирусов может быть направлено на перехват Вашей ключевой и/или парольной информации и передаче её третьим лицам.

- Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере. Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Дополнительно можно настроить брандмауэр на доступ только по адресам системы ДБО.

- Используйте на АРМ только лицензионное программное обеспечение с обновлениями. Регулярно выполняйте обновления (патчи) операционной системы и браузера MS Internet Explorer. Это значительно повысит уровень безопасности Вашего компьютера.

- На АРМ не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в системе ДБО.

- Права пользователя, работающего с системой ДБО, на данном компьютере должны быть минимально необходимыми (наличие администраторских прав нежелательно).

- В случае , появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО Банка, обратитесь в службу поддержки Банка, отложив при этом совершение операций.

- В случае сбоев в работе компьютера или его поломки во время работы с системой ДБО или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует НЕМЕДЛЕННО обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.

- Обращайте внимание на любые изменения в привычном для Вас процессе установления соединения с системой ДБО или в функционировании системы. При возникновении любых сомнений в правильности функционирования системы ДБО незамедлительно обратитесь в Банк.

- Разглашение пароля Системы «Клиент-Банк» запрещается (Если к Вам обратятся лица, представившиеся работниками Банка, и запросят пароль, помните, что работники Банка никогда не запрашивают такую информацию). В случае возникновения подозрений компрометации пароля, его необходимо изменить.

- При наличии подозрений на несанкционированный доступ к Вашим счетам через систему ДБО незамедлительно проинформируйте об этом Банк и заблокируйте технические средства, используемые в системе ДБО. При подтверждении факта несанкционированного доступа необходимо предоставить в Банк подробное письменное описание обстоятельств компрометации ключевой информации или факта несанкционированного доступа к системе ДБО.

Неукоснительное соблюдение приведенных рекомендаций сведет к минимуму риски хищения злоумышленниками Ваших денежных средств!