Памятка Клиенту по мерам безопасности при работе с системой «Мобильный банк» ОАО «Россельхозбанк»

Уважаемые Клиенты,
пользователи системы «Мобильный банк» ОАО «Россельхозбанк»

Обращаем Ваше внимание, что за последнее время существенно увеличилось количество мошеннических действий злоумышленников в системах дистанционного банковского обслуживания, включая случаи покушения на хищение денежных средств.

Появилось вредоносное программное обеспечение, действие которого направлено именно на системы дистанционного банковского обслуживания различных банков (хищение/несанкционированное копирование логинов, паролей доступа к системам дистанционного банковского обслуживания и иной конфиденциальной информации).

Технологии защиты операций в системах дистанционного банковского обслуживания ОАО «Россельхозбанк» используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень ее надежности и безопасности.

Вместе с тем эффективность этих механизмов зависит также от соблюдения Вами мер безопасности.

Настоятельно рекомендуем Вам работать в системе «Мобильный банк», соблюдая следующие дополнительные меры безопасности, позволяющие минимизировать риски мошеннических действий в отношении Вас и Ваших средств, а также руководствоваться *Памяткой держателя платежных карт ОАО «Россельхозбанк»*, размещенной на официальном сайте Банка (http://www.rshb.ru/download-file/20865/instructions.pdf):

1. **ПИН к M-Token и Логин** для входа в систему «Мобильный банк» это Ваша личная **КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ**, ни при каких обстоятельствах не раскрывайте ее кому-либо под каким-либо предлогом.

При первом входе в систему «Мобильный банк» обязательно создайте уникальный ПИН к M-Token, известный только Вам.

2. **НЕ СОХРАНЯЙТЕ и НЕ ХРАНИТЕ** Ваш **ПИН к M-Token в ТЕКСТОВЫХ ФАЙЛАХ** на мобильном устройте, или на других электронных носителях информации, так как это может привести к его хищению и/или компрометации. Не оставляйте записанные на бумаге и т.п. носителях информации Логин и ПИН к M-Token в легкодоступных местах (напр. на рабочем столе), не передавайте эти данные третьим лицам.

3. **ИСПОЛЬЗУЙТЕ** современное **АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** и обеспечьте его регулярное обновление.

4. Регулярно **ВЫПОЛНЯЙТЕ АНТИВИРУСНУЮ ПРОВЕРКУ** на своем мобильном устройстве для своевременного обнаружения и удаления вредоносных программ.

5. Своевременно **ОБНОВЛЯЙТЕ** операционную систему Вашего мобильного устройства в целях устранения выявленных в ней уязвимостей.

6. Не открывайте неизвестные письма и файлы, пришедшие с использованием электронной почты от недоверенных источников, не заходите по ссылкам, полученным в почтовом сообщении, прежде чем не будете уверены в благонадежности источника, даже если там написано что-то, кажущееся важным. Помните, что ссылки достаточно легко подменить даже в письме от благонадежного источника.

7. **НЕ УСТАНАВЛИВАЙТЕ** приложения из недоверенных источников, от неизвестных разработчиков/издателей и т.п. лиц.

8. При вводе логина и ПИН к M-Token **НЕ РАЗМЕЩАЙТЕ** экран мобильного устройства так, чтобы с него существовала возможность визуального считывания информации посторонними лицами.

9. **ПРИ КОМПРОМЕТАЦИИ** ПИН к M-Token необходимо незамедлительно предпринять меры по его **ЗАМЕНЕ**.

10. **КОНТРОЛИРУЙТЕ** состояние счета (путем просмотра выписки).

11. Постарайтесь не подключать мобильное устройство к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.п.).

12. Если в процессе работы Вы столкнулись с тем, что ранее действующий логин и ПИН к M-Token не позволят Вам войти в систему «Мобильный банк», или мобильное устройство, с установленной системой «Мобильный банк» внезапно вышло из строя (нет доступа, невозможно войти в систему, возникли ошибки при загрузке операционной системы и т.п.), незамедлительно сообщите об этом в службу поддержки Банка Банк по телефонам 8 (800)200-6099 (звонок по России бесплатный), +7(495)651-6099 КРУГЛОСУТОЧНО.

13. В случае передачи (списания, утилизации, сдачи в ремонт и т.п.) сторонним лицам мобильного устройства, на котором ранее было установлена система «Мобильный банк», необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести Вам финансовый ущерб.