**УВАЖАЕМЫЕ КЛИЕНТЫ - ПОЛЬЗОВАТЕЛИ МОБИЛЬНОГО БАНКИНГА!**

В банковской сфере в последнее время наблюдается рост числа мошенников, которые, используя различные механизмы (компьютерные вирусы, удаленный доступ и т.д.) и уязвимость мобильных устройств пользователей (отсутствие антивирусных программ, несоблюдение правил использования устройств, хранения паролей и кодов), стремятся получить несанкционированный доступ к управлению счетами юридических лиц с применением систем мобильного банкинга.

Атаки мошенников могут быть подготовлены на самом высоком уровне.

В целях недопущения несанкционированного списания денежных средств, размещенных на ваших банковских счетах, Банк РМП (АО) призывает вас при использовании системы «Мобильный банк для юридических лиц» строго соблюдать следующие **рекомендации по обеспечению информационной безопасности мобильных устройств**:

1. для установки системы «Мобильный банк для юридических лиц» используйте только официальные приложения Банка, доступные в официальных репозиториях производителей мобильных платформ App Store и Google Play. Обязательно убедитесь, что разработчиком приложения указан Банк РМП (АО). Банк никогда не рассылает своим клиентам ссылки и указания на установку приложений иных разработчиков. В случае получения предложений об установке приложений иных разработчиков незамедлительно сообщите об этом в Центральный офис Банка по телефонам:

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (МСК),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (МСК).***

1. минимизируйте число установленных приложений на вашем мобильном устройстве. Используйте только официальные магазины мобильных приложений, контролирующие размещаемые приложения на предмет наличия вредоносного кода. Не устанавливайте на мобильное устройство приложения, полученные от неизвестных вам источников;
2. контролируйте предоставляемые приложениям права на доступ к функциям и информации на мобильном устройстве, не предоставляйте приложениям права доступа не требуемые для их работы (например, для программы просмотра изображений или приложения «Фонарик» доступ к SMS-сообщениям будет избыточным);
3. установите и используйте антивирусное приложение известного производителя средств защиты от вредоносного кода;
4. используйте надежные пароли и PIN-коды, периодически их меняйте, установите PIN-код на SIM-карту. Пароли и PIN-коды не должны содержать даты значимых для вас событий (или их части, например – день и месяц), части номеров сотовых и городских телефонов вас и ваших близких, простых последовательностей цифр (12345, 0001, 0002, 1111, 2222, 0987 и т.п.);
5. никогда и никому (включая сотрудников Банка) не сообщайте ваш пароль и одноразовый пароль;
6. не сохраняйте ваш пароль на компьютере либо на других электронных носителях информации;
7. старайтесь не использовать бесплатные, общедоступные точки доступа и обращайте внимание на результаты проверки сертификата при HTTPS - соединении – есть вероятность перехвата и раскрытия передаваемых данных или взлома вашего мобильного устройства злоумышленниками;
8. отключите для уведомлений на мобильном устройстве показ текста сообщения, чтобы предотвратить возможность ознакомления злоумышленников с кодами подтверждения операций;
9. учетная запись, к которой привязано ваше мобильное устройство, должна контролироваться вами или вашей организацией, чтобы предотвратить возможность прямого или косвенного удаленного доступа к вашему устройству;
10. в случае утери мобильного устройства (или SIM-карты) с номером, указанным в Заявлении об акцепте оферты «Условия использования электронных средств платежа в системе «iBank2» Банка РМП (АО)» (данный номер используется для отправки Банком SMS-сообщений о совершении операций по вашим счетам), незамедлительно сообщите об этом оператору сотовой связи для блокировки SIM-карты. Затем незамедлительно сообщите об инциденте в Центральный офис Банка по телефонам:

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (МСК),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (МСК).***

Для проведения Банком удаленной идентификации вам потребуется назвать кодовое слово, которое вы указали в Заявлении об акцепте оферты;

1. внимательно проверяйте текст SMS-сообщения, которое содержит не только одноразовый пароль, но и краткую информацию о совершаемой операции. Никогда не подтверждайте операцию одноразовым паролем, если информация в SMS-сообщении не соответствует операции, которую вы хотите подтвердить.

**Руководство Банка РМП (АО)**