ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

Уважаемые Клиенты!

Для минимизации риска несанкционированного доступа к Счетам Клиента со стороны злоумышленников и минимизации риска компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:

- Использовать парольную защиту на мобильном устройстве, производить периодическую смену паролей. Пароли для доступа к мобильному устройству и для доступа к Системе Eurolink не должны совпадать.
- Установить автоматическую блокировку устройства по периоду неактивности.
- Не передавать мобильное устройство с запущенным приложением Системы Eurolink в третьи руки.
- Не сообщать пароли от мобильного устройства и Системы Eurolink третьим лицам.
- Использовать последнюю версию iOS, доступную для мобильного устройства. Устанавливать обновления безопасности iOS только с сайта производителя.
- Крайне не рекомендуется использование Системы Eurolink на мобильных устройствах подвергшихся взлому (т.н. джейлбрейк).
- При резервном копировании мобильного устройства обязательно шифровать резервные копии устройства.
- Не работать в Системе Eurolink при подключении мобильного устройства через открытые Wi-Fi сети в общественных местах (в кафе, аэропорту и т.п.) без защиты трафика шифрованием (должны быть сети с защитой WPA/WPA2 минимум).
- В случае выявления Клиентом подозрительных операций в Системе Eurolink незамедлительно сообщать об этом в Банк.
- В случае утери Клиентом мобильного устройства незамедлительно сообщать об этом в Банк.
- В случае продажи или передачи мобильного устройства третьим лицам обязательно удалите приложение Системы Eurolink и произведите сброс устройства к заводским настройкам (т.н. хард ресет).