Меры предосторожности при использовании мобильного приложения «ОТПбизнес»

Несмотря на то, что операционные системы мобильных устройств и приложения имеют различные инструменты для защиты персональных данных и денежных средств, ключевая роль в обеспечении безопасной работы принадлежит пользователю. Следуя приведенным ниже рекомендациям, вы максимально обезопасите себя от действий злоумышленников и вредоносного ПО:

- Установите и регулярно обновляйте специальное антивирусное ПО для мобильных устройств.
- На устройствах, используемых для работы с приложением, не рекомендуется выполнять процедуры получения доступа к файловой системе устройства (**Jailbreak, Rooting**). Такие операции наносят существенный ущерб системе безопасности, предоставленной производителем устройства.
- В целях безопасности банк может запретить доступ к приложению с устройств, на которых была осуществлена процедура получения доступа к файловой системе
- Скачивайте и устанавливайте приложение "**ОТПбизнес**" только из официальных магазинов приложений **Google Play, AppStore**. Помните - издатель приложения должен быть указан как **OTP Bank Russia**.
- Не записывайте и не сохраняйте свой код доступа к приложению на устройстве, с которого осуществляется работа в приложении.
- Используйте безопасную авторизацию для входа в приложение по отпечатку пальца (при наличии на Вашем устройстве).
- Не сообщайте код доступа третьим лицам, в том числе сотрудникам банка.
- Не переходите по ссылкам и не открывайте вложения из писем от подозрительных или неизвестных отправителей.

- После завершения работы с документами и банковскими счетами каждый раз выполняйте выход из приложения (**Меню → Выход**).
- При подозрении, что ваш код доступа к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых вы не совершали, немедленно обратитесь в Банк и заблокируйте свою учетную запись.
- Принимайте все возможные меры для предотвращения компрометации (несанкционированного использования) мобильного устройства и SIM-карты.
- Храните в тайне аутентификационную информацию и обеспечивайте сохранность мобильного устройства и SIM-карты, с помощью которых осуществляется доступ к приложению.