# СОВЕТЫ ПО БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ/ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ

- ✓ *Проходите регистрацию **в Мобильном приложении/Платежном приложении** только через личное мобильное устройство.*
- ✓ *Не храните конфиденциальную информацию, такую как номера Вашей дебетной/кредитной **карточки**, код CVC/CVV2/CVP2 или **ПИН**-код, на **своем мобильном устройстве (смартфоне/планшете и т.д.)**.*
- ✓ *Не скачивайте мобильные приложения из неизвестных источников. Используйте официальные магазины приложений (Apple Store, Google Play, через официальный сайт Банка).*
- ✓ *Установите на мобильное устройство эффективное антивирусное программное обеспечение и регулярно обновляйте его.*
- ✓ *Своевременно устанавливайте официальные обновления операционных систем **мобильных устройств**.*
- ✓ *Обращайте внимание на разрешения при установке **нового приложения**. Если разрешения вызывают подозрения или не соответствуют функционалу программы, лучше отказаться от **ее** использования.*
- ✓ *При потери доступа к своему **мобильному устройству**, на которое Банк отправляет Вам SMS-сообщения с подтверждающим одноразовым паролем, следует незамедлительно обратиться к своему оператору мобильной связи для блокировки мобильного **телефона**, а также в **Контакт Центр** Банка.*
- ✓ *Вы можете повысить уровень безопасности, устанавливая лимиты на свои карточные операции и пользуясь **услугой «SMS-сообщения»/ «Push-уведомления»**.*
- ✓ *В случае потери/смены номера телефона обязательно сообщите об этом в **Контакт центр** или отделение Банка (5030 или 8-8000-80-60-60).*
- ✓ *При замене **мобильного устройства** обязательно удалите мобильное приложение Банка со старого устройства, а также платежные **карточки**, привязанные **в** платежных приложениях **(Apple** Pay/Samsung Pay/Google Pay/Mir Pay**)**.*
- ✓ *Не снимайте ограничения, установленные производителем мобильного устройств**а**, путем выполнения операций rooting или jailbreak. Это значительно снижает эффективность заложенных производителем функций безопасности, в результате чего Ваше мобильное устройство **становится уязвимым к** заражению вирусным программным обеспечением.*
- ✓ *Всегда завершайте работу **Мобильном приложении/Платежного приложения** после совершения операций (блокируя **мобильное устройство)** либо выходите из аккаунтов).*
- ✓ *Установите парольную защиту на доступ к **м**обильному устройству, данная возможность доступна для любых мобильных **устройств**.*
- ✓ *Не используйте простые комбинации паролей, например, 0000, 7777, 1234 и т.д.*
- ✓ *Старайтесь не использовать общественные не надежные сети Wi-Fi (например в кафе, торговых центрах и т.д.).*
- ✓ *Не устанавливайте приложения удаленного доступа на мобильные устройства (**нап**ример, anydesk, radmin и т.д.).*
- ✓ *Никогда не сообщайте **«SMS-сообщения»/ «Push-уведомления»** полученные от банка **третьим** лицам (**работники Банка** не запрашивают такие данные).*