Памятка о мерах по обеспечению информационной безопасности

Уважаемый Клиент!

Напоминаем Вам о необходимости соблюдать принципы обеспечения информационной безопасности с целью защиты информации от воздействия вредоносного кода и исключения случаев несанкционированного доступа к Вашим счетам в мобильном приложении и торговой платформе STDI. Средства и методы защиты информации, применяемые в АО «ИК Standard» (далее - Компания), позволяют обеспечить необходимый уровень безопасности при условии выполнения клиентами рекомендаций, изложенных в данном документе.

Помните, что при работе со своими счетами в мобильном приложении и торговой платформе STDI следует быть столь же внимательными и бдительными, как при обращении с наличными деньгами!

Рекомендации для безопасной работы с мобильным приложением STDI

1. **Загрузка и установка приложений:**
   - Загружайте и устанавливайте программное обеспечение только из проверенных и надежных источников:
     - Магазин приложений для iOS: [указать ссылку].
     - Магазин приложений для Android: [указать ссылку].
   - Убедитесь, что в авторах приложения указан АО «ИК Standard».
2. **Создание и смена пароля:**
   - Длина пароля должна быть не менее 8-10 символов.
   - Включайте в пароль строчные и заглавные буквы, цифры и специальные символы (% $ @ & * # и т.п.).
   - Не используйте легкие для угадывания пароли (например, даты рождения, имена).
3. **Защита устройства паролем:**
   - Установите пароль, FaceID или PIN-код на доступ к мобильному устройству.
   - Установите PIN-код для доступ к SIM-карте / eSIM.
   - Настройте автоматическую блокировку устройства.
4. **Обновления операционной системы:**
   - Устанавливайте официальные обновления операционной системы, особенно касающиеся безопасности.
5. **Антивирусное ПО:**
   - Установите антивирусное программное обеспечение из официальных источников (Google Play, App Store).
   - Регулярно обновляйте антивирусные базы и проводите проверку устройства.
6. **Разрешения приложений:**
   - Проверяйте разрешения, требуемые приложениями. Если разрешения подозрительны, откажитесь от использования приложения.

7. **Защита устройства:**
   - Не используйте джейлбрейк (Jailbreak) или рутинг (Rooting).
   - Не перепрошивайте устройство прошивками сторонних лиц.
8. **Программы удаленного управления:**
   - Не устанавливайте программы для удаленного управления (Team Viewer, AnyDesk и т.п.).
9. **Использование Wi-Fi и Bluetooth:**
   - Используйте защищенные точки доступа и отключайте Wi-Fi и Bluetooth, когда они не используются. При использовании публично доступных Wi-Fi сетей (аэропорт, кафе, гостиница и тп) Ваши данные могут быть перехвачены злоумышленниками.
10. **Хранение конфиденциальной информации:**
    - Не храните логины и пароли в открытом виде на устройстве (используйте доверенные сервисы хранилищ).
11. **Передача устройства другим лицам:**
    - Не оставляйте ноутбук(laptop)/планшет/мобильное устройство в автомобиле, на столе в кафе либо в гостинице без присмотра.
    - Удаляйте конфиденциальную информацию перед передачей устройства 3 лицам.
12. **Безопасный выход из приложения:**
    - Завершайте сеанс работы с приложением, используя кнопку «Выход».
13. **Защита личных данных:**
    - Никогда никому не передавайте логины, пароли и одноразовые пароли из SMS-сообщений третьим лицам, включая сотрудников Компании.
14. **Утеря устройства:**
    - При утере/краже устройства немедленно обратитесь к оператору связи для блокировки SIM-карты и сообщите об этом в Компанию.
15. **Компрометация данных:**
    - При подозрении на утечку данных немедленно обратитесь в Компанию для их блокировки.

Рекомендации для безопасной работы с торговой платформой STDI на компьютере

1. **Безопасность компьютера:**
   - Используйте лицензионное программное обеспечение.
   - Установите антивирусное ПО и обеспечьте его регулярное обновление.
   - Настройте автоматическую установку обновлений операционной системы и ПО.
   - Минимизируйте состав установленного ПО, оставляя только необходимое.
2. **Программы удаленного управления:**
   - Не устанавливайте программы для удаленного управления и заблокируйте встроенные сервисы удаленного доступа (Team Viewer, Ammyy Admin, AnyDesk, VNC и т.п.).
3. **Пароли и учетные записи:**
   - Установите надежные пароли и регулярно их меняйте.
   - Не работайте под учетными записями с административными правами.
4. **Безопасность BIOS/UEFI:**
   - Настройте загрузку ОС только с основного жесткого диска и установите пароль на вход в BIOS/UEFI.
5. **Использование Интернета:**
   - Исключите использование сторонних Интернет-ресурсов и социальных сетей.
6. **Фишинг и ложные рассылки:**
   - Не переходите по ссылкам и не открывайте вложения в подозрительных письмах.
   - Помните, единственно верный домен нашей копании – это https://stdi.kz и субдомен https://trade.stdi.kz. Если Вам присылают иные ссылки – это фишинговые поддельные страницы.

*Компания владеет всей необходимой информацией и **НИКОГДА** не запрашивает авторизационные данные по телефону, электронной почте или SMS. В случае компрометации данных или обнаружения несанкционированных транзакций незамедлительно обратитесь в Контакт-центр Компании.*

Контакт-центр:

- Горячая линия службы поддержки: +7 (727) 310 01 10
- WhatsApp: +7 (701) 070 13 01
- pr@stdi.kz - для коммерческих предложений и иных вопросов
- client@stdi.kz - по вопросам обслуживания клиентов