



ONLINEBANK
by Halyk

Информационная безопасность



Защита от мошенников



Регулярно проводите обучение сотрудников по вопросам мошенничества с реальными примерами.

Почта

Обучайте сотрудников работе с почтой и необходимой проверке на подлинность адресов отправителей, а также файлов и ссылок из ненадежных источников.

Социальная инженерия

Обучайте сотрудников распознавать признаки социальной инженерии, например, манипуляции по телефону или запросы личных данных.

Личность собеседника

Проверяйте личность собеседника по телефону, особенно при нестандартных запросах (Полиция, Нацбанк и т.п.), и не сообщайте личные данные.

Кибербезопасность



Важные действия

- Разграничивайте доступ к информации внутри организации
- Используйте и регулярно обновляйте только **лицензионное программное обеспечение** и базы антивируса на всех устройствах, с которых вы пользуетесь Onlinebank. Чтобы повысить безопасность, поставьте автообновление на каждые 10 минут
- Не раскрывайте свою личную информацию в социальных сетях
- Для входа в важные бизнес системы используйте **двухфакторную аутентификацию**
- Никому не давайте доступ к вашему компьютеру и рабочему месту, а при уходе, **блокируйте свой компьютер**

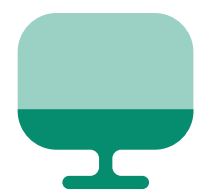


Используйте личные учетные записи и надежные пароли при работе в системах компании

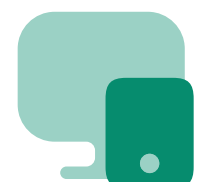
Физическая безопасность



Установите камеры видеонаблюдения в разрешенных законом местах



Установите систему контроля и управления доступов (СКУД)



Ведите записи всех посещений офиса



Храните конфиденциальные документы в запираемой полке/сейфе



Уничтожайте распечатанные конфиденциальные документы через уничтожитель бумаги



Также, чтобы обезопасить Ваш офис, можно разместить его в помещении с охраной

Вирус, в письмах электронной почты

Негативные тренды
в сфере информационной безопасности

Мошенники могут отправлять письма от имени контрагента, банка или государственных органов с информацией о деятельности компании или нарушениях.

Вложение в письме может содержать вирус, который активируется при его открытии.

Он может быть незаметен для антивирусов, собирать и передавать злоумышленникам/мошенникам конфиденциальную информацию, такую как данные о платежах, номерах счетов, пароли и т.д.

Вирус может **изменять суммы платежей и реквизиты получателей** или давать злоумышленникам удаленный доступ к вашему устройству для кражи информации и управлением интернет-банкингом в момент отправки платежа и др.

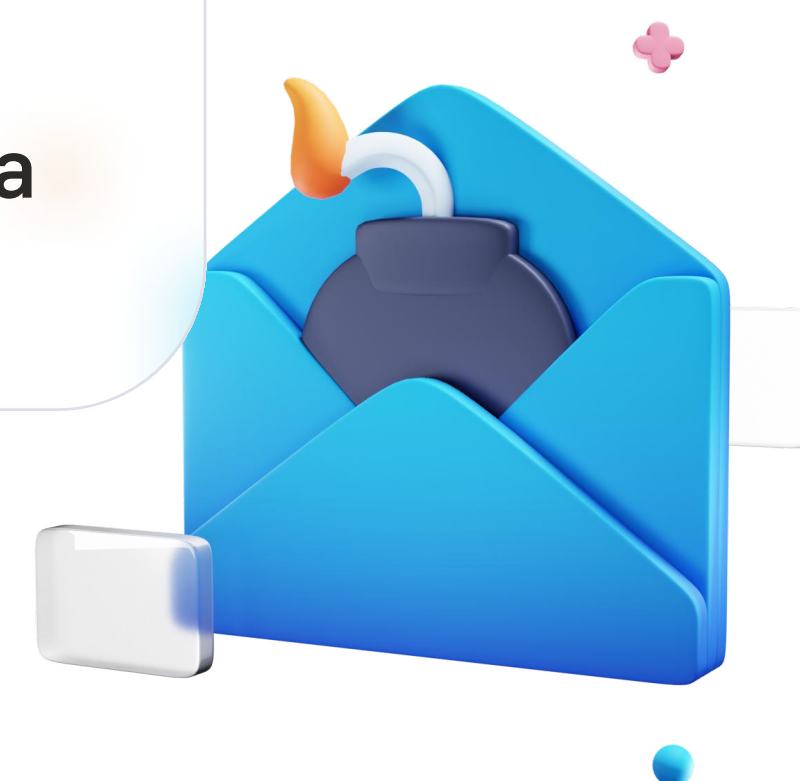


Неблагоденная аутсорсинговая компания

Негативные тренды
в сфере информационной безопасности

Вы наняли компанию, для администрирования и обслуживания компьютеров и систем, которая оказалась ненадежной.

При выполнении своих обязанностей, их представитель подключил свою инфицированную флешку, которая передала вирус на ваш компьютер.



Доступ третьих лиц

Негативные тренды
в сфере информационной безопасности

Сотрудники в вашей компании несерьезно относятся к информационной безопасности и оставляют записки с паролями на своих рабочих местах.

К тому же, клининговая компания имеет доступ в ваш офис, и их персонал может получить пароль от учетной записи сотрудника во время уборки.

Эти данные могут быть проданы злоумышленникам в интернете, которые могут использовать их для кибератак на вашу сеть.

Небрежность в отношении электронной цифровой подписи (ЭЦП), когда руководитель доверяет ее работнику, что позволяет ему подписывать документы от имени руководителя.

Это может привести к незаконным действиям, таким как создание фиктивных сделок и подделка счетов, подписанных ЭЦП руководителя.

Если злоумышленники получают доступ к ЭЦП, вы можете потерять все средства со счетов компании и саму компанию, т.к. они могут переоформлять документы с помощью вашей ЭЦП.

Безопасность при работе с **ONLINEBANK**

Устройства для входа

- Не передавайте третьим лицам
- Не оставляйте подключенным к компьютеру в свое отсутствие

Личная или рабочая почта

- Проверяйте адрес отправителя и остерегайтесь срочных требований
- Не нажимайте на подозрительные ссылки и не открывайте сомнительные файлы

ПО и Антивирус

- Не устанавливайте программы для удаленного управления (TeamViewer, AmmyyAdmin, AnyDesk, RustDesk и др)
- Проверьте, что сайт имеет шифрованное соединение и подлинный сертификат  onlinebank.kz  halyk.onlinebank.kz
- Используйте и регулярно обновляйте только лицензионное программное обеспечение и базы антивируса на всех устройствах, с которых вы пользуетесь Onlinebank. Чтобы повысить безопасность, поставьте автообновление на каждые 10 минут
- Используйте фильтр SmartScreen Windows Defender в браузере Microsoft Edge



Рекомендации по безопасности в **ONLINEBANK**

Контроль операций

- Установите Onlinebank и подключите уведомления о движениях по счету
- Установите несколько уровней подписания (право 1 подписи – Директор и 2 подписи - Гл.Бухгалтер)
- Подключение Дополнительного пользователя возможно в разделе «ЕЩЁ» приложения Onlinebank

Внимательней к партнерам

- При получении новых реквизитов Ваших партнеров рекомендуем созвониться с ними и подтвердить изменение реквизитов



Подозреваете? Звоните!

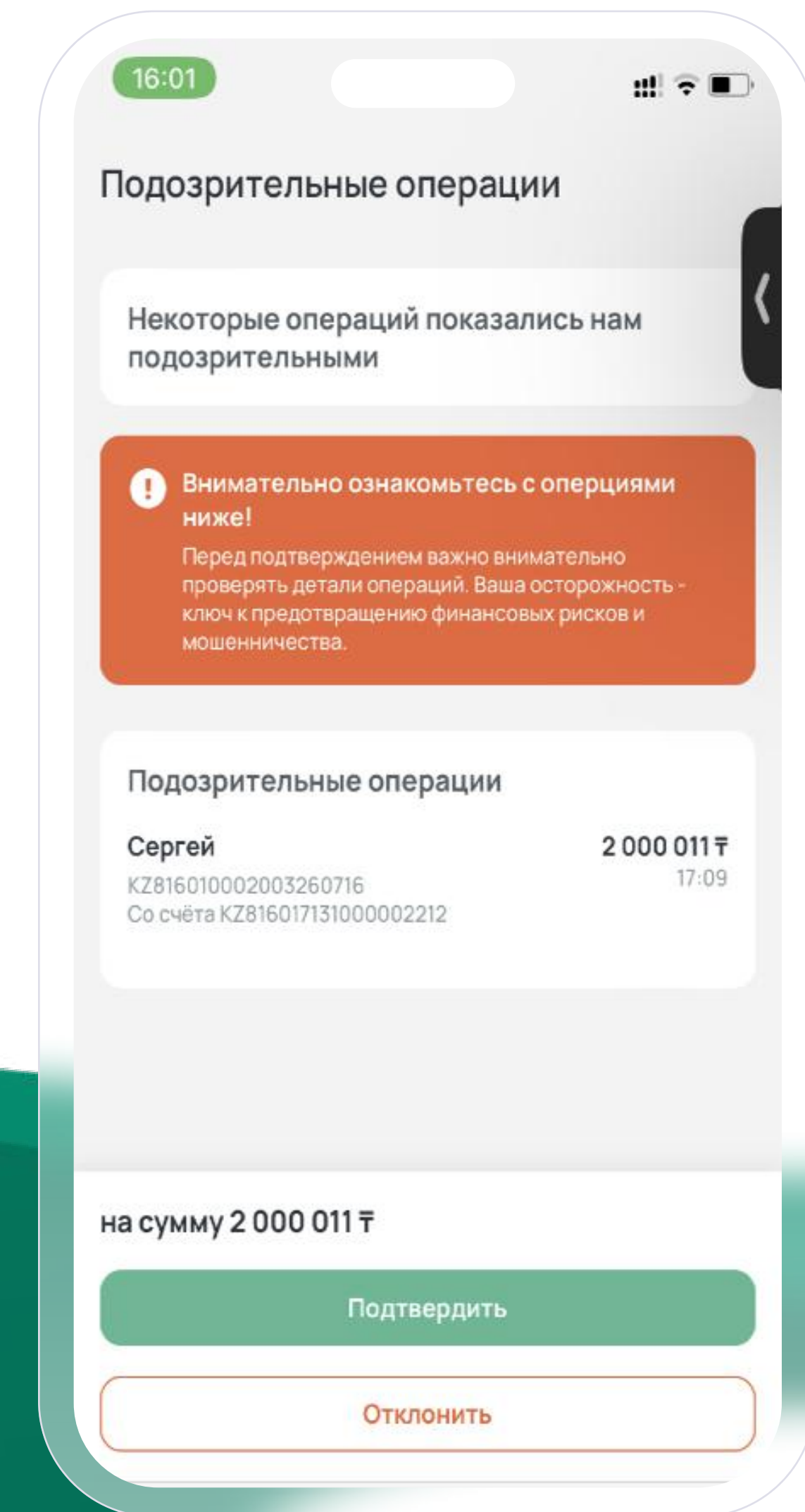
В случае проведения неутвержденных транзакций обращайтесь в Контакт центр Банка

Контакт центр для ЮЛ и ИП

- 9595 (бесплатно с мобильного)
- 8(727)259-07-77 (г. Алматы)
- 8 8000 8000 59 (бесплатно по Казахстану)

Проверка подозрительности

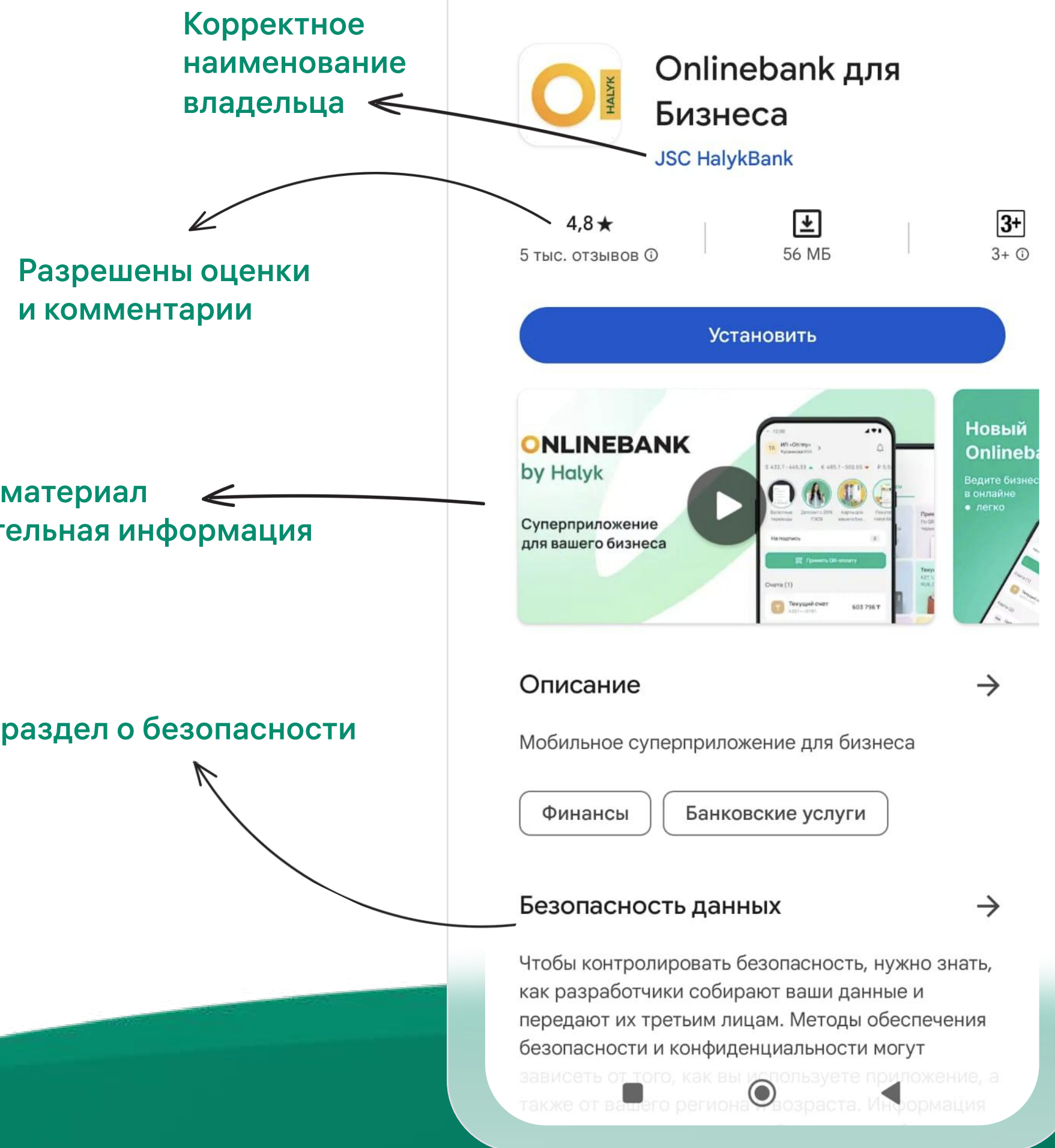
- Halyk проверяет и анализирует все операции на предмет мошенничества с помощью системы фрод-аналитики
- Если возникают подозрения по операциям, для дополнительной проверки Мы можем отправить SMS/Push-уведомление или позвонить вам для подтверждения платежей.
- Если к Вам не пришло SMS/Push-уведомление, установите доверенный номер в отделении Банка
- Время ожидания подтверждения – 30 минут
- Далее с вами созвонится оператор Банка для подтверждения операции



Фэйковые приложения в AppStore и Google Play

- При скачивании приложения Onlinebank, проверьте, что его владелец **JSC Halyk Bank**. Если владелец другой, это мошенники, которые хотят обмануть и украсть деньги
- Не скачивайте приложения по ссылке из SMS или от неизвестных отправителей в мессенджерах
- Смотрите на оценки и рейтинг приложения и возможность оставить комментарий
- Легитимные приложения всегда описывают свои функции в разделе "Безопасность данных". Проверяйте, есть ли этот раздел

✓ Настоящее



! Фэйк

