

# Защита от незаконных финансовых операций

Вы можете обмениваться с нами документами и информацией через:

- личный кабинет;
- мобильную связь;
- электронную почту.

По умолчанию мы полагаем что только вы действуете через вышеуказанные каналы.

Если не хранить в тайне или передать кому-либо свои логин, пароль и разовые уникальные коды, то, например, злоумышленники могут незаконно получить заём на ваше имя.

Чтобы не допустить подобного мы рекомендуем следующее:

## Устройство

- Старайтесь использовать только свои устройства.
- Обновляйте программное обеспечение и приложения ваших устройств.
- На чужих устройствах не сохраняйте персональные данные и другую информацию.
- Не забывайте выходить из своих аккаунтов.

## Пароли

- Не используйте известные пароли (например, qwerty, 123456).
- Не используйте пароли, состоящие только из имен, номеров телефонов и памятных дат (например, IvanovOleg, Petrov01.02.85).
- Не используйте одинаковые логин и пароль для различных систем.
- Не записывайте логины и пароли на бумаге, мониторе, и иных устройствах.
- Не используйте функцию запоминания логина и пароля.
- Периодически меняйте пароли.
- После регистрации на сайтах изменяйте пароли, которые вам приходят на почту.

## Сразу сообщите нам если:

- потеряли или ваше устройство украли;
- обнаружили на своем устройстве подозрительные действия;
- произошла незаконная финансовая операция с использованием ваших данных.

## Антивирус

- Используйте только лицензионные антивирусы;
- Не используйте пиратские версии антивирусов.
- Обновляйте антивирус.
- Старайтесь каждый день проверять устройство на вирусы.

## Подозрительные письма

- Не отвечайте на подозрительные сообщения от банка, госоргана и не звоните по телефонам, указанным в таких сообщениях.
- Не переходите по ссылкам из этих сообщений и не открывайте из них вложения. Во вложениях и ссылках могут быть вирусы.
- Через поисковик браузера найдите официальный сайт организации, от которой вам пришло письмо, и свяжитесь по контактам, указанным на этом сайте.