

Финансовая безопасность

ООО «Земский банк» создал надежные интернет-банк и мобильное приложение. Для их защиты мы используем самые современные технологии, которые соответствуют стандартам, принятым в мировой практике. Однако очень многое зависит и от действий самих держателей карт.

Пожалуйста, обратите внимание на несколько важных правил работы с интернет-банком и мобильным приложением. Их соблюдение поможет вам сохранить ваши деньги в безопасности.

Правила финансовой безопасности

- 1. Никому не сообщайте СМС-коды, CVV-код, а также информацию о банковских продуктах которыми вы пользуетесь: ни сотрудникам банка, ни сотрудникам службы безопасности, ни технической поддержке банка.**

Исключение могут составлять случаи, когда вы самостоятельно звонили в Банк и делали запрос на уточнение условий по своим продуктам.

Кроме того, запоминайте ваши пароли и ПИН-коды и нигде их не записывайте. Если пароль стал доступен кому-то еще, немедленно измените его. Не используйте в качестве паролей номера телефонов, даты рождения, а также последовательность символов, расположенных подряд в раскладке клавиатуры.

Не сообщайте незнакомым людям номер своей банковской карты и не передавайте ее в руки — в том числе официантам и продавцам в магазинах.

- 2. Внимательно читайте тексты СМС-сообщений с кодами подтверждений, проверяйте реквизиты операции.**

При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных сообщений от банка, например, «Ваша карта заблокирована», «Заблокирована сумма оплаты», «Есть проблемы с проведением операции» и т.п.):

- ни в коем случае не перезванивайте на указанные в сообщениях номера,
- не сообщайте данные банковских карт: срок действия, контрольный код с обратной стороны карты, СМС-коды подтверждения, а также персональные сведения: серия и номер паспорта, адрес регистрации и пр.

В такой ситуации следует считать, что звонки или сообщения приходят от мошенников. Вам нужно прекратить контакт и самостоятельно обратиться в банк по телефонам, содержащимся на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах.

- 3. Не переходите по ссылкам на незнакомые ресурсы: мошенники могут заразить ваш компьютер или телефон вирусом и завладеть вашими личными данными.**

Перед вводом логина и пароля для входа в интернет-банк обращайтесь внимание на адрес сайта. Вход в Интернет-банк осуществляется по адресу

<https://elf.faktura.ru/elf/app/?site=zemskybank>. Убедитесь в том, что адресная строка в браузере при входе в Интернет-банк начинается с <https://>. Не переходите по ссылкам в подозрительных письмах.

ООО «Земский банк» направляет сообщения с адресов, которые заканчиваются@zemsky.ru, а СМС — только с адресов Zemskybank. Помните, что сотрудники Банка никогда не просят сообщить ваши личные данные а также коды и пароли.

4. Используйте только официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store.

Никогда не пользуйтесь другими неофициальными приложениями во избежание передачи личной информации мошенникам.

5. Используйте антивирус.

Владельцам смартфонов настоятельно рекомендуем использовать антивирусное программное обеспечение, которое поможет уменьшить вероятность попадания в устройство вредоносных программ, предназначенных для перехвата входящих от банка СМС-сообщений, кражи персональных данных и карточных авторизационных данных.