**Уважаемые клиенты!**

**АО «Тольяттихимбанк» (далее Банк) сообщает о возможных случаях мошеннических действий третьих лиц, связанных с:**

* рассылкой в адрес клиентов ложных писем/уведомлений/ SMS-сообщений от лица Банка.
* обзвоном клиентов от лица Банка.

**ПАМЯТКА КЛИЕНТАМ О СОБЛЮДЕНИИ БЕЗОПАСНОСТИ ПРИ ПОЛЬЗОВАНИИ ПРОДУКТАМИ И УСЛУГАМИ БАНКА**

Для предотвращения мошеннических действий:

**1. Соблюдайте правила личной цифровой безопасности:**

* Не переходите по подозрительным ссылкам, полученным по электронной почте, в SMS-сообщениях, в мессенджерах или в социальных сетях.
* Связывайтесь с Банком только по официальным телефонам, указанным на оборотной стороне банковской карты или на официальном сайте Банка.
* Сообщите Банку о смене номера мобильного телефона и в случае утраты мобильного устройства, так как ваши данные могут попасть к мошенникам.
* Если Вы подозреваете, что Ваши персональные или банковские данные стали доступны постороннему человеку, то необходимо сразу уведомить Банк об этом и изменить логин, пароль для «Мобильного банка»/«Интернет-банка».
* Не заходите в личный кабинет «Интернет-банка» через общественные интернет подключения WI-FI.
* Не используйте функцию автосохранения паролей в браузере.

**Внимание!** Если для входа в мобильное приложение Банка или личный кабинет на официальном сайте Банка, Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номер мобильного телефона, контрольную информацию по банковским картам или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в системе и срочно обратиться в Банк. Если Вам предлагается ввести пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы в системе и срочно обратиться в Банк.

**2. Никогда не говорите никому и нигде не записывайте:**

* ПИН-код к карте;
* CVV/CVC-код (трехзначный номер на оборотной стороне карты);
* коды подтверждения из СМС-сообщений;
* логин, пароль для входа в «Мобильный банк»/«Интернет-банк».

**3. Полный номер карты работники Банка запрашивать никогда не будут.**

**4. Пользуйтесь защищёнными банкоматами:**

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах: в государственных учреждениях, банках, крупных торговых центрах и т.д.

**5.** Для получения платежа можно предложить **перевести Вам денежные средства по номеру телефона**. Этой информации достаточно для получения платежа или Вы можете отправителю денежных средств озвучить только **16 цифр** на лицевой стороне карты.

**6.** **Не доверяйте карту официантам и продавцам:**

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

**7.** При совершении покупок в интернет-магазинах, участвующих в программе 3-D Secure, для обеспечения дополнительной безопасности держатель карты должен подтвердить операцию специальным 3-D паролем. Этот одноразовый пароль направляется на номер мобильного телефона, который держатель карты ранее указал для получения 3-D паролей при обращении в Банк/ в банкомате/ информационно-платежном терминале Банка.

**8.** При получении от Банка СМС-сообщения с одноразовым паролем внимательно ознакомьтесь с информацией в сообщении: все реквизиты операции в направленном Вам сообщении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом СМС- сообщении корректна, можно вводить пароль.

**Внимание!** Если Вы получили СМС-сообщение от Банка по операции, которую Вы не

совершали, необходимо срочно заблокировать карту обратившись в Контактный центр Банка **+7(8482)71-81-71**.

**9.** Мошенники рассылают массово письма, направляют сообщения или размещают рекламу в социальных сетях, все ссылки в таких сообщениях или рекламах ведут на подменные сайты, которые внешне похожи на настоящие официальные страницы. Будьте бдительны и запомните:

* Обязательно проверяйте написание адреса в командной строке;
* Не вводите данные, если видите предупреждение «Сертификат не является достоверным»/ «Ваше подключение не защищено»;
* Официальные страницы Банка:

<https://www.thbank.ru/>

<https://work.vk.com/thb_tlt>

Обратите внимание, что протокол HTTP небезопасен и заходить на сайты с HTTP нельзя.

**10.** Существуют технологии подмены отображаемого на экране телефона номера ВХОДЯЩЕГО звонка. В случае сомнения, что входящий звонок осуществляется работником Банка, необходимо завершить разговор и перезвонить по официальным телефонам, указанным на оборотной стороне банковской карты или на официальном сайте Банка.

Официальный номер телефона контактного центра АО «Тольяттихимбанк» **+7(8482)71-81-71**
При этом обращаем внимание, что указанный номер предназначен только для приема входящих звонков, рассылка СМС-сообщений с него не осуществляется.

При возникновении сомнений в том, что Вам звонят сотрудники Банка или при возникновении вопросов рекомендуем обратиться за разъяснениями в любое отделение АО «Тольяттихимбанк» или по номеру телефона официального контактного центра Банка **+7(8482)71-81-71.**

**Внимание!** В случае если Вы все же пострадали от мошенничества:

1. Необходимо немедленно обратиться (желательно лично) в Контактный Центр Банка для

блокировки карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции, и следовать рекомендациям специалиста.

2. По факту мошенничества рекомендуется обратиться в правоохранительные органы по

телефонам 02 или 102, а также подать заявление.