Безопасность банковских карточек



*Доля пользователей банковскими карточками стремится к 100 % населения страны, поэтому стать объектом интереса мошенников сегодня может каждый. Злоумышленники придумывают все новые способы списания денежных средств, а помогают им в этом сами потерпевшие, чаще даже этого не осознавая.*

*Мы заботимся о вашей безопасности и предоставляем обобщенную информацию, которая позволит быть бдительными и осознанно действовать в нетипичных ситуациях.*

**ОБЯЗАТЕЛЬНЫЕ ПРАВИЛА:**

1. Никому не сообщайте:
   * паспортные данные
   * данные карточки
   * пароли и коды из SMS
   * PIN-код
2. Никому не передавайте карточку
3. Об утерянной или украденной карте немедленно сообщите в банк либо заблокируйте её Интернет банке или мобильном приложении.

**ЧТО БАНК ПРО ВАС ЗНАЕТ:**

* Ваши ФИО
* паспортные данные
* какие карты у вас оформлены
* сумму денежных средств у вас на карте

**ЧТО БАНКИ НЕ СПРАШИВАЮТ ПО ТЕЛЕФОНУ У КЛИЕНТОВ:**

* полный номер карточки
* срок ее действия
* CVC/CVV (трехзначный код на обороте карточки)
* логин и пароль к интернет-банкингу
* код из SMS-сообщения

***Банк может уточнять эти данные, только в случае если ВЫ сами в него обратились***

**Рассмотрим реальные ситуации и как в них себя правильно вести**

**Пример 1**

Вам поступил звонок, собеседник представился «сотрудником» банка и сообщил:

«С вашей картой происходят подозрительные транзакции»;

«На ваше имя поступила заявка на кредит, нужны ваши данные, чтобы ее отменить»;

«Скажите срочно пароль, иначе банк заблокирует карточку».



**Ваши действия:**Ответить, что вы приедете в банк лично. После разговора вы можете перезвонить в банк, контакты указаны на официальном сайте.

Важно! Злоумышленники активно пользуются IP-телефонией. Это позволяет использовать номера, которые похожи на номера банков, указанных на официальных сайтах. Иногда они и вовсе могут совпадать.

Не перезванивайте на номер, с которого вам поступил звонок.

**Пример 2**

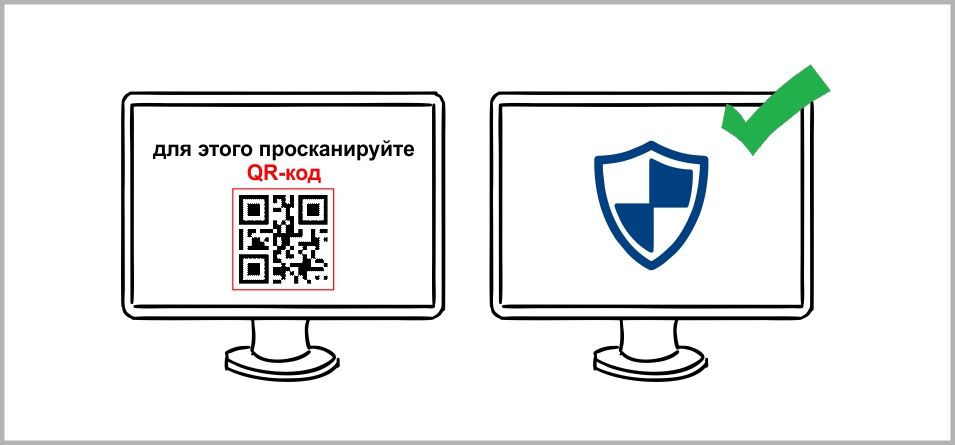
Вы получили письмо на электронную почту от хорошо известной вам компании, с просьбой подтвердить ваш логин и пароль, пройдя по ссылке.



**Ваши действия:**Устанавливайте и регулярно обновляйте антивирусное ПО на Ваших устройствах – компьютерах, планшетах, телефонах. Не переходите по ссылкам на незнакомые ресурсы, не открывайте вложения в подозрительных сообщениях (в социальных сетях, в электронной почте) во избежание заражения Вашего устройства вирусом.

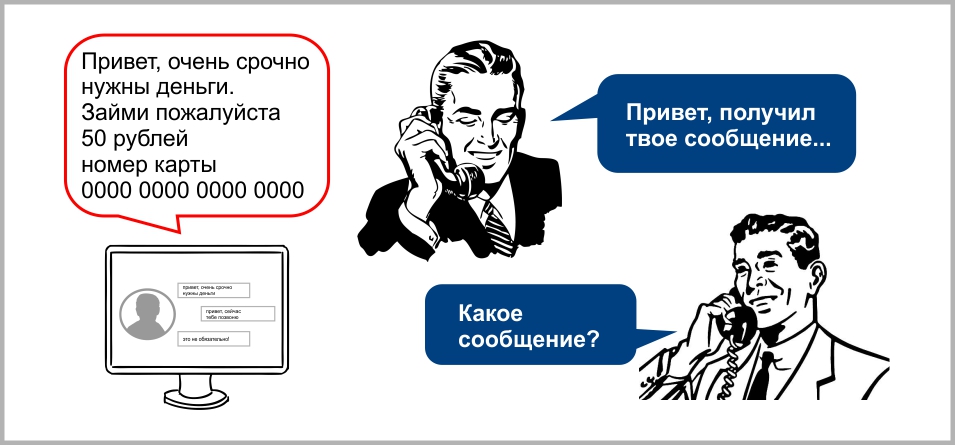
**Пример 3**

Вместо ссылок мошенники теперь отправляют также и QR-коды, которые ведут на поддельные сайты.



**Ваши действия:** Чтобы не рисковать своими деньгами, запомните простое правило: не сканируйте любые QR-коды, которые вам присылают

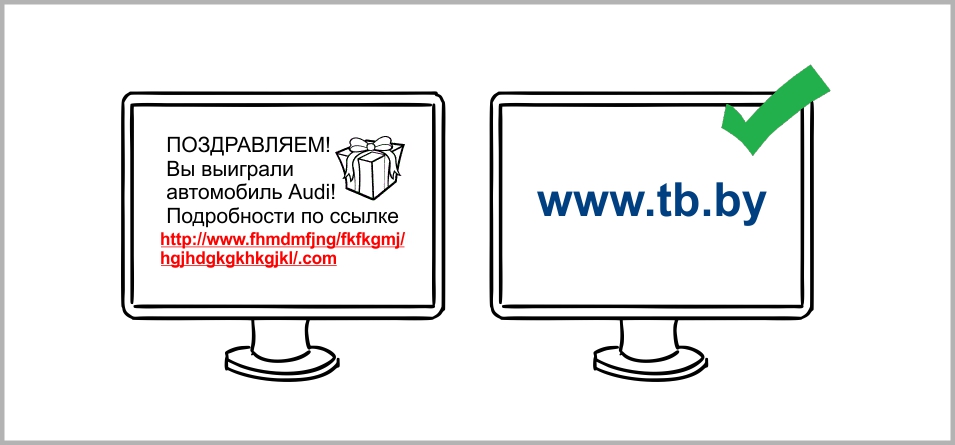
**Пример 4**В социальных сетях вы получили сообщение от имени владельца аккаунта с просьбой занять или перевести некоторую денежную сумму.



**Ваши действия:**Найдите любой способ связаться с владельцем страницы и узнать лично, действительно ли нужна ваша помощь.

**Пример 5**

Вам пришла ссылка с сообщением о том, что вы выиграли приз.

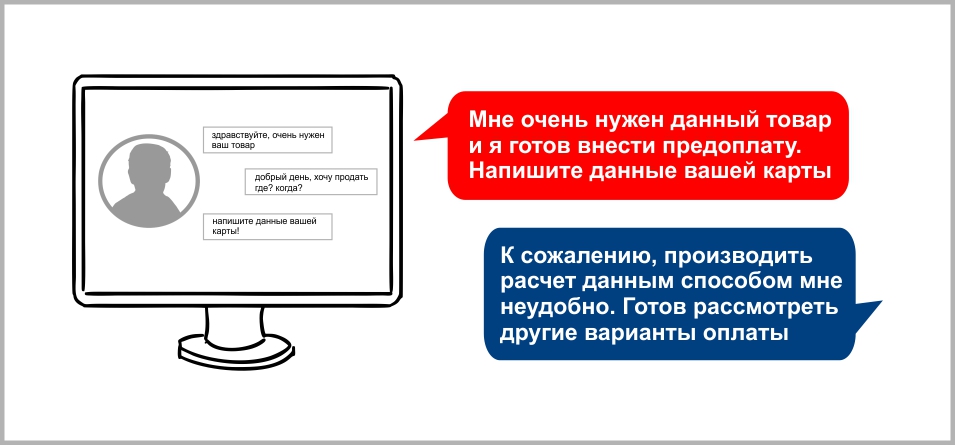


**Ваши действия:**

Прежде чем переходить по ссылке, узнайте, действительно ли был такой розыгрыш. Информация об акциях, конкурсах и розыгрышах публикуется на официальном сайте банка.

**Пример 6**

Вы разместили объявление о продаже вещей, после чего мошенники предлагают произвести вам предоплату путем перевода средств на карточку или электронный кошелек.



**Ваши действия:**

Не следуйте данным просьбам! Никому не сообщайте данные вашей банковской карточки.