



## Какие данные карты нельзя называть

**Если вам должны перевести деньги,  
ни в коем случае не сообщайте:**

- ✗** трёхзначный код на обороте (CVV, CVC)
- ✗** ПИН-код
- ✗** пароли и коды из банковских СМС  
и уведомлений
- ✗** срок действия карты

**Для перевода достаточно указать номер карты,  
расчётного счёта или телефон для СБП.**

# Признаки поддельного сайта

- **В адресе есть ошибки:** название бренда написано неправильно, есть лишние буквы или цифры.
- **На сайте вас просят ввести ПИН-код от карты или СМС-код** — только банки имеют право запрашивать эти данные.



С помощью таких сайтов мошенники могут украсть ваши данные и деньги с карты.

# Правила безопасных онлайн-покупок

**Для интернет-магазинов и автоплатежей (ЖКУ, подписки) заведите отдельные карты —** обычные или виртуальные. Пополняйте их по необходимости на определённую сумму. Если данные с них похитят, основной счёт будет в безопасности.

- ✓ **Включите уведомления обо всех операциях с картой.** Проверяйте историю платежей, чтобы не пропустить подозрительную активность
- ✓ **Не используйте чужие устройства и Wi-Fi-сети** для покупок — из них проще похитить данные
- ✓ **Сохраняйте электронные чеки** — обычно их присылают на почту

# Как защитить сбережения

- **Храните большие суммы на сберегательных счетах и вкладах** — к ним сложнее получить доступ
- **Ограничьте суммы на снятие наличных и покупки в настройках карты** в разделе «Лимиты». Если мошенники получат данные, они не смогут разом списать с карты большую сумму
- **Узнайте, как быстро заблокировать карту**, на случай, если потеряете её или телефон. Сделать это можно в приложении, на горячей линии или лично в отделении банка

