

# СКАЖИТЕ «НЕТ» МОШЕННИКАМ

ТОП уловок и методы  
борьбы с ними



[Подробнее ▶](#)



# ЗВОНОК ИЗ «БАНКА»

## Схема обмана

Звонок с незнакомого номера: «С вашего счета пытаются украсть деньги. Чтобы спасти их, скажите данные карты»



## Как защититься?

Никому не говорите следующую информацию:

- срок действия карты;
- ПИН-код;
- CVC/CVV-код;
- Коды из PUSH и СМС-сообщений

Только мошенники просят такие данные



# «КРИК» О ПОМОЩИ В СОЦСЕТЯХ

## Схема обмана

Сообщение от знакомого: «Помоги, одноклассник сына попал в ДТП. Срочно нужна помощь».  
Далее — душераздирающая история и номер карты



## Как защититься?

Если историю разместил ваш знакомый, дозвонитесь до него и уточните, действительно ли требуется помощь



# «ВОЗВРАТ» ЗА ОТМЕНЕННЫЙ АВИАРЕЙС

## Схема обмана

Представляются сотрудниками авиакомпании и предлагают вернуть деньги за отмененный из-за коронавируса рейс



## Как защититься?

Никому не сообщайте данные своей банковской карты.

Обращайтесь напрямую в авиакомпанию



# ОФОРМЛЕНИЕ «КРЕДИТА»

## Схема обмана

Звонят якобы из банка и говорят, что на вас оформляют кредит. Просят установить приложение и сообщить пароли и коды из СМС, снять деньги из банкомата и перевести их на безопасный счет

## Как защититься?

Если вам звонит «сотрудник банка», положите трубку и перезвоните в банк сами

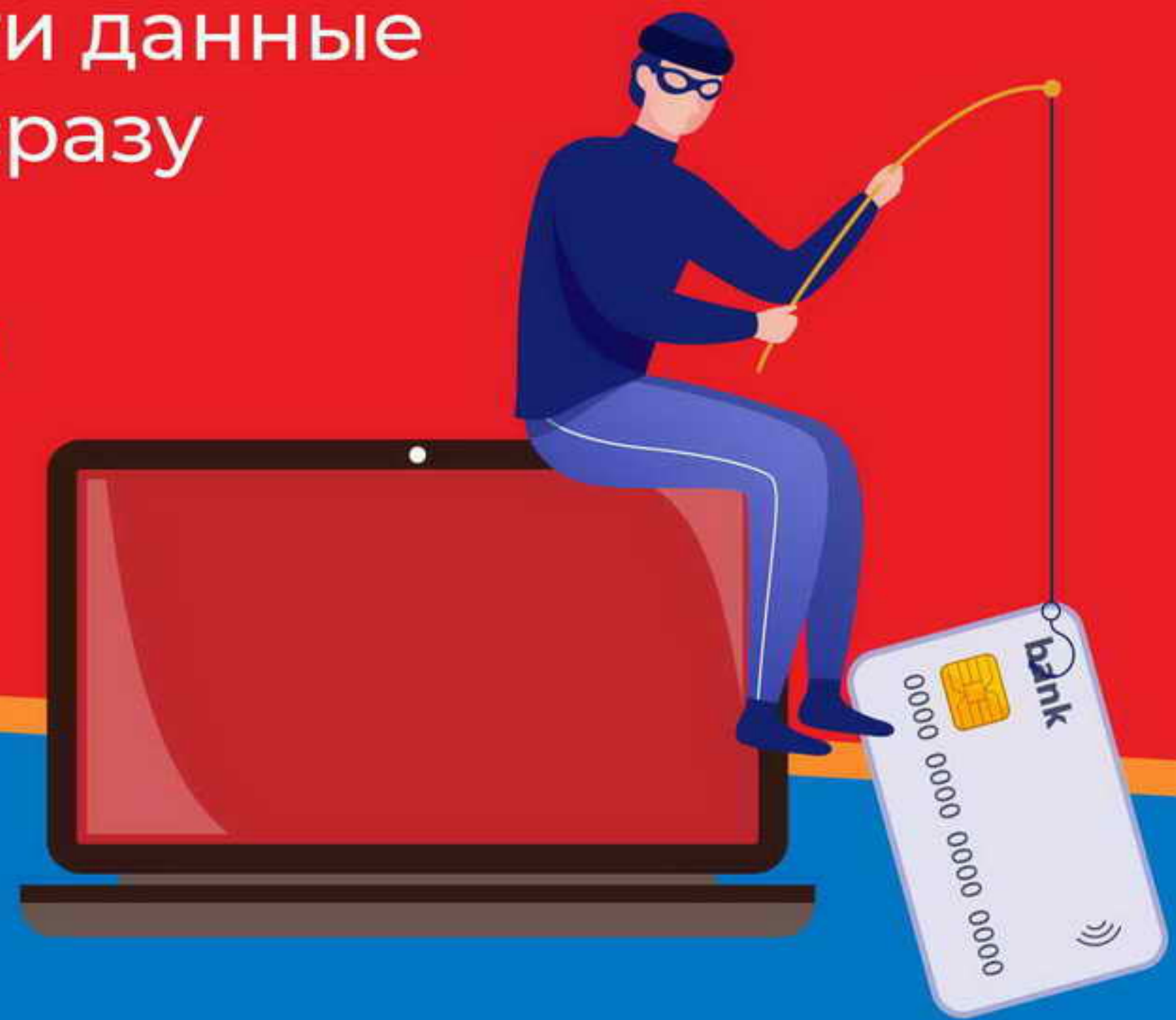




# ФИШИНГОВЫЕ САЙТЫ

## Схема обмана

Мошенники делают поддельные сайты. Для покупки надо ввести данные банковской карты или сразу оплатить с помощью электронного кошелька или прямого перевода



## Как защититься?

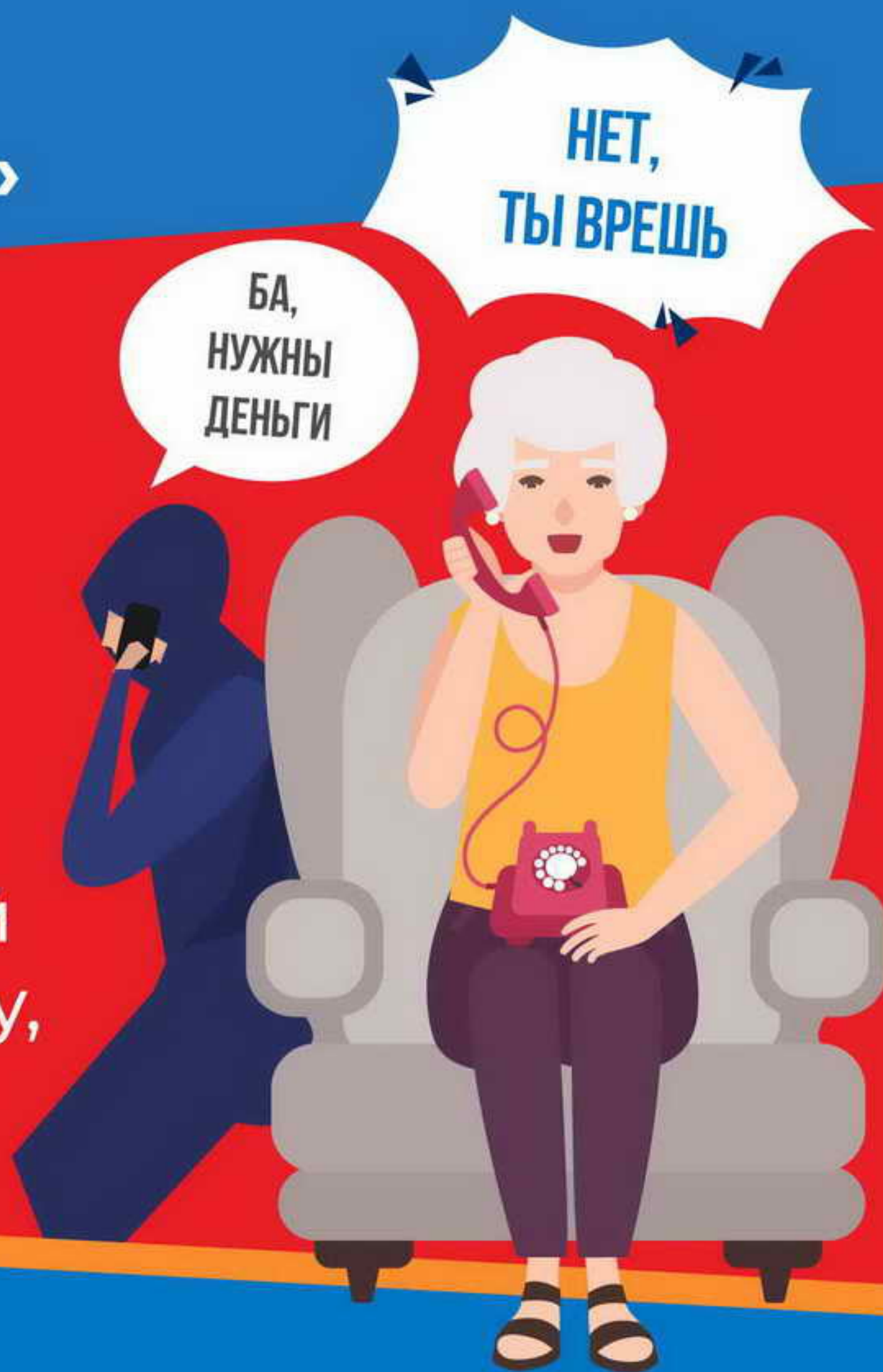
- Проверяйте сайты и адресные строки браузера
- Убедитесь, что все транзакции идут через отдельную безопасную страницу платежной системы
- Используйте антивирус



# ЗВОНКИ ОТ «РОДСТВЕННИКОВ»

## Схема обмана

Мошенники звонят с незнакомого номера и представляются вашим родственником. Просят перевести деньги на чужой счет или передать человеку, который сейчас зайдет



## Как защититься?

Положите трубку, перезвоните родственнику и уточните, нужна ли ему помощь



# ЗАПОМНИТЕ




- **Не сообщайте CVV-код, ПИН-код, коды из СМС и PUSH-уведомлений, а также срок действия карты**
- **Проверяйте, действительно ли людям нужна помощь, когда просят деньги на лечение и т.п.**
- **Сами перезванивайте в банки и другие организации при подозрительных звонках**
- **Используйте антивирус**



# ЗАПОМНИТЕ



- **Не переходите по подозрительным ссылкам**
- **Проверяйте сайты вручную.** Вводите их названия в браузере самостоятельно. Если в адресной строке есть иконка «замочка»  — сайт безопасен
- **Удостоверьтесь, что услуга или товар действительно существуют.** Особенно это важно при покупке билетов
- **Используйте отдельную карту с денежным лимитом для покупок онлайн**



# ЧТО ЭКСПЛУАТИРУЮТ МОШЕННИКИ



- Неожиданность: звонки и сообщения с незнакомых номеров и адресов
- Жадность: подозрительно выгодные предложения
- Слабость: психологическое давление
- Доверчивость: запрос паролей и кодов
- Невнимательность: фальшивые сайты, ссылки и несуществующие услуги

**При любом сомнении — остановитесь,  
скажите «нет»**