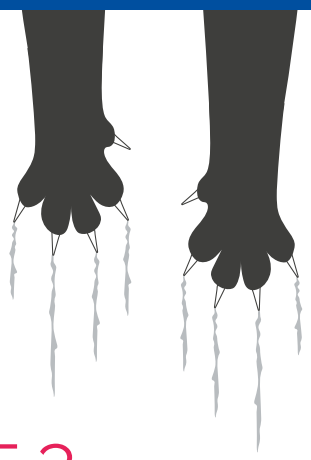
ЧЕК-ЛИСТ БЕЗОПАСНОЙ ОПЛАТЫ ОНЛАЙН

АНАТОМИЯ ФИШИНГОВОГО САЙТА



Простые шаги проверки любого интернет-магазина или сервиса перед тем, как ввести туда данные. Сохраните на телефон или распечатайте.

ШАГ 1

ПРОВЕРЬТЕ АДРЕСНУЮ СТРОКУ

- **Внимательно читайте название сайта.** Мошенники меняют одну-две буквы в известных брендах или просто переставляют слова местами. Например, avito.dostavka.com вместо официального dostavka.avito.com или sberbunk.ru вместо sberbank.ru.
- **Проверяйте доменную зону.** Если официальный сайт всегда был в зоне .ru или .com, а вам прислали ссылку на .xyz, .top или .net-orders, это обман.
- **Замочек не гарантия безопасности.** Наличие значка «замочек» (https://) означает лишь то, что трафик шифруется. Сегодня мошенники легко получают эти значки на свои поддельные сайты.

ШАГ 2

ПРОВЕРЬТЕ ПОЛЕ «СУММА ПЕРЕВОДА»

В поле оплаты должна стоять фиксированная сумма. Настоящие магазины сразу выводят точную сумму вашей покупки, например: «К оплате: 1 450 руб.». Мошеннические формы часто оставляют это поле пустым.



ШАГ 3

ОБРАТИТЕ ВНИМАНИЕ НА ЗАПРОС ДАННЫХ

Посмотрите на поля для ввода. Настоящему банку для списания по карте нужны только ее номер, срок действия и три цифры с оборота (CVV). Если форма просит вас ввести «баланс карты», «ПИН-код» или «девичью фамилию матери», то перед вами мошенник.

На портале ***моифинансы.рф*** *рассказываем все про финансовую грамотность, накопления и страхование*

ШАГ 4

ОТКЛОНЯЙТЕ ПЕРЕВОДЫ НА КАРТЫ ФИЗЛИЦ

Если интернет-магазин просит перевести деньги «по номеру телефона на карту физлица» (типа Мамедов Т. или Иван Петрович П.), то это не магазин, а мошенники. Легальные сервисы используют защищенные шлюзы интернет-эквайринга.