ПСБ

МОШЕННИЧЕСТВО

как защитить деньги на карте

О ЧЕМ ПОГОВОРИМ

01
ОСОБЕННОСТИ И РИСКИ
связанные с платежными услугами

02
ЭЛЕМЕНТЫ БАНКОВСКОЙ КАРТЫ
для безопасности

03
ПРАВИЛА БЕЗОПАСНОСТИ
осуществления платежных операций

04
ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО
способы защиты

05
ИНТЕРНЕТ МОШЕННИЧЕСТВО
способы защиты

06
ИНВЕСТИЦИОННОЕ МОШЕННИЧЕСТВО
новые виды и прочие финансовые «разводы»

07
ЧТО ДЕЛАТЬ
если с карты украли деньги

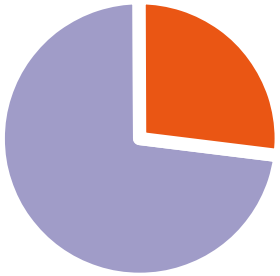
РОСТ МОШЕННИЧЕСТВА В РОССИИ 2021 год

+32%
до 2,5 млрд рублей

Объём мошеннических операций

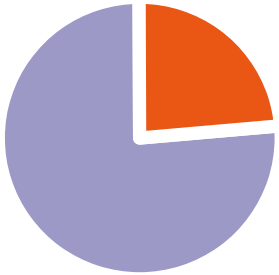
+41%
1,2 млрд рублей

Число мошеннических транзакций через интернет-платежи



+27%
с 17,5 тысячи рублей до 30,3 тысячи рублей

Объём мошеннических переводов с помощью банковских услуг



+13%
с 7,6 тысяч рублей до 8,6 тысяч рублей

Средний чек похищенных средств

КТО СТАНОВИТСЯ ЖЕРТВОЙ МОШЕННИКА

МУЖЧИНЫ
чаще попадаются на удочку мошенников - 57%

ВОЗРАСТ 28- 37 ЛЕТ
это 39% жертв - чем моложе человек, тем больше шансов, что преступники уговорят перевести деньги на чужой счет

С ВЫСШИМ ОБРАЗОВАНИЕМ
люди с 2 высшими образованиями и ученой степенью в 1,5 раза чаще становятся жертвами мошенников

ЖЕНЩИНЫ
их пытаются обмануть на большие суммы (12,7 тысяч рублей против 11,6 тысяч)

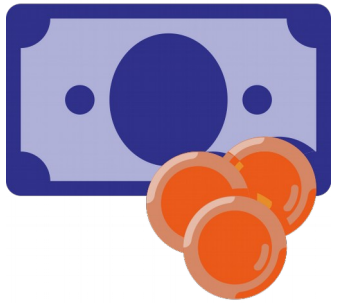
ПОЖИЛЫЕ ЛЮДИ
в 6 раз чаще сообщают посторонним данные своей карты или пароль от СМС

ОДИНОКИЕ ЛЮДИ
семейный люди реже лишаются денег, чем те, кто живут в гражданском браке и одинокие люди

МОШЕННИКИ ХОТЯТ ПОЛУЧИТЬ

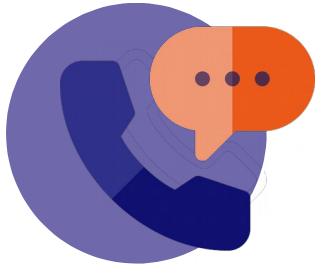
Ваши персональные данные

Конфиденциальную информацию о ваших банковских данных, финансовых операциях



Ваши деньги/ имущество

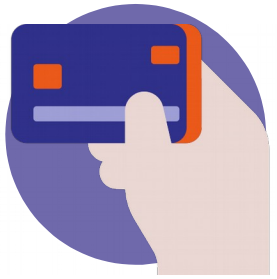
ВИДЫ МОШЕННИЧЕСТВА



Телефонное мошенничество

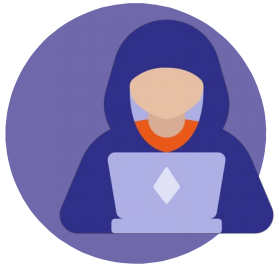
Интернет и мобильный банк

Интернет мошенничество



При совершении операций в банкоматах

Платежные системы

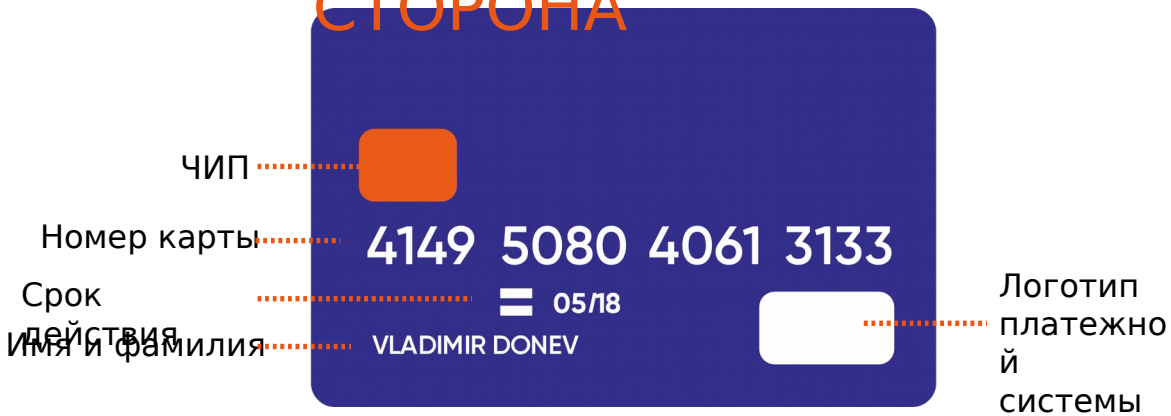


Прочие финансовые «разводы»

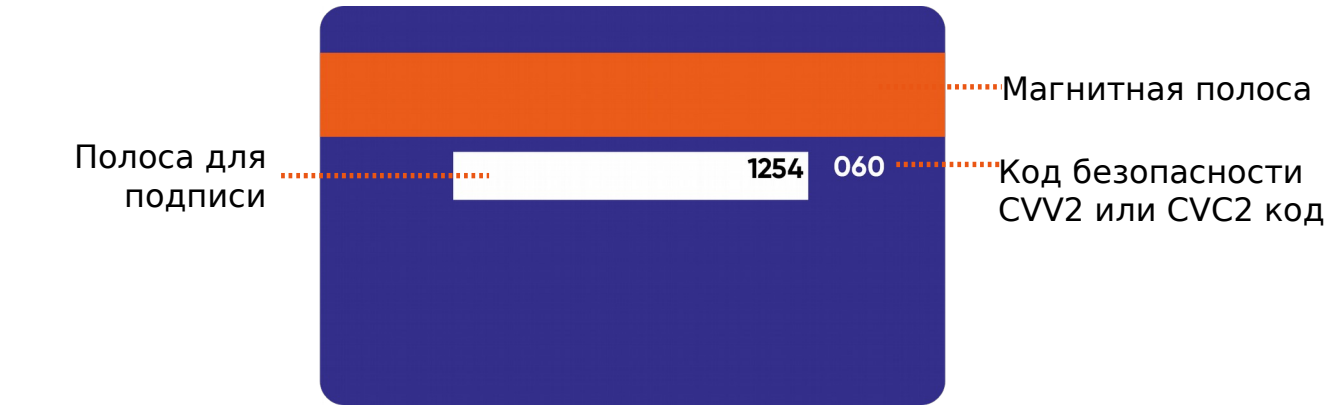
БАНКОВСКАЯ КАРТА

Элементы банковской карты для обеспечения безопасности и секретности.

ЛИЦЕВАЯ СТОРОНА



ОБОРОТНАЯ СТОРОНА



КАК ДЕЙСТВУЮТ МОШЕННИКИ

Крадут реквизиты карт или находят потерянные банковские карты, получая доступ к указанной на них информации: номер, имя владельца, срок действия, CVC-код

Устанавливают на банкоматы незаметные устройства для считывания данных с магнитной полосы карты.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

СОВОКУПНОСТЬ ПСИХОЛОГИЧЕСКИХ И СОЦИОЛОГИЧЕСКИХ ПРИЕМОВ,
методов и технологий, которые позволяют получить конфиденциальную информацию.

ПСИХОЛОГИЧЕСКОЕ МАНИПУЛИРОВАНИЕ
людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

ЗВОНЯТ С КОРОТКИХ НОМЕРОВ

Мошенники представляются сотрудником различных организаций.

«СОТРУДНИКИ БАНКА»

Предлагают Вам перевести деньги на безопасный счет через удаленный доступ.

ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКОМ БАНКА

Мошенники звонят и обманным путем получают Ваши банковские данные.

ВВОДЯТ ВАС В ЗАБЛУЖДЕНИЕ

Мошенники манипулируют безопасностью родных, знакомых, а также играют на Ваших слабостях.

«ЛЖЕСОТРУДНИКИ» ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Информируют о проводимой операции по поимке мошенников.
Для успеха операции просят содействия - делать все, что они говорят. Нередко угрожают

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО
ЗВОНКИ

ЗВОНОК ИЗ «БАНКА»

“Говорит служба поддержки. Наберите на клавиатуре телефона «звездочку», а потом цифры....

ЗВОНОК ПО ОБЪЯВЛЕНИЮ НА АВИТО

“Вы продаете (вещь)?... Я Вам доверяю и готов оплатить ее... Мне нужно привязать Вашу карту к моему счету, продиктуйте пароль, который придет к Вам в СМС...

НЕЗНАКОМЕЦ НА УЛИЦЕ

“Подошел с просьбой позвонить с вашего телефона

ЗВОНОК С НЕЗНАКОМОГО НОМЕРА

“Ошибся, указывая номер телефона, сообщите код,

ТЕЛЕФОННОЕ **МОШЕННИЧЕСТВ**

СМС

СМС С ИНФОРМАЦИЕЙ О ВЫИГРЫШЕ
и предложением направить ответное СМС, позвонить, отписаться от рассылки

СМС СО ССЫЛКОЙ
о которой нужно обязательно перейти

СМС С ИНФОРМАЦИЕЙ
что у вас задолженность по кредиту и просьбой перезвонить по указанному номеру

СМС ОТ ЯКОБЫ ДРУГА/РОДСТВЕННИКА
с просьбой срочно перевести деньги

СМС С КОРОТКОГО НОМЕРА
о зачислении денег и следом с просьбой вернуть деньги

ИНТЕРНЕТ МОШЕННИЧЕСТВО

ПОДДЕЛКА САЙТА
путем незначительного изменения адреса сайта и завлечение пользователей на данный сайт

ПОХИЩЕНИЕ ДАННЫХ
при их передаче оператору-злоумышленнику на поддельном сайте

«ФАЛЬШИВЫЕ» ИНТЕРНЕТ-МАГАЗИНЫ
предоставление некачественного или продажа несуществующего товара, завышение цен на товары

«ВАШ АККАУНТ ЗАБЛОКИРОВАН»
пришлите СМС для получения кода доступа или перейдите по ссылке

ПРОЧИЕ ФИНАНСОВЫЕ «РАЗВОДЫ»

КРИЗИСНЫЕ ЮРИСТЫ

Юридические компании, зарабатывающие на обещаниях и гарантирующие то, что невозможно. Например, забрать их деньги из финансовых пирамид, помочь списать долги перед банками

ФИНАНСОВЫЕ ПИРАМИДЫ

Предлагают вложиться в инвестиционные проекты, криптовалюту, обещают высокий доход за привлечение новых вкладчиков

БИНАРНЫЕ ОПЦИОНЫ

Площадки для инвестирования, участники которых делают ставки на рост или снижение различных котировок: валюта, нефть, золото и др.

РАЗДОЛЖНИТЕЛИ

Предлагают вложиться в свою компанию, чтобы не отдавать долги банкам.
ПРИМЕР: «Древпром»
(признана банкротом в мае 2015 года) предлагала погашение банковских кредитов за комиссию в 20–30% от суммы займа

ЛЖЕБАНКИ

Предлагают людям с испорченной кредитной историей оформить кредиты по ставкам ниже банковских. Чтобы получить деньги, надо внести первоначальный взнос в размере 5-20%

ВИДЫ МОШЕННИЧЕСТВА С БАНКОМАТОМ

СКИММИНГ

Использование различных устройств типа – скиммер. С их помощью мошенники считывают информацию, содержащуюся на магнитной полосе карты. Скиммеры, как правило, прикрепляются к банкоматам, а именно – к принимающему слоту.

ТРАПИНГ

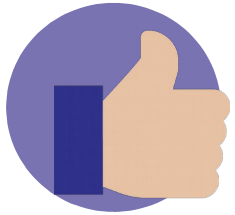
Использование специальных приспособлений для захвата пластиковой карты в банкоматах

БЕЗОПАСНОСТЬ ПРИ ПОЛЬЗОВАНИИ БАНКОВСКОЙ КАРТОЙ

- Для каждой карты создавайте в банкомате отдельный ПИН-код, известный только вам;
- Не записывайте ПИН-код, не храните информацию о нем вместе с картой, никому не сообщайте его;
- Никому не показывайте CVC/CVV-код, расположенный на обороте карты;
- При оплате старайтесь не выпускать карту из рук и тем более – из поля зрения, не позволяйте уносить ее куда-либо;
- Подключите СМС-уведомление от банка: вам будет приходить информация обо всех операциях по карте;
- Запомните телефонный номер вашего банка и храните его не только в телефоне, но и записанным на бумаге – отдельно от карт и денег;
- Используйте банкоматы, расположенные в хорошо охраняемых, просматриваемых местах с постоянным видеонаблюдением, например, в отделениях банков;
- При наборе ПИН-кода прикрывайте клавиатуру рукой;
- Заведите отдельную карту для совершения интернет-платежей или установите лимит на проведение платежей в интернете с картой, часто банки позволяют настроить такую опцию просто и быстро в мобильном приложении;
- В случае потери карты немедленно звоните в банк для ее блокировки.

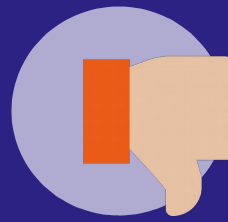
БЕЗОПАСНОСТЬ ПРИ ПОЛЬЗОВАНИИ БАНКОВСКОЙ КАРТО

ПРИ ОНЛАЙН-ПЛАТЕЖАХ



МОЖНО

- ✓ УКАЗЫВАТЬ НОМЕР ТЕЛЕФОНА И ЭЛЕКТРОННУЮ ПОЧТУ
- ✓ СООБЩАТЬ ДРУГИМ ЛИЦАМ НОМЕР ВАШЕЙ КАРТЫ
- ✓ ВВОДИТЬ В ФОРМУ ДЛЯ ОПЛАТЫ ДАННЫЕ КАРТЫ
  номер, срок действия, имя, фамилию, CVV-код на сайтах https://
- ✓ УКАЗЫВАТЬ ПАСПОРТНЫЕ ДАННЫЕ
  при регистрации в платежной системе (типа WebMoney)



НЕЛЬЗЯ

- – СОВЕРШАТЬ ЛЮБЫЕ ОПЕРАЦИИ С ДЕНЬГАМИ
  с чужого компьютера
- – ДЕЛАТЬ ПОКУПКИ НА НЕЗНАКОМЫХ САЙТАХ
- – ДАВАТЬ ДРУГИМ ДАННЫЕ КАРТЫ
  помимо номера карты
- – ИГНОРИРОВАТЬ СОВРЕМЕННЫЕ БРАУЗЕРЫ
  со встроенной защитой и антивирусы
- – СООБЩАТЬ КОМУ-ЛИБО ПИН-КОДЫ ВАШИХ КАРТ

БЕЗОПАСНОСТЬ ПРИ ТЕЛЕФОННОМ МОШЕННИЧЕСТВЕ

НЕ ВОЛНОВАТЬСЯ И НЕ ПОДДАВАТЬСЯ ПАНИКЕ,
связаться с «пострадавшими» родственниками и обратиться в полицию! Ни в коем случае не передавать деньги незнакомым людям!

НЕ ТОРОПИТЬСЯ СООБЩАТЬ РЕКВИЗИТЫ ВАШЕЙ КАРТЫ!
Никто, включая банк, не вправе требовать данные вашей пластиковой карты! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

ОФОРМЛЕНИЕ КРУПНОГО ВЫИГРЫША
никогда не происходит только по телефону или интернету.

ДЛЯ ВОЗВРАТА СРЕДСТВ

БЕЗОПАСНОСТЬ ПРИ ФИНАНСОВЫХ ОПЕРАЦИЯХ

01

ПОДКЛЮЧИТЕ СМС-УВЕДОМЛЕНИЯ

по банковской карте и электронному кошельку и отслеживайте движение и остаток средств

02

СООБЩАЙТЕ В ФИНАНСОВУЮ ОРГАНИЗАЦИЮ

если кошелек «взломан», карта потерялась, данные карты стали известны посторонним или с нее без согласия держателя списаны деньги

03

НЕ ДОПУСКАЙТЕ ПОСТОРОННИХ

к банковской карте, электронному кошельку, мобильному телефону и компьютеру

04

СТАРАЙТЕСЬ НЕ ОТКРЫВАТЬ САЙТЫ

платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке, или посмотрите в свойствах ссылки, куда она ведет

05

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ И РАЗНЫЕ ПАРОЛИ

не сохраняйте их в интернет-сервисах

ЗАЩИТА ОТ ИНТЕРНЕТ-МОШЕННИКОВ

Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами»

это предложения от участников финансовых пирамид. Не верьте таким предложениям, в пирамидах выигрывают только их создатели.

Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас

отправляйте в корзину, не открывая.
Техническая поддержка платежных систем никогда не рассылает таких писем.

В большинстве случаев платежи, которые вы делаете онлайн, отменить нельзя

не торопитесь, подумайте, прежде чем заплатить
за товар или услугу.

БЕЗОПАСНОСТЬ ПРИ ПОЛЬЗОВАНИИ БАНКОМАТАМИ

СМС-ИНФОРМИРОВАНИЕ

Подключите услугу в целях безопасности и контроля за вашими денежными средствами

ПРОЯВЛЯЙТЕ ОСТОРОЖНОСТЬ

При пользовании банкоматом, обращайте внимание на посторонних вокруг
и подозрительные устройства, и накладки
в местах ввода ПИН-кода и карты

«ОТМЕНА»

Перед началом любых операций с банкоматом нажмите несколько раз на кнопку «отмена»

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИЧЕСТВА

ЧТО ДЕЛАТЬ?

- Если мошенники использовали Вашу банковскую карту, заблокируйте ее в мобильном приложении или позвоните в банк по официальному номеру.
- Сообщите о мошенничестве в Ваш банк по телефону, через форму обратной связи на сайте/в мобильном приложении, по электронной почте или обратившись в отделение Банка.
- Оставьте заявление о действиях мошенников по телефону горячей линии МВД России 8-800-222-74-47, через портал https://мвд.рф/request_main или в отделение полиции по месту жительства

КЛЮЧЕВЫЕ ВЫВОДЫ

- Увеличивается количество мошеннических схем с помощью инструментов социальной инженерии
- Мошенники придумывают все новые и новые мошеннические схемы
- Проявляйте бдительность при совершении любых финансовых операций
- Защищайте свои деньги, имущество и персональную информацию
- Делитесь информацией о принципах безопасных финансовых операциях с близкими и коллегами

Готовы ответить на ваши вопросы