Банк России

КИБЕРБЕЗОПАСНОСТЬ КАК НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВЫХ МОШЕННИКОВ*

*Данные в презентации актуальны на 24.01.2023

Цель мошенника – получение информации

Мотивация мошенника – деньги

Используемый инструментарий:

- Социальная инженерия
- Сбор информации из открытых источников
- Поддельные сервисы и сайты
- Вирусы и другое вредоносное ПО

Информация – это деньги

Для управления деньгами используется информация :

- Данные карты *(Номер, срок действия, Ф.И.О. владельца, код подтверждения (CVV2 или CVC2)*
- Логин и пароль от личного кабинета *(онлайн-банк)*
- Кодовое слово *(для обращения в банк по телефону)*
- Код в СМС-сообщении или уведомлении в приложении банка *(как второй фактор аутентификации)*

Социальная инженерия

Звонок «специалиста» – один из самых популярных способов.

Основные принципы:

- «Втереться» в доверие
- Психологическое давление
- Отсутствие времени на принятие взвешенного решения
- Введение в заблуждение
- Целью могут быть не только деньги, но и ваши персональные данные

Мошенники могут представиться:

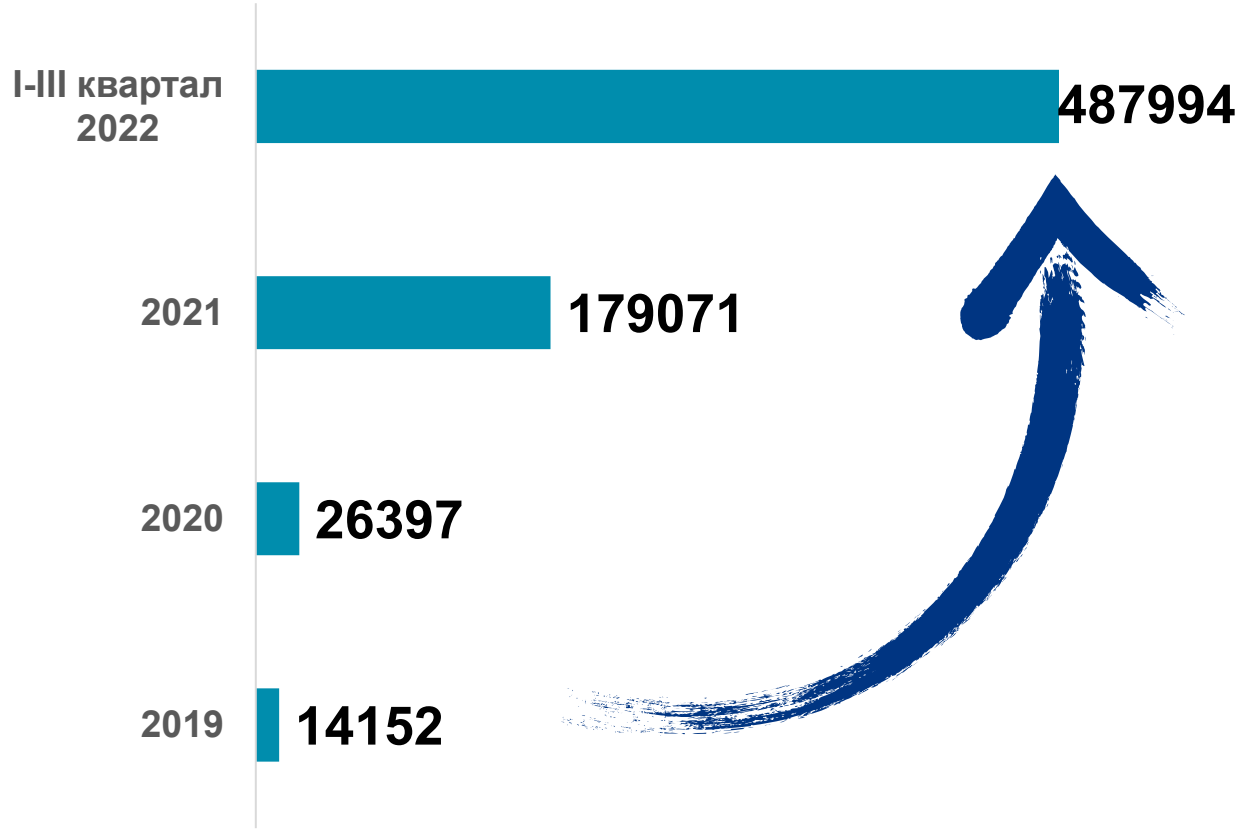
- Специалистами «службы безопасности банка»
- Сотрудниками правоохранительных органов
- Врачами
- Соцработниками

Могут предлагать:

- Уникальное лекарство
- Секретную вакцину
- Несуществующие льготы,

пособия и компенсации, «бронь», диплом IT-специальности

Количество телефонных номеров, направленных операторам связи в целях блокировки



Звонки якобы от представителей банков, правоохранительных органов, Банка России, а также роботизированных помощников

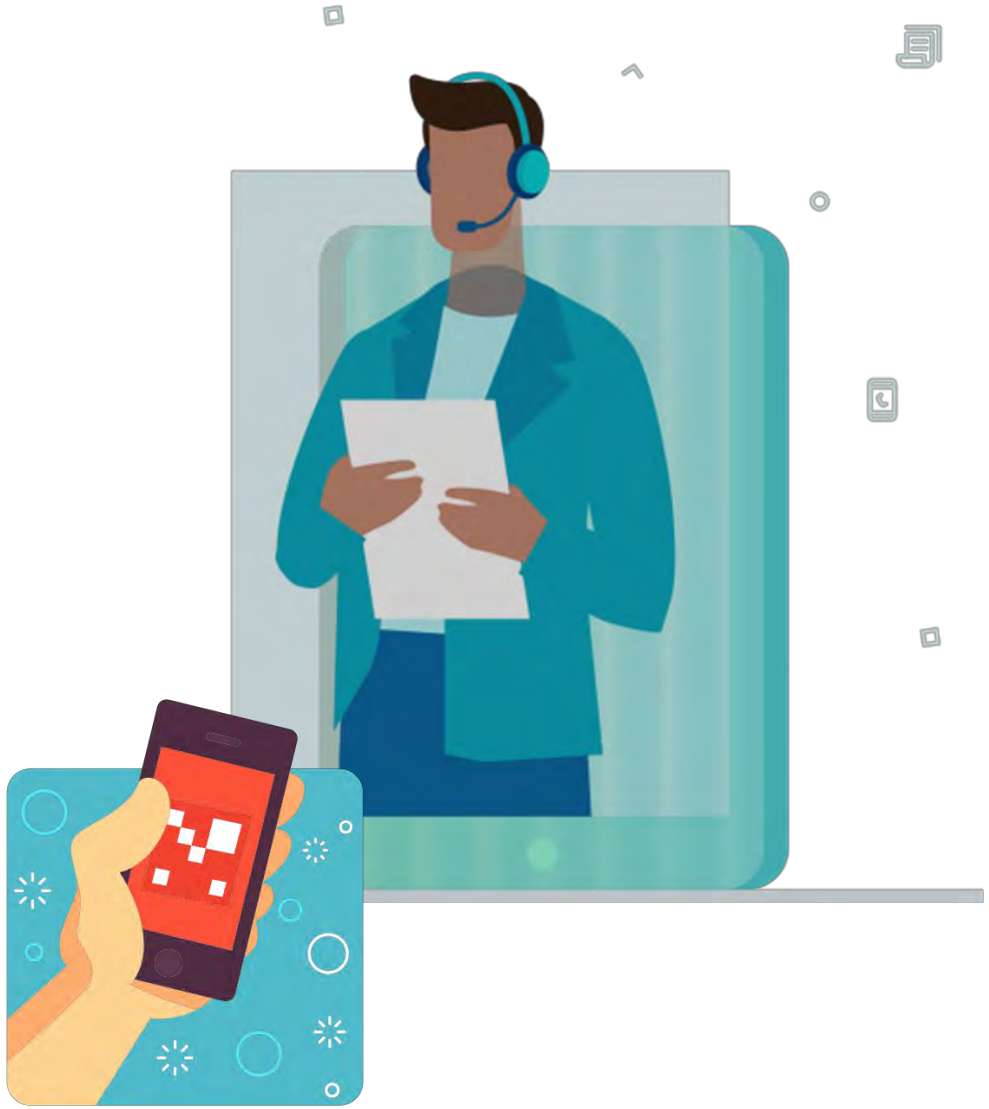
В большинстве звонков используется технология подмены номера

Средний чек хищений (физлица и юрлица)

Социальная инженерия

Помните, что:

- Бесплатный сыр (выплаты) только в мышеловке
- Если вам перевели случайно деньги, они вам не принадлежат, сообщите в банк об ошибке
- Если на вас давят, это повод усомниться в том, что звонят из банка
- Сотрудник банка не будет вам угрожать уголовной ответственностью или блокировкой счета
- Все действительно нужные данные у банка уже есть
- Если вашу операцию действительно заблокировали, у вас есть два дня на ее подтверждение



Как мошенники добывают информацию?

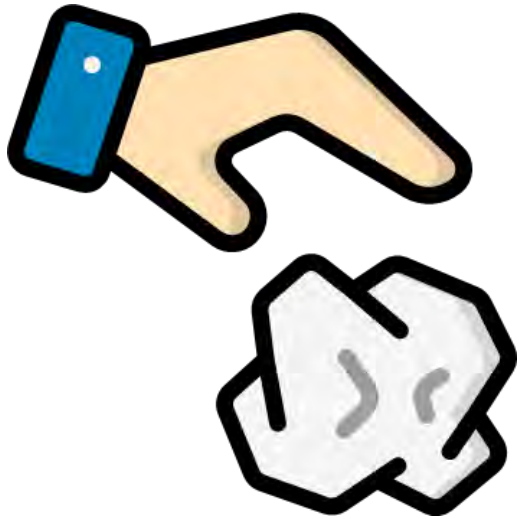
Основные способы:

1) Поиск в социальных сетях фотографий, на которые попали данные карты или другие полезные сведения
2) Установка камер на банкоматы, фальшивые банкоматы
3) Подсмотреть в очереди в магазине
4) Просьба скинуть фото карты
5) Мошенник использует ваши данные напрямую для перевода средств или для «звонка из банка»

Сбор информации

Выбрасывая чеки, накладные, распечатку по заказу или технику:

- Внимательно следите, чтобы в них отсутствовали ваши данные (Ф. И. О., телефон, номер карты)
- Технику лучше уничтожать перед тем, как выбросить
- Помните, что ваши данные могут быть использованы против вас, не доверяйте всем, кто знает, что вы купили прошлым вечером



Разбор кейсов: фразы-триггеры

Выберите фразу, которую вы можете услышать от настоящего сотрудника банка:

1. Чтобы избежать мошеннических действий, необходимо перевести деньги на «защищенный счёт»
2. Вам нужно будет дойти до банкомата и совершить действия, которые вам скажет по телефону наш сотрудник
3. Назовите 4 последние цифры карты, которую вы назвали мошенникам, чтобы заблокировать её
4. Поступила заявка на оформление кредита на ваше имя...
5. Если мы не отменим транзакцию в течение 30 минут, с вашей карты будут списаны деньги...
6. Я вам задам несколько вопросов, чтобы идентифицировать вас, как клиента нашего банка...
7. Через несколько минут с Вами свяжется сотрудник следственного комитета, который проводит расследование дела, в котором вы свидетель.
8. Назовите код из СМС для подтверждения операции.

Правила безопасности

Сотрудники банков не обзванивают людей, чтобы рассказать о проблемах с платежными системами или о мошеннических операциях

ЗАПОМНИТЕ!

Если вам пришло письмо или уведомление якобы от Центрального банка – это мошенники!

Банк России не работает с физическими лицами и никогда не пишет подобных писем. Обратитесь в правоохранительные органы.

Бесплатный wi-fi

Бесплатный wi-fi – всегда «небезопасное соединение»

Не используйте его для совершения финансовых операций!

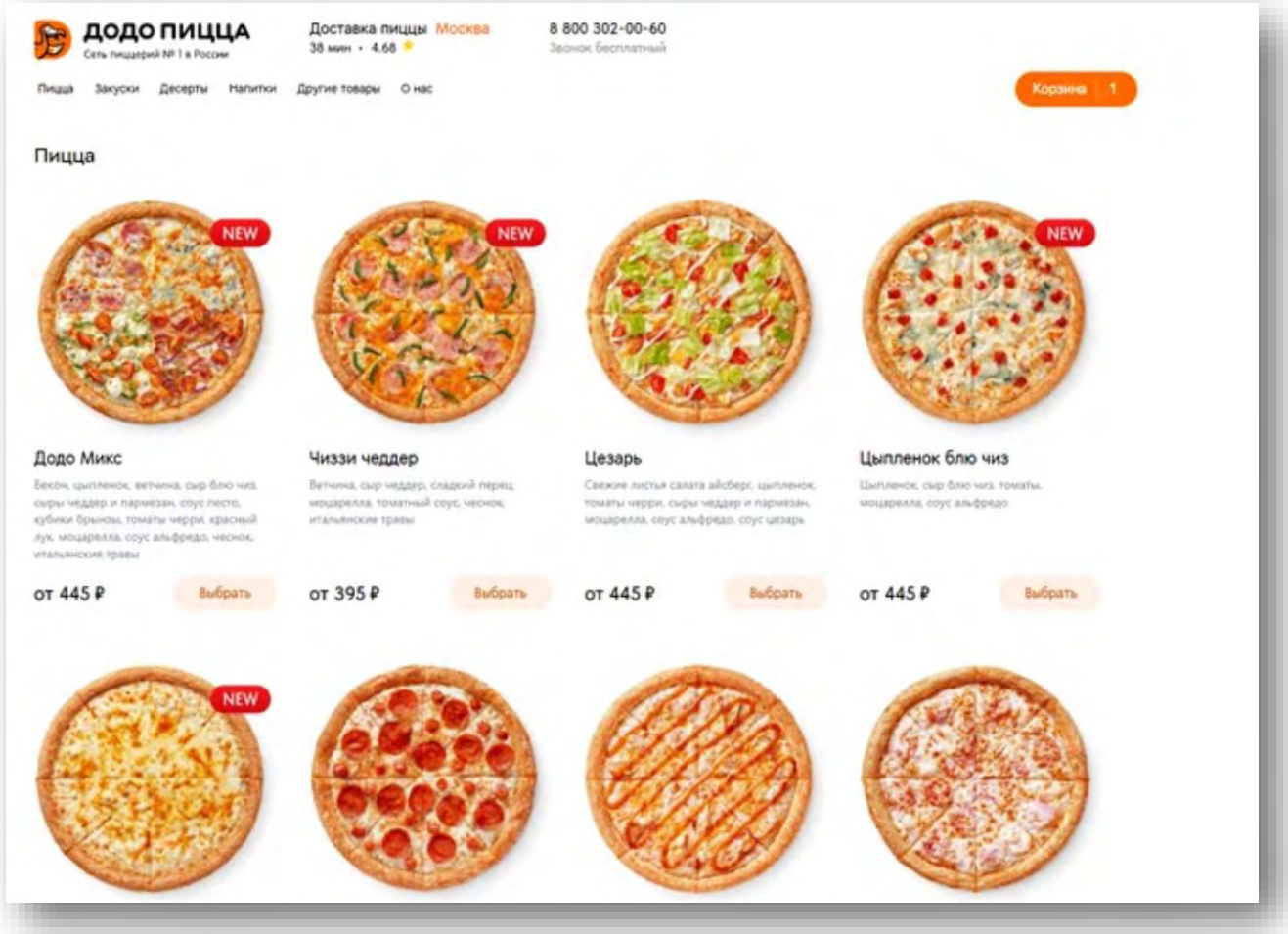
Платите только на защищенных страницах

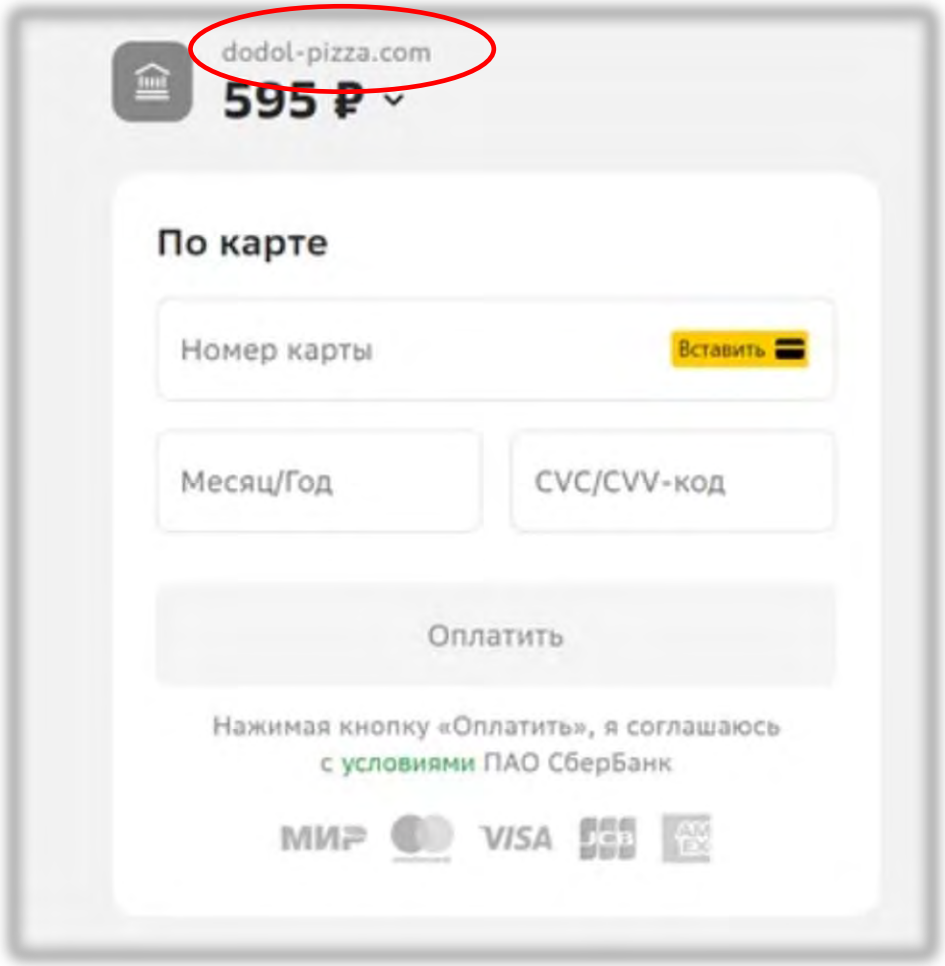
Защищенная страница в адресно-поисковой строке браузера имеет формат **HTTPS** (включает протокол шифрования данных).

Незащищенная страница

Защищенная страница

Пример фишингового сайта

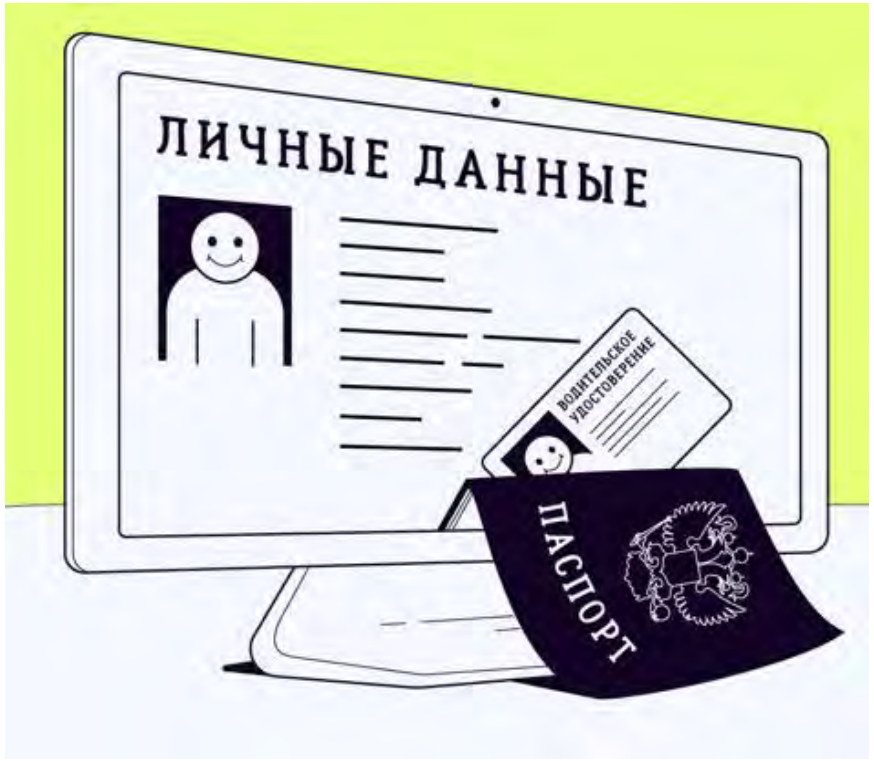




Как себя обезопасить?

У кибермошенников множество легенд и способов обмануть человека, которые всегда сводятся к одному:
у человека пытаются выманить конфиденциальные данные, либо провоцируют самостоятельно перевести деньги

- Не переводите деньги на счет по просьбе неизвестного абонента, кем бы он не представлялся
- Никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС, а еще лучше вообще не переходите на сайты по ссылкам
из подозрительных писем
- Проверяйте информацию
- Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую



Как сделать так, чтобы персональные данные не стали общеизвестными?

- уничтожать личные данные на бумаге
- не разглашать информацию о себе самостоятельно
- ограничить количество личной информации, которой мы делимся с третьими лицами
- «очищать» технику перед передачей третьим лицам.

Если в отношении вас совершены мошеннические действия, необходимо:

- Заблокировать карту
- Сообщить в банк о мошеннической операции

Запросите выписку по счету и напишите заявление о несогласии с операцией

- Обратиться с заявлением в полицию

Обратитесь с заявлением в отдел полиции по месту жительства или отправьте обращение в Управление «К» МВД России

Если банк, микрофинансовая или страховая организация действует некорректно, сообщите об этом в Банк России (по телефону контакт-центра или через интернет-приемную сайта cbr.ru)

Новые инструменты самозащиты для граждан

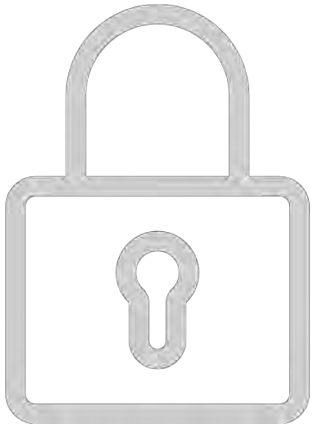
С 1 октября 2022 года граждане могут:

- Устанавливать максимальную сумму перевода по банковской карте или лимит средств на определенный период
- Устанавливать полный запрет онлайн-переводов
- Ограничивать или запрещать оформление онлайн-кредитов

Если у гражданина есть счета в нескольких банках, то написать заявление необходимо в каждом из них

Отменить запрет или изменить параметры онлайн-операций можно будет в любое время

Правила безопасности



- Не экономьте на SMS-уведомлениях о платежах и переводах с вашей карты – это малая цена за спокойствие
- Никому не сообщайте PIN-коды и пароли
- Осторожно обращайтесь с логинами и номерами банковских карт
- Записанные PIN-коды, логины и пароли от ваших личных кабинетов держите в отдельном месте
- Двухфакторная аутентификация — это еще один защитный рубеж между вами и мошенниками
- Банк обязан по вашему требованию незамедлительно заблокировать утраченную карту
- Установите приложение-антиспам

Как связаться с Банком России?

Направить жалобу в Банк России

Ответы на часто задаваемые вопросы

Мобильное приложение «ЦБ онлайн» - можно задать вопрос специалисту в чате

Контакт-центр Банка России

8 800 300-30-00

круглосуточно, бесплатно для звонков с мобильных телефонов

300

Банк России

СПАСИБО
ЗА ВНИМАНИЕ