

Кибермошенничество

Как себя защитить?

Республиканский классный час

21 октября, 10:00



Кибермошенничество

70%

всех преступлений в
сети приходится на
кибермошенничество

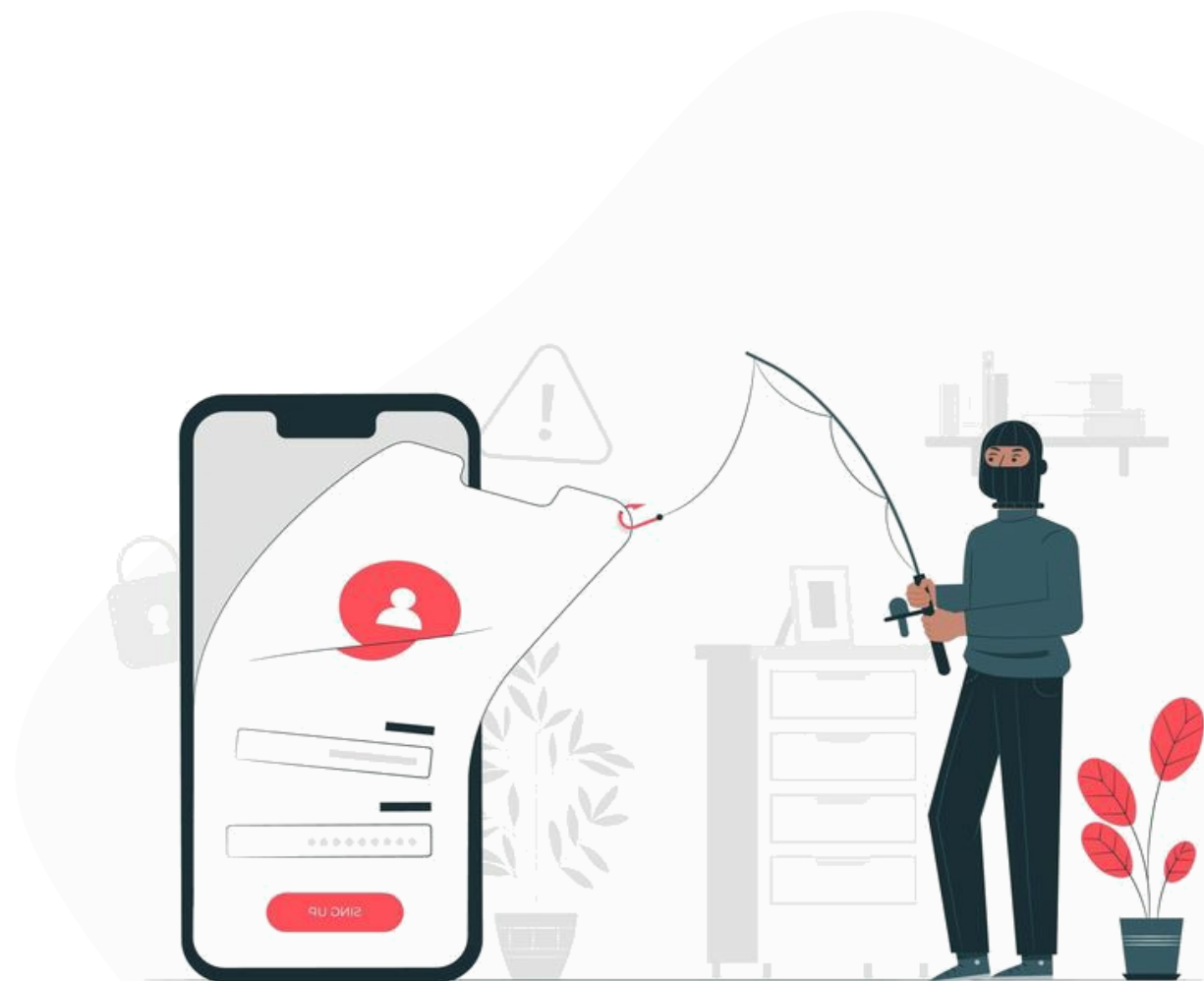


Основные методы кибермошенничества

Технические



Социальные



Вирусы-шифровальщики

Попадая на ваш компьютер, они шифруют ценные файлы: документы, фотографии, сохранения к играм таким образом, что их нельзя открыть



Как себя защитить?

Никогда и ни при каких обстоятельствах **нельзя**:

Переходить

по сомнительным
ссылкам из
электронных писем



Открывать

подозрительные
вложения
электронных писем



Скачивать и устанавливать

«пиратское» или
бесплатное ПО,
полученное из
непроверенных
источников



Использовать

**флешки, внешние
жесткие диски,
телефоны** и др.
устройства,
предварительно не
проверив их
антивирусами



«Белый пластик» или карты-клоны

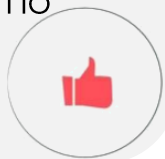
Чтобы завладеть денежными средствами своей жертвы, мошенникам нужна не карта, а ее реквизиты

Злоумышленники могут украсть данные карты с помощью устройств на банкоматах, сфотографировать в кафе или общественном транспорте

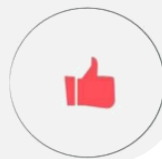


Перед снятием денег в банкомате обращайтесь внимание на следующее:

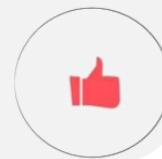
на банкомате не
должно быть
выступающих частей,
тем более
отличающихся по
цвету



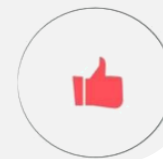
на картоприемнике
не должно быть
посторонних
предметов



клавиатура не
должна шататься



ПИН-код
обязательно
прикрывайте рукой



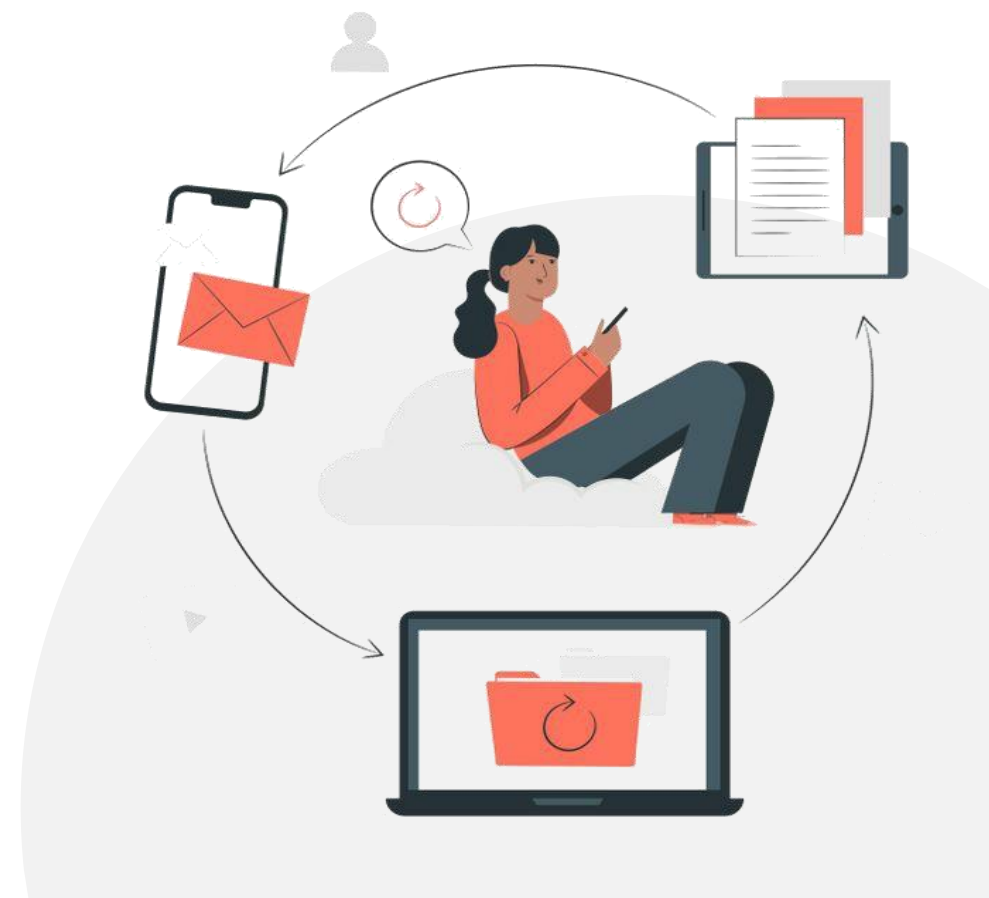
Социальная инженерия

Один из самых известных в мире социальных инженеров, бывший хакер Кевин Митник, говорил, что получал пароли именно путем обмана, а не взламывая систему безопасности с помощью программ.



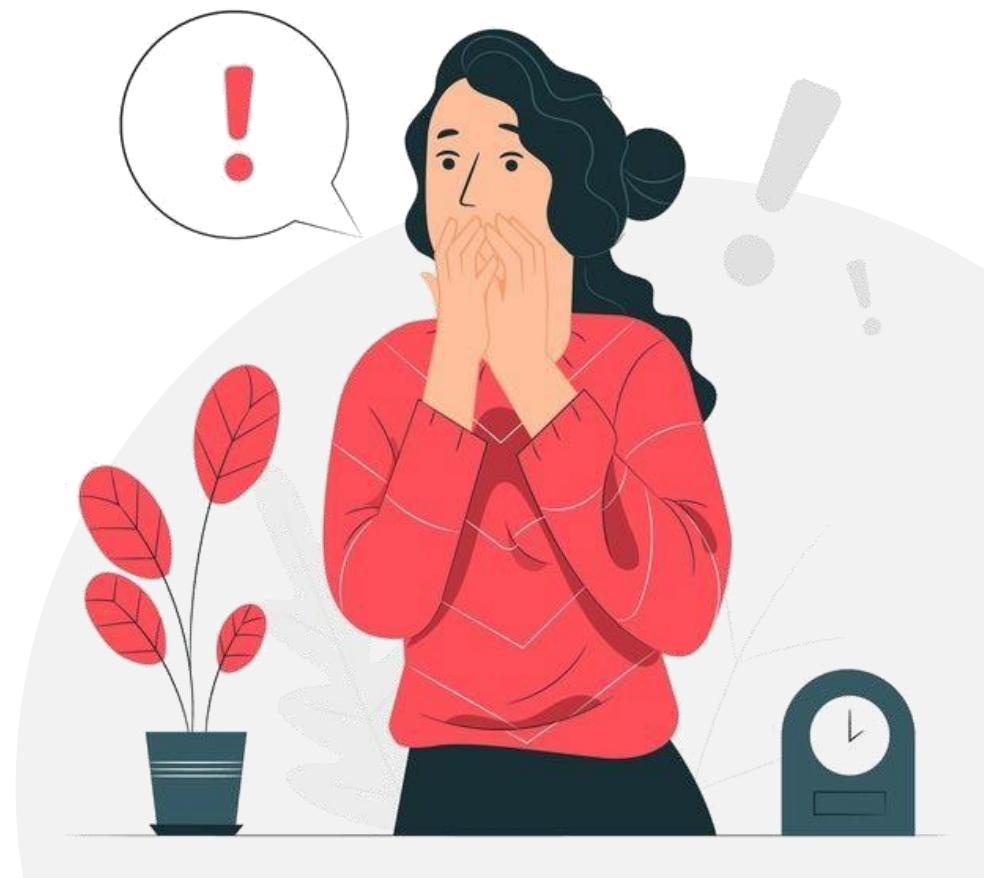
Мобильное мошенничество

это различные СМС-рассылки, требующие пройти по какой-то ссылке для оплаты какой-либо задолженности или услуги, уведомления о неожиданном крупном выигрыше или родственниках, попавших в беду



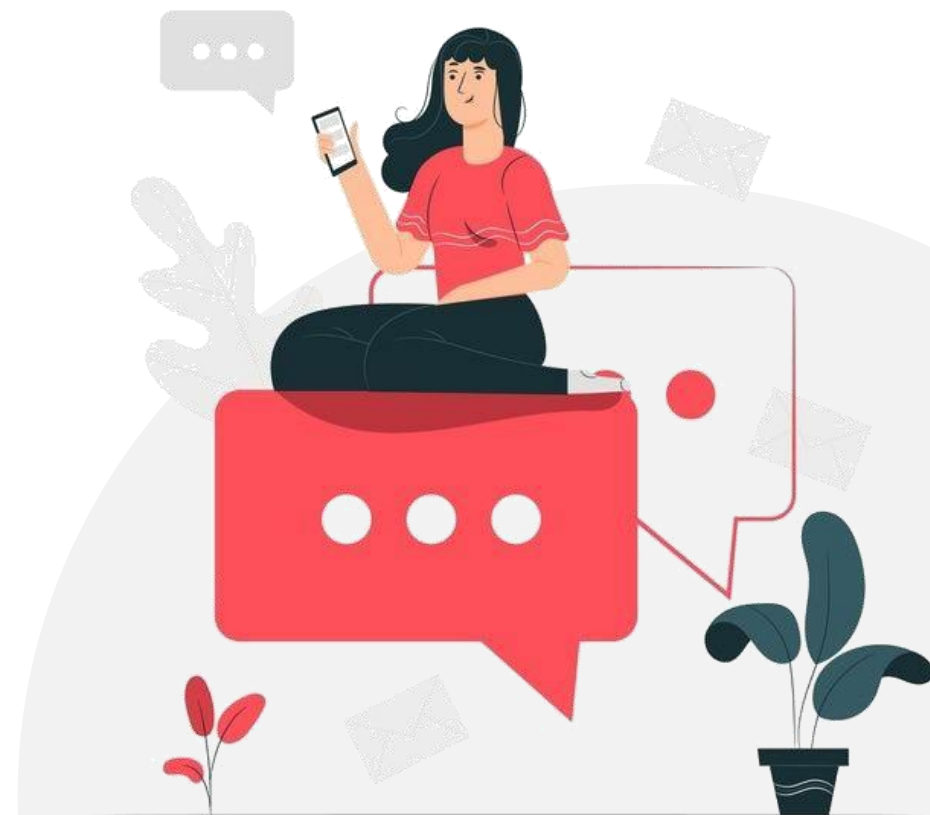
СМС-рассылка или СМС-мошенничество

«На вашем счете заморозена сумма 3 650
рублей из-за факта мошенничества»



Положи на счет...

«Мама, у меня закончились деньги, говорить не могу, пополни мой счет»



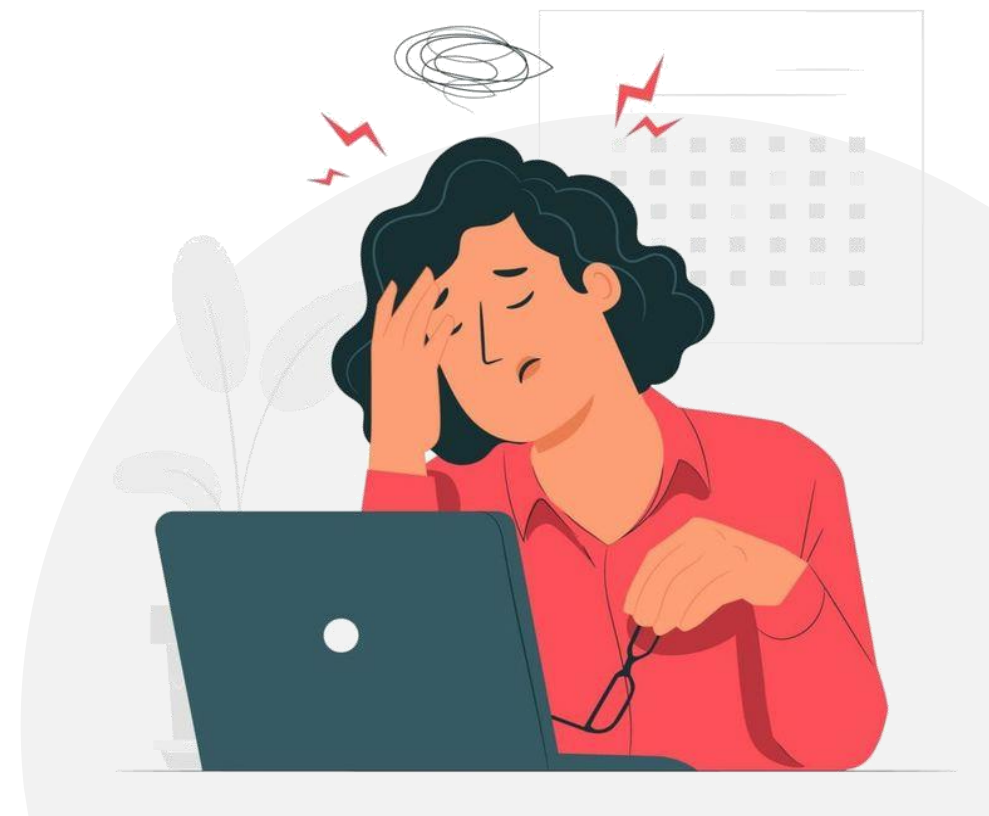
Отдайте деньги

После СМС-оповещения о зачислении средств на счет мобильного телефона раздается звонок с просьбой вернуть деньги, переведенные по ошибке



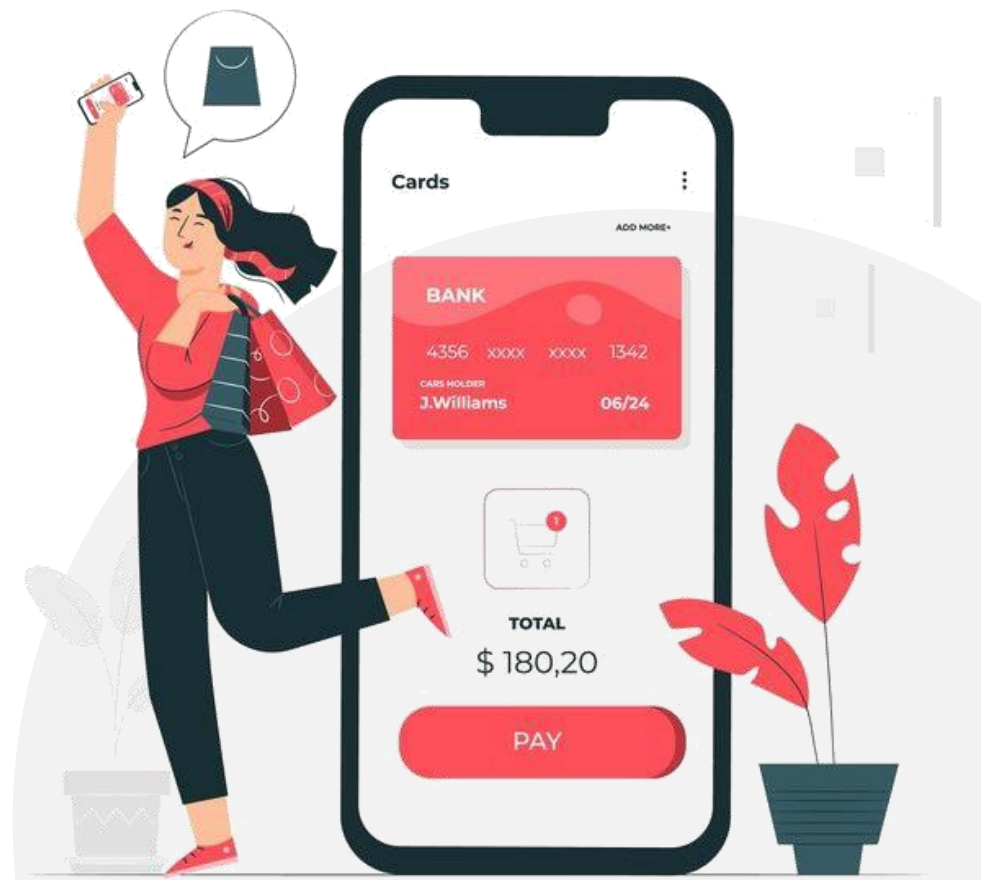
Родственник в беде

Сообщения о родственниках, попавших в ДТП, с
просьбой очевидцев срочно пополнить их
мобильный телефон



Жертве звонит якобы ведущий известной радиостанции и поздравляет ее с выигрышем ценного приза

Республиканский классный час
Кибермошенничество. Как себя защитить?



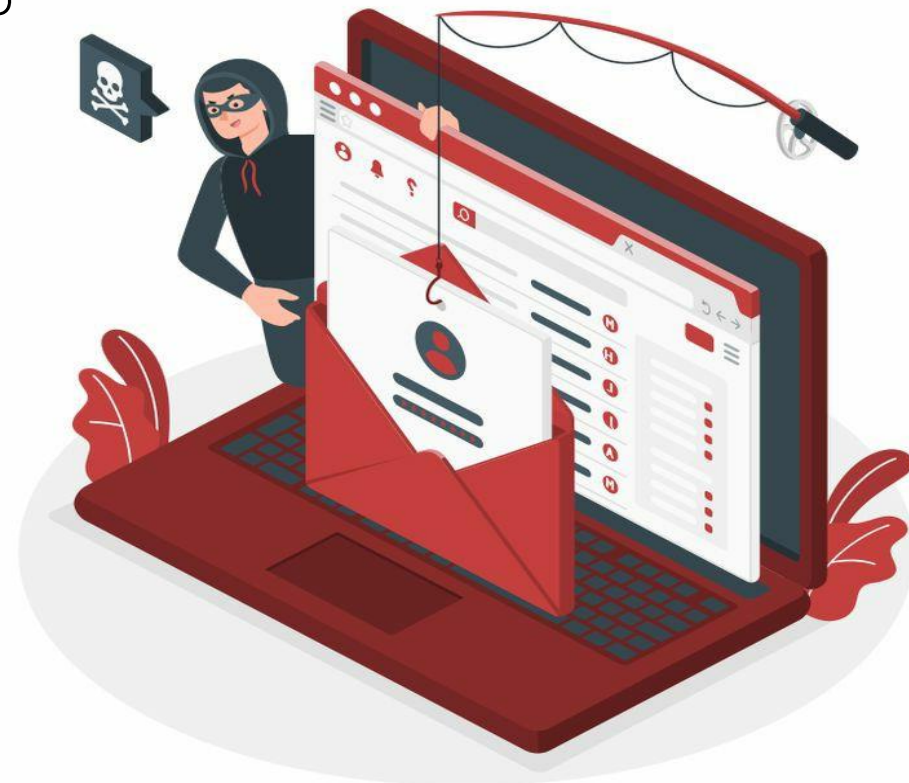
Голос автоинформатора

Голос, записанный на автоответчик, представляется сотрудником банка, сообщает клиенту о списании с его счета определенной суммы денег и просит перезвонить по указанному номеру для установления причин этой операции



Фишинг

это вид мошенничества, когда получение конфиденциальной информации происходит с помощью фальшивых сайтов или поддельных писем со ссылками



Правила кибербезопасности

Пользуйтесь только
личными устройствами
с антивирусной
защитой



Оформите отдельную
карту для совершения
покупок в Интернете



Используйте
безопасные сайты



https://

Используйте систему
безопасных платежей



CVC / CVV



Никогда и ни при каких обстоятельствах
никому не сообщайте
персональную информацию





Банк России

**Будьте бдительны и
не принимайте поспешных решений!**