ВБРР

Финансовая безопасность

Как распознать мошенника и сохранить деньги

Век цифровых технологий

- Маркетплейсы
- Доставка
- Платежи и покупки онлайн
- Онлайн-банкинг

Обратная сторона развития технологий –

рост активности мошенников

Социальная инженерия

- психологическое воздействие с целью совершения определенных действий или разглашения конфиденциальной информации

МЕТОДЫ

обман или злоупотребление доверием

психологическое давление

манипулирование

ЭМОЦИИ,

которые вызывает информация от мошенников:

страх
паника
чувство стыда

радость
надежда
желание получить деньги

15,8 МЛРД ₽

мошенники похитили с банковских счетов россиян в 2023 году*

*по данным Банка России

ВБРР

Телефонное мошенничество

Кем чаще всего представляются мошенники

Сотрудник службы безопасности банка

Работник силовых структур и государственных органов:

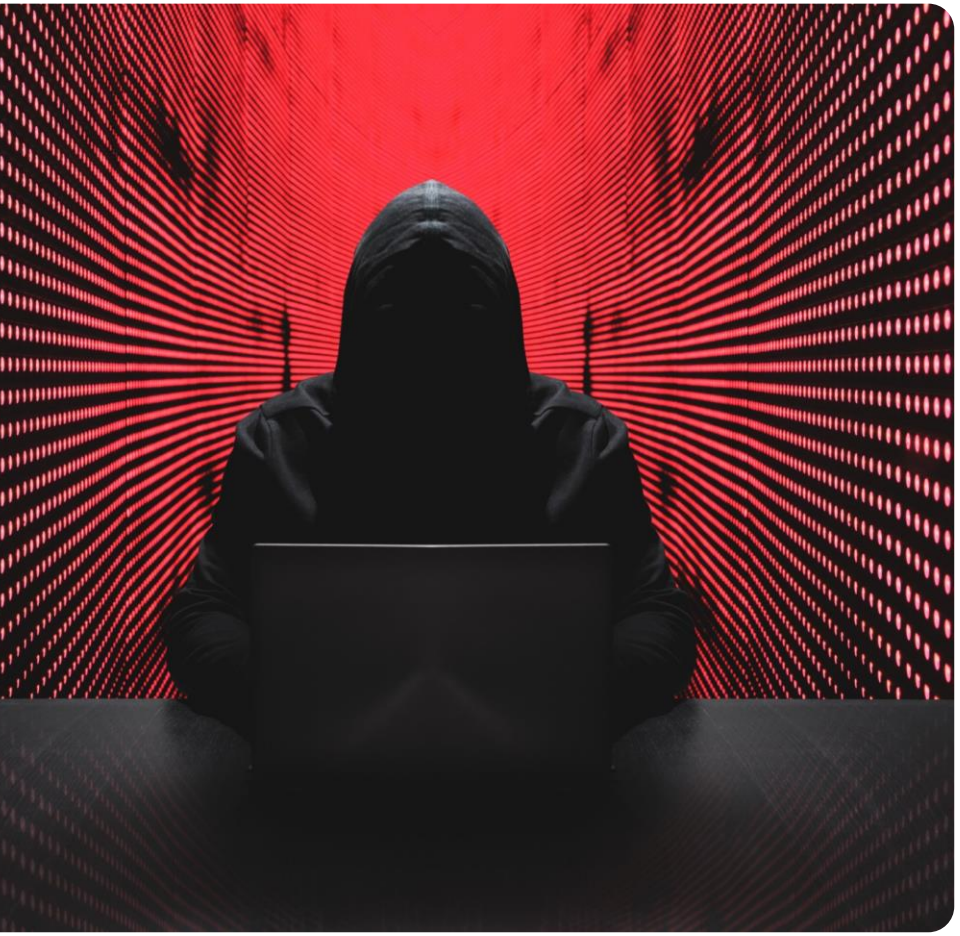
- МВД, ФСБ
- Налоговая служба
- Банк России

и иные

Представитель оператора сотовой связи

Сотрудник портала Госуслуг

5 признаков звонка мошенника



#1 Звонит через мессенджеры

Банки и ведомства
НЕ ЗВОНЯТ
через мессенджеры

#2 Представляется работником Банка России, других министерств и ведомств

Банк России
НЕ ВЗАИМОДЕЙСТВУЕТ
с физическими лицами

#3 Просит сообщить конфиденциальную информацию

Сотрудники банков, ведомств
НЕ СПРАШИВАЮТ
номер карты, CVC, смс, пароли

#4 Пытается вызвать сильные эмоции, сообщает шоковую информацию

#5 Вынуждает провести финансовую операцию: перевод денег на «безопасный» счет, оформление кредита или подтверждение перевода

ВБРР

Сценарии мошенников

Звонок из **«банка»**

Сотрудник «службы безопасности банка»

Цель мошенника

вывести из равновесия, создать чувство паники или страха, отключить критическое мышление

1

Кем представится мошенник

- работник службы безопасности
- персональный менеджер

2

О какой угрозе скажет

- Ваши деньги под угрозой
- нужно предотвратить потерю денег
- Поступила заявка на кредит

3

Частые сценарии

- обновление приложения Банка
- перевод денег на безопасный счет
- необходимо подать заявку на кредит

!

Другие предлоги

- отмена подозрительной операции
- финансовый контроль
- утечка персональных данных или данных по счетам

Звонок от **«правоохранительных органов»**

Сотрудник «надзорных органов»

Цель мошенника

воздействовать авторитетом государственной организации, чтобы надавить и запугать

1

Кем представится мошенник

- сотрудник полиции, Следственного комитета, ФСБ, Службы Финансового мониторинга,
- сотрудник налоговой, ЦБ РФ

2

О какой угрозе / выгоде скажет

- Ваши деньги под угрозой
- нужно срочно предотвратить потерю денег
- проводится доследственная проверка
- **получение дохода** – налоговый вычет

3

Что попросит Вас сделать

- перевести деньги для «сохранности»
- помочь правоохранительным органам в следственных мероприятиях, для этого нужно совершить перевод
- выполнить любые другие действия для помощи правоохранительным органам

Звонок из «Госуслуг»

Представитель «портала Госуслуг»

Цель мошенника

Получить доступ к личному кабинету на портале Госуслуг

1

Кем представится мошенник

- техническая поддержка портала
- сотрудник службы безопасности портала Госуслуг

2

О какой угрозе скажет

- взлом учетной записи на Госуслугах
- учетная запись ошибочно удалена или заблокирована
- корреспонденция от гос.органов

3

Зачем мошенникам доступ

- получить Ваши персональные данные
- получить доступ к Личным кабинетам в банках и других организациях
- отправить заявки на получение займов

!

Если учетная запись взломана

- позвоните в службу поддержки: 115, 8 800 100-70-10 и восстановите доступ
- проверьте заявления, оформленные от Вашего имени
- проверьте и отредактируйте раздел «Согласия и доверенности»

Звонок от **«оператора сотовой связи»**

Представитель «оператора сотовой связи»

Цель мошенника

Выманить учетные данные от личного кабинета абонента

1

Кем представится мошенник

- сотрудник оператора сотовой связи

2

О какой угрозе / выгоде скажет

- завершение срока действия договора / блокировка сим-карты
- нехватка средств на балансе
- настройка / смена тарифа

3

Зачем мошенникам доступ

- переадресация смс для получения одноразовых паролей
- выпуск виртуального дубликата сим-карты
- использование бонусных баллов или денег на счете
- по истории звонков узнать, в каких банках обслуживается абонент

Сообщение от **«руководства»**

Ваш «руководитель»

1

Кем представится мошенник

- Вы получите сообщение / звонок в мессенджере с фейкового аккаунта руководителя

2

О чем сообщит

- нужно выполнить срочное поручение, в связи с проверкой гос.органов или заключением срочной сделки и т.д.

3

Зачем

- получить конфиденциальную информацию о Вас, о коллегах или о компании
- совершить платеж
- дать поручение Вашим подчиненным и вовлечь их в мошенническую схему

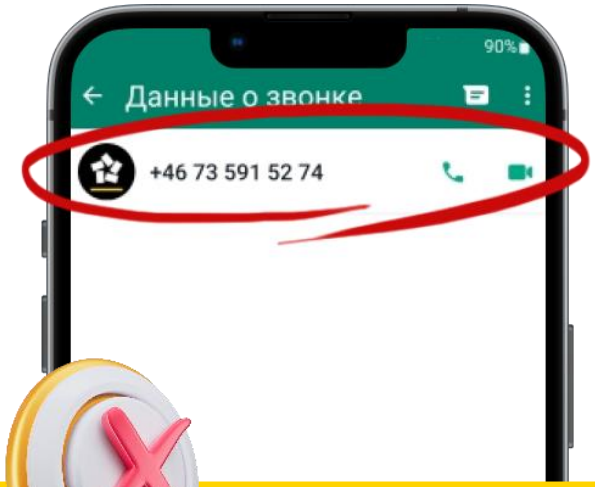
Цель мошенника

Создать шоковую ситуацию, чтобы получить конфиденциальную информацию или выманить денежные средства

Мессенджеры

>60%

мошеннических звонков в 2023 году совершено через мессенджеры*



Почему мошенники используют мессенджеры?

- Нет блокировки со стороны операторов сотовой связи
- Можно направить фиктивный документ в качестве вложения
- На аватарке легко установить логотип банка или ведомства
- Можно направить ссылки, например, на вирусы и вредоносные программы
- Можно использовать подменный номер банка 8800…
- Можно запустить демонстрацию экрана

Банки и государственные органы

НЕ ИСПОЛЬЗУЮТ

мессенджеры для общения с клиентами

НЕ ВКЛЮЧАЙТЕ

демонстрацию экрана по просьбе звонящего

Так мошенники получают доступ к просмотру всех Ваших СМС, банковским приложениям и другой конфиденциальной информации

*по данным экспертов по итогам 2023 года

Программы для удаленного доступа

Мошенники просят установить на смартфон программы для удаленного доступа под предлогом увеличения защищенности устройства или оперативного предотвращения хищения денег

Примеры приложений:

TeamViewer rustdesk Radmin®

НЕ УСТАНАВЛИВАЙТЕ

приложения на телефон по просьбе мошенников

НЕ ВКЛЮЧАЙТЕ

демонстрацию экрана по просьбе звонящего

Так мошенники получают доступ к просмотру всех Ваших СМС, банковским приложениям и другой конфиденциальной информации

ВБРР

Как защитить себя

Соблюдайте правила

#1 Никому не сообщайте, не передавайте, не пересылайте

- коды и одноразовые пароли из смс
- полный номер карты (как физической, так и виртуальной или цифровой)
- данные карты:
код CVV/CVC, срок действия карты
- логины и пароли
- информацию о себе и своих родственниках, иные персональные данные
- информацию о наличии счетов

#2 Не совершайте действия под воздействием третьих лиц

- оформление заявок на кредит
- переводы денежных средств на «безопасные счета»
- перевод на счета сторонних лиц, организаций
- привязку новых номеров телефонов
- передачу денежных средств посторонним лицам
- пополнение счетов через банкоматы
- установку на свой телефон или компьютер программного обеспечения
- включение демонстрации экрана

ПРЕРВИТЕ ЗВОНОК И ПЕРЕЗВОНИТЕ В БАНК САМИ

- по номеру, указанному на Вашей банковской карте
- по номеру, указанному на официальном сайте банка

ВБРР

Фишинг

Фишинг в интернете

от англ. *fishing* «рыбная ловля, выуживание

- вид интернет-мошенничества, целью которого является получение критичной для пользователя информации

Цель

получение логинов, паролей, данных карт

Каналы фишинг-атак

- email
- мессенджеры, социальные сети
- смс

Фишинговое письмо

выглядит как официальное сообщение от банка, гос.органов или интернет-магазина

под предлогом получения выгоды или важной информации побуждает жертву открыть вредоносный файл или перейти по мошеннической ссылке

отправитель письма использует в имени узнаваемое название, но при этом домен отличается от официального

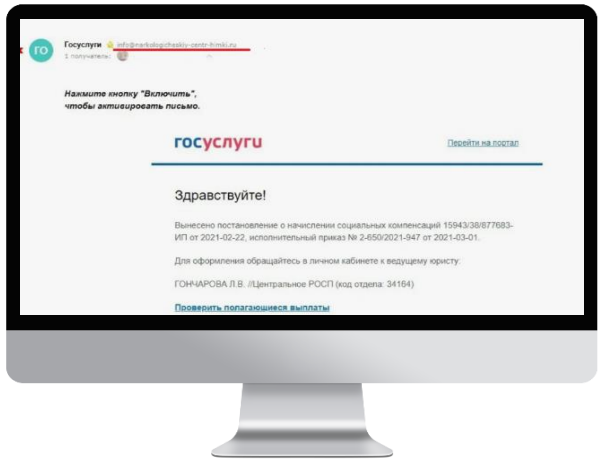
Например:
gosuslugi@mail[.]ru,nalog@hotmail[.]org и т.д.

Как отличить

- содержит вложенные файлы, программы или ссылки
- имеются ошибки в теме и тексте сообщения, бланках, или другие неточности
- предлагает быстрый доход, большие скидки или содержит шоковую информации о проблемах с законом, штрафах
- использование публичных почтовых сервисов для отправки официальных писем

Как себя защитить

- не сообщайте свои учетные и персональные данные
- не открывайте вложения от незнакомых отправителей
- не переходите по подозрительным ссылки
- используйте средства антивирусной защиты на своих устройствах

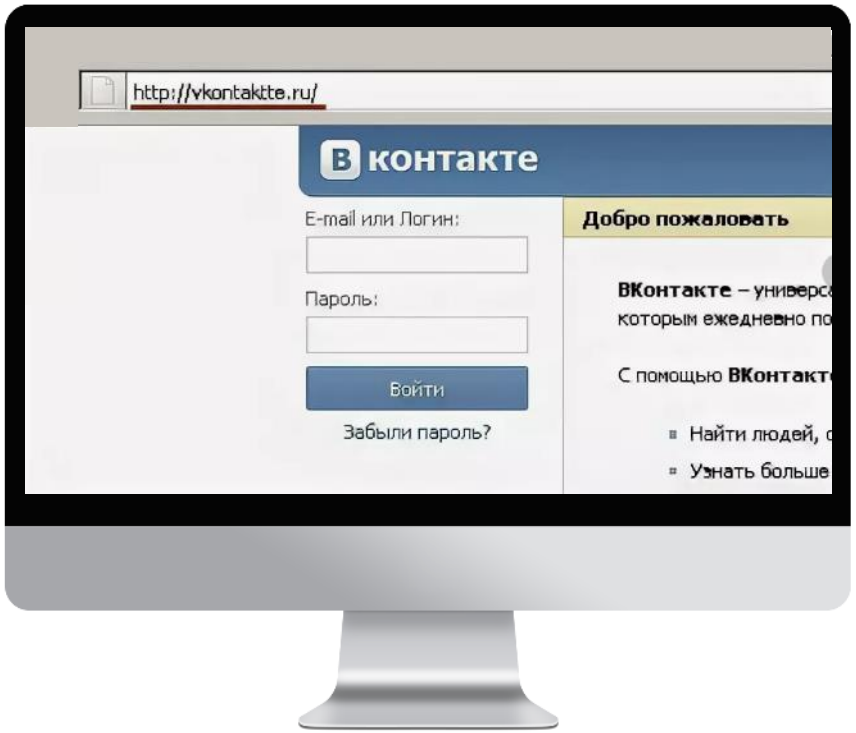


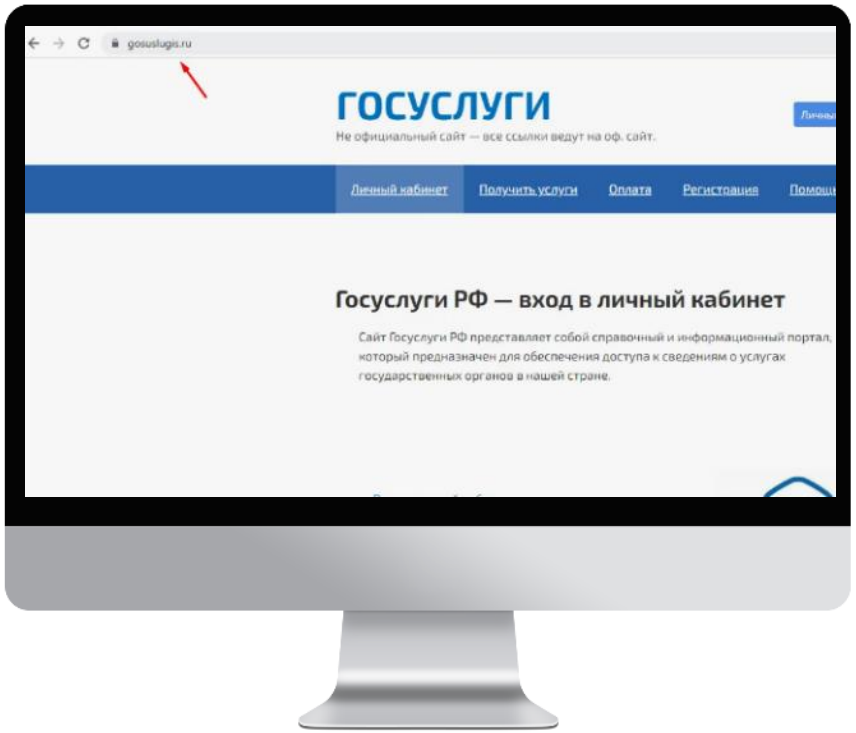
Фишинговые сайты

сайт, который максимально похож на настоящий сайт

создан мошенниками для кражи данных

название поддельного сайта отличается на 1-2 символа от настоящего





Как распознать мошеннический сайт

#1 НЕЗАЩИЩЕННОЕ ПОДКЛЮЧЕНИЕ
Подключение должно быть защищенным: адрес сайта начинается с «https://». В данных сертификата указана информация о владельце, совпадает с адресом сайта

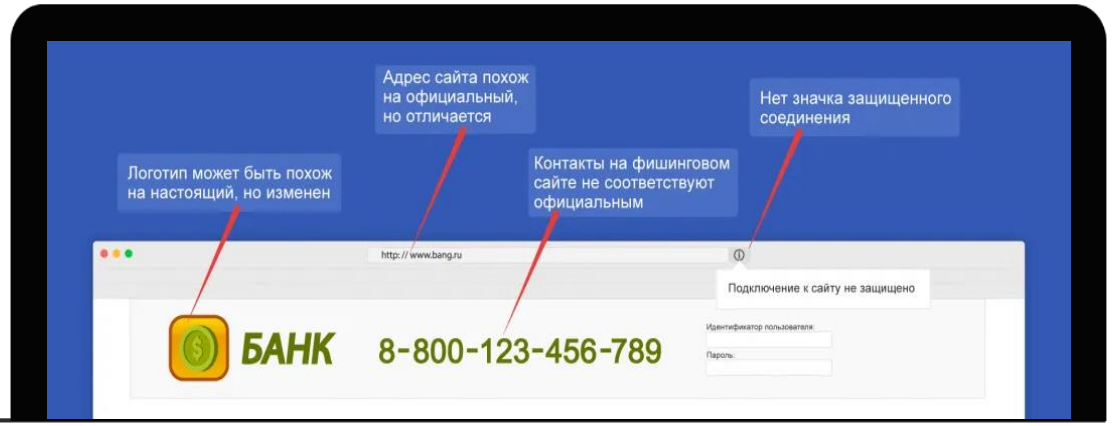
#2 БОЛЬШИЕ СКИДКИ
Не доверяйте большим скидкам и предложениям цены ниже рыночной

#3 ОПЛАТА ТОВАРА ПУТЕМ ПЕРЕВОДА НА КАРТУ ИЛИ ПО НОМЕРУ ТЕЛЕФОНА, ИЛИ ИНЫЕ НЕСТАНДАРТНЫЕ УСЛОВИЯ
Оплата должна производится на защищенной платежной форме Банка по фиксированной цене

#4 НЕКОРРЕКТНЫЙ АДРЕС
В адресе сайта есть 1-2 лишних символа

Как себя обезопасить

- проверьте надежность и безопасность сайта, изучите отзывы, не вводите персональные данные и данные платежной карты, если не уверены в надежности сайта
- не оплачивайте товары и услуги методом перевода физическому лицу (p2p-переводы), убедитесь, что платежная страница принадлежит банку
- внимательно прочитайте текст смс от Банка для подтверждения платежа, проверьте сумму и назначение



ВБРР

Онлайн-платежи

Правила совершения онлайн-платежей

#1 оформите отдельную карту для онлайн-покупок и храните на ней небольшую сумму

#2 не оплачивайте покупки через Wi-Fi в общественных местах и не используйте компьютеры в общественных местах (интернет-кафе, гостиницы и пр.)

#3 оплачивайте покупки только через официальные интернет-магазины

#4 не сообщайте никому пароли из смс от банка

#5 внимательно читайте смс от банка при подтверждении платежа: проверяйте наименование точки продаж, сумму и назначение платежа

ПРЕРВИТЕ ЗВОНОК И ПЕРЕЗВОНИТЕ В БАНК САМИ

- по номеру, указанному на Вашей банковской карте
- по номеру, указанному на официальном сайте банка

ВБРР

Что делать, если стал жертвой мошенника

Если все же случилось…

Заблокируйте карты, счета, доступ в ДБО

Позвоните в Банк по официальному номеру

Оформите заявление о несогласии с операциями

в Банке на официальном бланке

Обратитесь в полицию

Подайте заявление о мошеннических действиях

Дополнительно

- Смените/восстановите пароли ко всем ресурсам, куда потенциально могли получить доступ мошенники
- перевыпустите банковские карты
- на всех ресурсах проверьте историю своих последних действий, изменений аккаунта
- проверьте разрешения и настройки телефона, список установленного программного обеспечения, проведите антивирусную проверку
- проверьте раздел «Согласия и доверенности» на сайте Госуслуг

ВБРР

Соучастие в мошенничестве

Дропперы

- люди, которые помогают обналичивать и выводить деньги после совершения преступником финансового преступления

через суд с Вас могут взыскать сумму, которую мошенники перевели через ваш счет

НЕ СОГЛАШАЙТЕСЬ

на предложения мошенников

Схемы вербовки дропперов

#1 Объявления о заработке, о подработке, связанной с переводами, обналичиванием, работой в IT-сфере

#2 Звонки от правоохранительных органов с целью помочь в поимке преступников

#3 «Случайный» перевод денег на карту с просьбой вернуть их по другим реквизитам

#4 Объявления о покупке действующих банковских карт и доступов в ДБО

#5 Взлом онлайн-банка будущего дроппера не с целью хищения его денег, а с целью вывода уже похищенных

ЗА СОУЧАСТИЕ В МОШЕННИЧЕСТВЕ ПРЕДУСМОТРЕНА ОТВЕТСТВЕННОСТЬ

Статьи Уголовного кодекса

Статья 174	Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем
Статья 187	Неправомерный оборот средств платежей
Статья 159	Мошенничество

ВБРР

Спасибо
за внимание!