

**Как не дать
мошенникам
похитить
деньги**
и заставить
совершить
преступление?

Основные схемы обмана, скрипты,
которые применяют мошенники
для влияния на человека, с целью
украсть средства, и даже заста-
вить совершить преступление



МОШЕННИКИ ВЫНУЖДАЮТ «СПАСАТЬ» СРЕДСТВА / ИМУЩЕСТВО ОТ ЛЖЕМОШЕННИКОВ

КАКИЕ СХЕМЫ ОБМАНА ИСПОЛЬЗУЮТ?

Просят перевести
деньги на
безопасный счет

Предлагают взять
встречный кредит
для исчерпания
кредитного
лимита

Предлагают продать
недвижимость по
доверенности для
предотвращения
сделки

Просят помочь
поймать
мошенников

КАКИЕ СПОСОБЫ ВЛИЯНИЯ?

Звонки, письма по электронной почте,
в почтовый ящик, сообщения от:

- служб безопасности банков
- ЦБ
- ФСБ
- МВД



КАК ЗАЩИТИТЬ СЕБЯ?



Не сообщайте
свои личные и банковские
данные незнакомцам



Не переходите
по ссылкам из сообщений,
удалите его и заблокируйте
злоумышленника



Не совершайте
никаких действий и банковских
операций по инструкциям
звонящих



Узнайте
о состоянии средств, позвонив
в контактный центр вашего банка,
указанный на обороте карты,
в онлайн приложении или
отделении своего банка



Сообщите о звонке /
мошенничестве в свой банк
(Сбербанк по номеру 900)
и в полицию 112



Помните!
сотрудники банков и государственных
органов не звонят / не пишут
в мессенджерах и не отправляют свои
личные документы и не заставляют
совершать нападения на учреждения

МОШЕННИКИ ПОХИЩАЮТ ЛИЧНЫЕ ИЛИ БАНКОВСКИЕ ДАННЫЕ

КАКИЕ СХЕМЫ ОБМАНА ИСПОЛЬЗУЮТ?

Обновите личный кабинет/ аккаунт

Продление договора

Оформление выплат

КАКИЕ СПОСОБЫ ВЛИЯНИЯ?

Звонки, письма по электронной почте, в почтовый ящик, сообщения от:

- Госуслуг
- МФЦ
- Пенс фонд
- Сотовых операторов
- Министерства здравоохранения
- Социальных организаций

КАК ЗАЩИТИТЬ СЕБЯ?



Не сообщайте
свои личные и банковские данные незнакомцам



Не переходите
по ссылкам из сообщений, удалите его и заблокируйте злоумышленника



Не совершайте
никаких действий и банковских операций по инструкциям звонящих



Обратитесь
в официальные органы / организации для проверки информации



Сообщите
о мошенничестве в Банк по номеру 900, в приложении Сбербанк Онлайн или в любом офисе



Сообщите о мошенничестве
в полицию

Помните, что сотрудники банков и государственных органов не звонят / не пишут в мессенджерах и не отправляют свои личные документы и не заставляют совершать нападения на учреждения

МОШЕННИКИ ВЗЛАМЫВАЮТ ИЛИ ПОДДЕЛЫВАЮТ АККАУНТ ВАШЕГО ЗНАКОМОГО ЛИБО ВАШ

КАКИЕ СПОСОБЫ ВЛИЯНИЯ?

- **Руководитель** – с вами свяжутся правоохранительные органы
- **Родственник** – переведи денег
- **Знакомый** – проголосуй

КАК ЗАЩИТИТЬ СЕБЯ?



Не переходите

по ссылкам / не скачивайте файлы / не устанавливайте программы



Не совершайте

никаких переводов, пока лично не убедитесь, что Вам написал Ваш знакомый



Поменяйте пароли

от социальных сетей и мессенджеров



Срочно заблокируйте

или восстановите Ваш аккаунт, если его уже взломали



Сообщите

своим родственникам и знакомым о взломе аккаунта



МОШЕННИКИ ПРЕДЛАГАЮТ БЫСТРО ЗАРАБОТАТЬ / ОБОГАТИТЬСЯ

КАКИЕ СПОСОБЫ ВЛИЯНИЯ?

- Финансовые пирамиды
- Криптовиржи
- Участие в акциях и выполнение заданий
- Получение «выигрыша»
- Доставка «посылок»
- Покупки / переводы в блогах, играх, сайтах

КАК ЗАЩИТИТЬ СЕБЯ?



Не верьте

обещаниям быстрого дохода / выигрыша / получения подарков



Не сообщайте

свои персональные и банковские данные



Не совершайте

покупки / переводы на непроверенных платформах



Не совершайте

никаких действий и банковских операций по инструкциям в сообщениях



Сообщите

о мошенничестве в Банк по номеру 900, в приложении Сбербанк Онлайн или в любом офисе



Сообщите о мошенничестве

в полицию



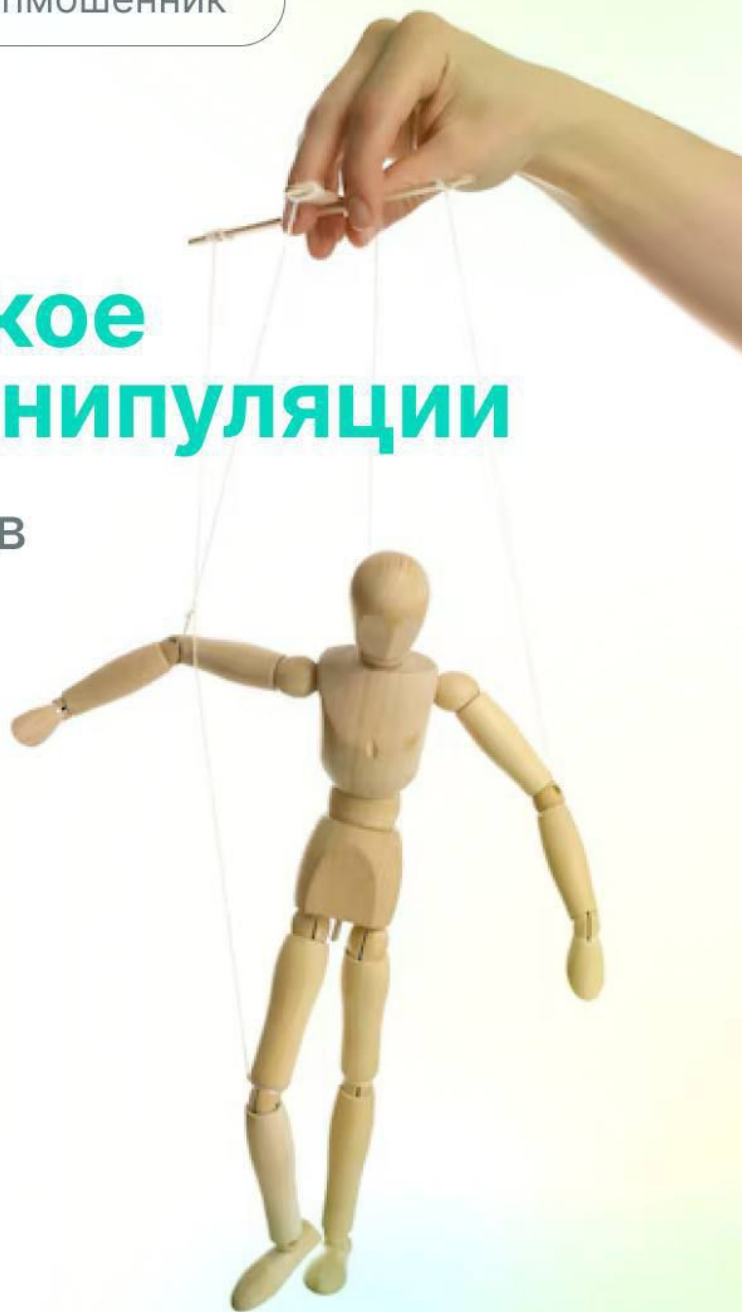
#недайсебяобмануть

#стопмошенник

психологическое давление и манипуляции

со стороны мошенников

важные правила →



#СТОПМОШЕННИК

ПОМНИТЕ

у мошенников нет моральных ориентиров, **они будут играть на ваших чувствах и эмоциях**




БУДЬТЕ БДИТЕЛЬНЫ

необходимо быть готовыми к тому, что **мошенники изобретают новые, еще более изощренные способы обмана**

Основные правила как защитить себя от мошенничества




ЗВОНКИ / СООБЩЕНИЯ ИЗ «СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА» ИЛИ «ПРЕДСТАВИТЕЛЕЙ ГОС. ОРГАНОВ»

ЧТО ДЕЛАТЬ?

-  Не отвечайте на звонки с неизвестных номеров
-  Не совершайте никаких действий и банковских операций по инструкциям звонящего
-  При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру горячей линии или обратитесь в любой офис Банка**






СООБЩЕНИЕ ОТ «РУКОВОДИТЕЛЯ» ИЛИ ЗВОНОК / СООБЩЕНИЕ ОТ БЛИЗКОГО РОДСТВЕННОГО

ЧТО ДЕЛАТЬ?

-  Свяжитесь со своим руководителем, от которого якобы поступило сообщение или со своим родственником, по известному Вам номеру
-  Не совершайте никаких действий и банковских операций по инструкциям звонящего или из сообщений
-  При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру горячей линии или обратитесь в любой офис Банка**




ЗВОНКИ/СООБЩЕНИЯ ОТ «ПРЕДСТАВИТЕЛЕЙ ГОС. ОРГАНОВ» С УГРОЗОЙ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ

ЧТО ДЕЛАТЬ?

-  Сохраняйте спокойствие, не паникуйте и не поддавайтесь на эмоциональное давление мошенников
-  Не предоставляйте **персональную информацию**
-  Сбросьте звонок/Запишите номер звонившего
-  Сообщите о случившемся в полицию/оповестите Банк
-  Проинформируйте своих близких

ПОСТУПЛЕНИЕ ЗВОНКА/СООБЩЕНИЯ ОТ «СОТОВОГО ОПЕРАТОРА»


ЧТО ДЕЛАТЬ?


-  Не совершайте никаких действий: не переходите по ссылкам; не указывайте свои данные; не скачивайте какие-либо направленные в сообщении/письме файлы
-  Перепроверьте информацию, позвонив своему сотовому оператору на официальный номер телефона (указан на сайте)
-  Удалите сообщение / письмо

Основные правила как защитить себя от мошенничества

ПОСТУПЛЕНИЕ СООБЩЕНИЯ ОТ «ГОСУСЛУГ» ИЛИ «ПОЧТЫ РОССИИ»

ЧТО ДЕЛАТЬ?


 **Не совершайте никаких действий:** не переходите по ссылкам; не указывайте свои данные; не скачивайте какие-либо закрепленные в сообщении/письме файлы


 **Перепроверьте информацию в личном кабинете на официальном сайте / в мобильном приложении**


 **Удалите сообщение / письмо**

УСТАНОВКА ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЧТО ДЕЛАТЬ?


 **Не устанавливайте программы по просьбе 3-х лиц на телефон**


 **Не совершайте никаких действий** и банковских операций по инструкциям звонящего


 При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру горячей линии** или обратитесь в любой офис Банка


ВЗЛОМ АККАУНТОВ В МЕССЕНДЖЕРАХ/СОЦИАЛЬНЫХ СЕТЯХ – РАССЫЛКА СООБЩЕНИЙ С ПРОСЬБОЙ ПЕРЕВОДА ДЕНЕГ В ДОЛГ

ЧТО ДЕЛАТЬ?

 **Не совершайте никаких переводов,** пока лично не убедитесь, что Вам написал Ваш знакомый


 **Поменяйте пароли от социальных сетей и мессенджеров, если они очень простые** (Имя/Фамилия, дата рождения, простые слова и т.д.)


 **Если Ваш аккаунт уже взломали, то немедленно восстановите его**


 **Незамедлительно уведомите своих родственников и знакомых,** которым мошенники успели отправить сообщения, о взломе Вашего аккаунта

УЧАСТИЕ В АКЦИЯХ И ВЫПОЛНЕНИЕ ЗАДАНИЙ

ЧТО ДЕЛАТЬ?

 **Не сообщайте свои персональные данные,** в частности банковские реквизиты (ваши деньги могут украсть)

 **Не совершайте никаких действий** и банковских операций по инструкциям звонящего

 При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру горячей линии** или обратитесь в любой офис Банка